Copyrights and Notices

Copyright

© 2015 Attachmate Corporation. All rights reserved.

No part of the documentation materials accompanying this Attachmate software product may be reproduced, transmitted, transcribed, or translated into any language, in any form by any means, without the written permission of Attachmate Corporation.

Patents

This Attachmate software is protected by U.S. patents 6252607 and 6803914. Additional Patent Pending.

Trademarks

Attachmate, the Attachmate logo, and Reflection are registered trademarks of Attachmate Corporation in the USA. All other trademarks, trade names, or company names referenced in this product are used for identification only and are the property of their respective owners.

Attachmate Corporation
705 5th Avenue South
Suite 1100
Seattle, WA 98104
USA
+1.206.217.7100
http://www.attachmate.com

Third-Party Notices

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org).

Additional third-party notices, including copyrights and software license texts, can be found in a 'thirdpartynotices' file in the root directory of the software.
## Contents

**Introduction**  
11

**1 What's New?**  
15

**2 InfoConnect Technical Notes**  
17

**3 Installation**  
19
- System Requirements ............................................................. 19
- Upgrading from Previous Versions .......................................... 20
- Install Reflection on a Workstation ........................................ 22
- Features Selection Tab ......................................................... 23
- Set Your User Data Directory .................................................. 24
- Advanced Tab ........................................................................... 24

**4 How Do I?**  
27
- Add a Button that Opens a Session Document .............................. 28
- Add Controls to the Ribbon ........................................................ 28
  - Add a Button ......................................................................... 29
  - Add a Button to Run a Macro .................................................. 30
  - Add a Button with an Action and a Menu .................................. 31
  - Add a Menu that Holds Buttons .............................................. 31
  - Add a Group ........................................................................... 32
  - Add a Group of Buttons .......................................................... 32
  - Add a Dialog Launcher to a Group ............................................ 33
  - Add a Tab ............................................................................... 34
- Add a Keyboard Shortcut That Sends Special Character Data (VT) .... 34
- Configure Host Connection Options .......................................... 35
- Configure Color Settings ............................................................ 35
- Configure non-FTP File Transfer ................................................ 36
- Configure Workspace Arrangement ............................................ 37
- Copy and Paste Host Data .......................................................... 39
- Create a Custom Context Menu ................................................ 40
- Create a New Theme File ............................................................ 41
- Customize Microsoft Office Productivity Features .......................... 42
- Customize the Quick Access Toolbar ........................................... 42
- Create or Modify a Layout .......................................................... 43
- Define Hot Spots ....................................................................... 45
- Edit the Translation Table .......................................................... 46
- Edit or Move a Button on the Quick Access Toolbar ....................... 47
- Import Legacy VT Toolbars to the Ribbon ..................................... 47
- Map a Sound to an Event ............................................................ 48
- Minimize the Ribbon .................................................................. 49
- Modify Existing Controls on the Ribbon ....................................... 49
- Move Controls on the Ribbon ...................................................... 50
- Open a Layout .......................................................................... 51
- Print More Than One Screen per Page ........................................ 52
# The User Interface

- **Using the Browser** .................................................. 69
- **Configuring InfoConnect** ............................................ 70
- **Using Layouts** .......................................................... 72
  - Layout Settings Dialog Box ........................................... 72
  - Tab Properties Dialog Box ........................................... 73
- **Customize the Ribbon** ................................................. 74
  - Add Controls to the Ribbon ........................................... 75
  - Remove Controls from the Ribbon ................................... 81
  - Modify Existing Controls on the Ribbon .......................... 81
  - Move Controls on the Ribbon ......................................... 82
  - Restore the Default Ribbon .......................................... 83
  - Manage Ribbon Dialog Box ........................................... 83
  - Select a Ribbon File Dialog Box .................................... 84
  - UI Designer ............................................................... 84
  - Create a New Ribbon File Dialog Box ............................... 87
  - Subitems Collection Editor Dialog Box (UI Designer) ............ 87
  - Built-In Controls Dialog Box (UI Designer) ........................ 88
  - Locking Down the User Interface .................................... 89
- **The User Interface** .................................................... 120
- **Create New Document Dialog Box** .................................. 122
- **Change the UI Language** ............................................. 123
- **InfoConnect Workspace Settings Dialog Box** ...................... 124
- **Configure Workspace Defaults Dialog Box** ........................ 125
- **Configure Workspace Attributes Dialog Box** .................... 128
- **Configure User Interface Dialog Box** ............................. 129
- **Manage On-Screen Keyboard Settings** ............................. 131
- **Manage Themes Dialog Box** ......................................... 132
- **Select a Theme File Dialog Box** ................................... 133
- **Modify Theme Dialog Box (3270 Terminal Sessions)** .......... 133
- **Modify Theme Dialog Box (5250 Terminal Sessions)** .......... 136
- **Modify Theme Dialog Box (VT Terminal Sessions)** ............ 139
- **Manage QuickPads Dialog Box** .................................... 141
- **Workspace Settings Dialog Box** .................................... 143
# Terminal Sessions

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session Documents and Related Files</td>
<td>146</td>
</tr>
<tr>
<td>Create a Session Document File</td>
<td>147</td>
</tr>
<tr>
<td>Open a Terminal Session</td>
<td>148</td>
</tr>
<tr>
<td>Share Sessions as Templates</td>
<td>149</td>
</tr>
<tr>
<td>Encrypt a Session File</td>
<td>151</td>
</tr>
<tr>
<td>Connecting to the Host</td>
<td>152</td>
</tr>
<tr>
<td>Context Menu Editor Dialog Box</td>
<td>153</td>
</tr>
<tr>
<td>Terminal Settings</td>
<td>155</td>
</tr>
<tr>
<td>Configuring Input and Text Handling</td>
<td>155</td>
</tr>
<tr>
<td>Clear the Clipboard on Close</td>
<td>155</td>
</tr>
<tr>
<td>Quick Keys</td>
<td>156</td>
</tr>
<tr>
<td>Select Action Dialog Box</td>
<td>161</td>
</tr>
<tr>
<td>Configure Clipboard Settings Dialog Box (3270 and 5250)</td>
<td>165</td>
</tr>
<tr>
<td>Configure Clipboard Settings Dialog Box (VT)</td>
<td>167</td>
</tr>
<tr>
<td>Manage Hotspots Dialog Box</td>
<td>169</td>
</tr>
<tr>
<td>Select a Hotspots File Dialog Box</td>
<td>169</td>
</tr>
<tr>
<td>Modify Hotspots Dialog Box</td>
<td>170</td>
</tr>
<tr>
<td>Hotspot Options Dialog Box</td>
<td>171</td>
</tr>
<tr>
<td>Set Up Hotspot Display Settings Dialog Box</td>
<td>173</td>
</tr>
<tr>
<td>Create a New Hotspots File Dialog Box</td>
<td>175</td>
</tr>
<tr>
<td>Specify which Dialog Box to Open when InfoConnect Starts</td>
<td>175</td>
</tr>
<tr>
<td>Set Up a Workspace Startup Action Sequence</td>
<td>176</td>
</tr>
<tr>
<td>Specifying a Custom Keyboard Map</td>
<td>177</td>
</tr>
<tr>
<td>Select the Keyboard Map for a Session</td>
<td>177</td>
</tr>
<tr>
<td>Create a Custom Keyboard Map</td>
<td>178</td>
</tr>
<tr>
<td>Add a Keyboard Shortcut</td>
<td>179</td>
</tr>
<tr>
<td>Delete a Keyboard Shortcut</td>
<td>180</td>
</tr>
<tr>
<td>Restore the Default Keyboard Map</td>
<td>181</td>
</tr>
<tr>
<td>Manage Keyboard Map Dialog Box</td>
<td>181</td>
</tr>
<tr>
<td>Select a Keyboard Map File Dialog Box</td>
<td>182</td>
</tr>
<tr>
<td>Keyboard Mapper</td>
<td>183</td>
</tr>
<tr>
<td>Create a New Keyboard Map File Dialog Box</td>
<td>183</td>
</tr>
<tr>
<td>Specifying a Mouse Map</td>
<td>184</td>
</tr>
<tr>
<td>Select the Mouse Map for a Session</td>
<td>185</td>
</tr>
<tr>
<td>Add a Mouse Action</td>
<td>185</td>
</tr>
<tr>
<td>Delete a Mouse Action</td>
<td>186</td>
</tr>
<tr>
<td>Restore the Default Mouse Map</td>
<td>187</td>
</tr>
<tr>
<td>Manage Mouse Map Dialog Box</td>
<td>187</td>
</tr>
<tr>
<td>Select a Mouse Map File Dialog Box</td>
<td>188</td>
</tr>
<tr>
<td>Mouse Mapper</td>
<td>189</td>
</tr>
<tr>
<td>Create a New Mouse Map File Dialog Box</td>
<td>190</td>
</tr>
<tr>
<td>Productivity Tools</td>
<td>190</td>
</tr>
<tr>
<td>Integrate Host Data with Office Tools</td>
<td>192</td>
</tr>
<tr>
<td>Enter Data with Recent Typing</td>
<td>195</td>
</tr>
<tr>
<td>Take Notes with Scratch Pad</td>
<td>196</td>
</tr>
<tr>
<td>Enter Data with Auto Complete</td>
<td>197</td>
</tr>
<tr>
<td>Enter Data with Auto Expand</td>
<td>198</td>
</tr>
<tr>
<td>Find and Fix Spelling Errors</td>
<td>199</td>
</tr>
<tr>
<td>Create a Custom Spell Check Dictionary</td>
<td>201</td>
</tr>
<tr>
<td>Configure Office Tools Dialog Box</td>
<td>202</td>
</tr>
<tr>
<td>Office Tools Dialog Box</td>
<td>203</td>
</tr>
<tr>
<td>Configure Recent Typing Dialog Box</td>
<td>204</td>
</tr>
<tr>
<td>Configure Auto Complete Dialog Box</td>
<td>205</td>
</tr>
<tr>
<td>Configure Auto Expand Dialog Box</td>
<td>207</td>
</tr>
<tr>
<td>Configure Spell Checking Dialog Box</td>
<td>208</td>
</tr>
<tr>
<td>Configure Productivity Defaults Dialog Box</td>
<td>210</td>
</tr>
<tr>
<td>IBM 3270 Sessions</td>
<td>211</td>
</tr>
</tbody>
</table>
7 Navigation

Open a Web Session ............................................. 315
Navigate the Ribbon .......................................... 317
Search .......................................................... 318
Capture Screen History ....................................... 320
Capture Screens Manually .................................... 322
Navigate Screen History From the Ribbon .............. 323
Configure Screen History Dialog Box ...................... 324
Create New Web Session Document Dialog Box ........... 325

8 Secure Connections

FIPS Mode ....................................................... 327
Protecting Data and Information Privacy ................. 328
Add Trusted Locations ....................................... 329
Specify Trusted Locations Dialog Box ..................... 329
Set Up Information Privacy Dialog Box .................... 330
Add (or Modify) Privacy Filter Dialog Box ............... 334
Add (or Modify) Custom Detection Rule or Exception Dialog Box 334
Set Up API and Macro Security Dialog Box .............. 335
SSL/TLS Connections .......................................... 337
SSL/TLS Overview ............................................. 337
Connect Using SSL/TLS ....................................... 339
Digital Certificates in SSL/TLS Sessions .................... 341
## Contents

- Troubleshooting SSL/TLS Error Messages ........................................... 342
- Secure Shell Connections ................................................................. 347
- Secure Shell Overview ................................................................. 347
- Connect using Secure Shell (SSH) .......................................................... 349
- Configure Secure Shell Settings ........................................................... 351
- Understanding Secure Shell ............................................................. 352
- Reflection Secure Shell Settings Dialog Box ........................................... 353
- Authentication .................................................................................. 359
- Certificate Authentication (PKI) .......................................................... 363
- Public Key Authentication .................................................................. 363
- GSSAPI (Kerberos) Authentication for Secure Shell Sessions ................. 385
- Port Forwarding .................................................................................. 391
- Secure Shell Configuration Files .......................................................... 402
- Command Line Utilities ...................................................................... 423
- Troubleshooting Secure Shell ............................................................... 435
- Certificate Authentication (PKI) .......................................................... 437
  - PKI Overview ................................................................................. 438
  - Enabling and Disabling Use of the Windows Certificate Store .............. 439
  - Configuring Certificate Revocation Checking ..................................... 440
  - Distributing Intermediate Certificates using an LDAP Directory .......... 441
  - DOD PKI Information ................................................................. 442
  - Reflection Certificate Manager .................................................... 446
- SOCKS or HTTP ................................................................................. 454
  - SOCKS Overview ............................................................................ 455
  - Socks Configuration Dialog Box ....................................................... 455
  - Set up a SOCKS or HTTP Proxy Server Session .................................. 457
- HTTP Configuration Dialog Box .......................................................... 458
- Routing Filter Dialog Box .................................................................... 460
- Kerberos Connections ......................................................................... 461
  - Kerberos Overview ........................................................................... 462
  - Connect Using Kerberos .................................................................... 462
  - Reflection Kerberos Initial Configuration Dialog Box ....................... 464
  - Kerberos Manager ................................................................. 465
- Security Properties Dialog Box ............................................................... 511
  - Which Protocols Can I Use? ............................................................ 512
  - Firewall Tab (Security Properties Dialog Box) .................................... 513
  - Kerberos Tab (Security Properties Dialog Box) .................................... 514
  - Secure Shell Tab (Security Properties Dialog Box) .......................... 516
  - Proxy Tab (Security Properties Dialog Box) ....................................... 517
  - SSL/TLS Tab (Security Properties Dialog Box) ..................................... 518
  - SSL/TLS Tab (FTP Options) .............................................................. 521
  - PKI Configuration Dialog Box ....................................................... 523

### 9 Printing

- Printing from IBM Sessions ................................................................. 525
  - 3270 Printer Emulation .................................................................... 526
  - 5250 Printer Emulation .................................................................... 535
  - Configure Printer Session Settings ................................................... 546
  - Page Setup Dialog Box ................................................................. 548
  - Page Options Dialog Box ............................................................... 550
  - Page Scaling Dialog Box .................................................................. 551
  - Print Setup Dialog Box .................................................................... 552
  - Printing to a Form or Label ............................................................. 554
  - Reset Printer Session to Defaults ...................................................... 554
  - Run a Trace (Printer Sessions) .......................................................... 555
  - Save Changes on Exit (Printer Sessions) ............................................ 556
  - Printing IBM Host Terminal Screens ................................................ 557
- Printing from VT Sessions ................................................................. 559

- Troubleshooting SSL/TLS Error Messages ........................................... 342
- Secure Shell Connections ................................................................. 347
- Secure Shell Overview ...................................................................... 347
- Connect using Secure Shell (SSH) ......................................................... 349
- Configure Secure Shell Settings ........................................................ 351
- Understanding Secure Shell ............................................................. 352
- Reflection Secure Shell Settings Dialog Box ......................................... 353
- Authentication .................................................................................. 359
- Certificate Authentication (PKI) .......................................................... 363
- Public Key Authentication .................................................................. 363
- GSSAPI (Kerberos) Authentication for Secure Shell Sessions .......... 385
- Port Forwarding .................................................................................. 391
- Secure Shell Configuration Files .......................................................... 402
- Command Line Utilities ...................................................................... 423
- Troubleshooting Secure Shell ............................................................... 435
- Certificate Authentication (PKI) .......................................................... 437
  - PKI Overview ................................................................................. 438
  - Enabling and Disabling Use of the Windows Certificate Store .......... 439
  - Configuring Certificate Revocation Checking .................................. 440
  - Distributing Intermediate Certificates using an LDAP Directory ....... 441
  - DOD PKI Information ................................................................. 442
  - Reflection Certificate Manager .................................................... 446
- SOCKS or HTTP ................................................................................. 454
  - SOCKS Overview ............................................................................ 455
  - Socks Configuration Dialog Box ....................................................... 455
  - Set up a SOCKS or HTTP Proxy Server Session ............................... 457
- HTTP Configuration Dialog Box .......................................................... 458
- Routing Filter Dialog Box .................................................................... 460
- Kerberos Connections ......................................................................... 461
  - Kerberos Overview ........................................................................... 462
  - Connect Using Kerberos .................................................................... 462
  - Reflection Kerberos Initial Configuration Dialog Box ....................... 464
  - Kerberos Manager ................................................................. 465
- Security Properties Dialog Box ............................................................... 511
  - Which Protocols Can I Use? ............................................................ 512
  - Firewall Tab (Security Properties Dialog Box) .................................... 513
  - Kerberos Tab (Security Properties Dialog Box) .................................... 514
  - Secure Shell Tab (Security Properties Dialog Box) .......................... 516
  - Proxy Tab (Security Properties Dialog Box) ....................................... 517
  - SSL/TLS Tab (Security Properties Dialog Box) ..................................... 518
  - SSL/TLS Tab (FTP Options) .............................................................. 521
  - PKI Configuration Dialog Box ....................................................... 523

### 9 Printing

- Printing from IBM Sessions ................................................................. 525
  - 3270 Printer Emulation .................................................................... 526
  - 5250 Printer Emulation .................................................................... 535
  - Configure Printer Session Settings ................................................... 546
  - Page Setup Dialog Box ................................................................. 548
  - Page Options Dialog Box ............................................................... 550
  - Page Scaling Dialog Box .................................................................. 551
  - Print Setup Dialog Box .................................................................... 552
  - Printing to a Form or Label ............................................................. 554
  - Reset Printer Session to Defaults ...................................................... 554
  - Run a Trace (Printer Sessions) .......................................................... 555
  - Save Changes on Exit (Printer Sessions) ............................................ 556
  - Printing IBM Host Terminal Screens ................................................ 557
- Printing from VT Sessions ................................................................. 559

- Troubleshooting SSL/TLS Error Messages ........................................... 342
- Secure Shell Connections ................................................................. 347
- Secure Shell Overview ...................................................................... 347
- Connect using Secure Shell (SSH) ......................................................... 349
- Configure Secure Shell Settings ........................................................ 351
- Understanding Secure Shell ............................................................. 352
- Reflection Secure Shell Settings Dialog Box ......................................... 353
- Authentication .................................................................................. 359
- Certificate Authentication (PKI) .......................................................... 363
- Public Key Authentication .................................................................. 363
- GSSAPI (Kerberos) Authentication for Secure Shell Sessions .......... 385
- Port Forwarding .................................................................................. 391
- Secure Shell Configuration Files .......................................................... 402
- Command Line Utilities ...................................................................... 423
- Troubleshooting Secure Shell ............................................................... 435
- Certificate Authentication (PKI) .......................................................... 437
  - PKI Overview ................................................................................. 438
  - Enabling and Disabling Use of the Windows Certificate Store .......... 439
  - Configuring Certificate Revocation Checking .................................. 440
  - Distributing Intermediate Certificates using an LDAP Directory ....... 441
  - DOD PKI Information ................................................................. 442
  - Reflection Certificate Manager .................................................... 446
- SOCKS or HTTP ................................................................................. 454
  - SOCKS Overview ............................................................................ 455
  - Socks Configuration Dialog Box ....................................................... 455
  - Set up a SOCKS or HTTP Proxy Server Session ............................... 457
- HTTP Configuration Dialog Box .......................................................... 458
- Routing Filter Dialog Box .................................................................... 460
- Kerberos Connections ......................................................................... 461
  - Kerberos Overview ........................................................................... 462
  - Connect Using Kerberos .................................................................... 462
  - Reflection Kerberos Initial Configuration Dialog Box ....................... 464
  - Kerberos Manager ................................................................. 465
- Security Properties Dialog Box ............................................................... 511
  - Which Protocols Can I Use? ............................................................ 512
  - Firewall Tab (Security Properties Dialog Box) .................................... 513
  - Kerberos Tab (Security Properties Dialog Box) .................................... 514
  - Secure Shell Tab (Security Properties Dialog Box) .......................... 516
  - Proxy Tab (Security Properties Dialog Box) ....................................... 517
  - SSL/TLS Tab (Security Properties Dialog Box) ..................................... 518
  - SSL/TLS Tab (FTP Options) .............................................................. 521
  - PKI Configuration Dialog Box ....................................................... 523

### 9 Printing

- Printing from IBM Sessions ................................................................. 525
  - 3270 Printer Emulation .................................................................... 526
  - 5250 Printer Emulation .................................................................... 535
  - Configure Printer Session Settings ................................................... 546
  - Page Setup Dialog Box ................................................................. 548
  - Page Options Dialog Box ............................................................... 550
  - Page Scaling Dialog Box .................................................................. 551
  - Print Setup Dialog Box .................................................................... 552
  - Printing to a Form or Label ............................................................. 554
  - Reset Printer Session to Defaults ...................................................... 554
  - Run a Trace (Printer Sessions) .......................................................... 555
  - Save Changes on Exit (Printer Sessions) ............................................ 556
  - Printing IBM Host Terminal Screens ................................................ 557
- Printing from VT Sessions ................................................................. 559
11 Creating and Using Macros

Run a Macro ......................................................... 871
Create a Macro in the Visual Basic Editor ......................... 873
Record a Macro ......................................................... 874
Edit a Macro ........................................................... 874
Run a Startup Macro .................................................. 875
Set up Macros that run before or after a host connection ....... 876
Naming Macros ......................................................... 877
Recording Complete Dialog Box ..................................... 878
Using Legacy Macros ................................................ 878
Welcome to InfoConnect 2014, a full-featured desktop application that allows you to run host applications, transfer files, and integrate host data into the latest Windows and Office software applications. You can start multiple terminal sessions and even Web pages in a single workspace the same way you'd open multiple documents in most applications.

With InfoConnect providing terminal emulation, you can use your PC to connect to:

- An IBM mainframe as a 3270 terminal or 3287 printer, using Telnet or Telnet Extended (TN3270/E).
- An AS/400 or iSeries midrange computer as a 5250 terminal or 3812 printer, using Telnet (TN5250/E).
- A UNIX or Open VMS host, using a variety of connection methods.

**NOTE:** Depending on the version of InfoConnect you have installed, the details of your license agreement, and the security settings applied by your system administrator, some connection types and features described in this Guide may not be available to you.

If you've previously used Reflection or EXTRA! for product emulation, you'll find many new features in InfoConnect 2014. These features combine the best emulation features of Reflection and EXTRA! into a single solution, optimized for Microsoft Windows 7, Windows 8, and Microsoft Office.

Following is a summary of the many new and enhanced user interface, productivity, management, and security features you'll find in InfoConnect.

**User Interface**

You can choose from four types of user experiences: Ribbon, Browser, Classic, or TouchUx. The InfoConnect Ribbon has the look and feel of Windows 7 and Microsoft Office, including integrated search and theme support. The InfoConnect Browser has a look and feel similar to the latest Web browsers where screen real estate is maximized. The Classic interface is similar to the legacy Attachmate InfoConnect and EXTRA! X-treme terminal emulation applications. And the TouchUx interface provides a touchscreen user experience with an iOS, Android or Windows 8 look and feel.

The Ribbon, Browser, and TouchUx interfaces provide a multiple document interface, in which you can open multiple sessions. These interfaces also allow you to view and interact with Web pages within the InfoConnect workspace.

**Productivity Tools**

Tightly integrated with Microsoft Office, InfoConnect supports productivity features such as Recent Typing, Scratch Pad, Auto Complete, Auto Expand, Spell Check, and Screen History to drive user efficiency. If Microsoft Office 2007 or later is installed, you can leverage host data in e-mail messages, contacts, appointments, notes, tasks, and word-processing documents.
Management
You can create and distribute customized 3270, 5250, and VT session documents that include host specifications, or add Web pages to your workspace or layout. Session documents include pointers to mouse maps, keyboard maps, theme files, hotspot files, and Ribbons that you can use to customize the behavior of the session. You can further customize each session by adding macros, scripts, executables, and other options to context menus.

You can connect to hosts that use IP version 6 (IPv6) addresses. And, you can specify a backup host to which InfoConnect automatically connects in case of connection failure or interruption.

License metering for InfoConnect 2014 is available through the optional InfoConnect Security Gateway and its administrative console.

Security Services
InfoConnect provides the following security features for determining who can access and use sensitive host data.

- **User Account Control (UAC) for Installation** — Build Microsoft Installer (.msi) packages and lock down features.
- **Online Certificate Revocation** — When making secure connections, check the authenticity of certificates using Online Certificate Status Protocol (OCSP), a faster alternative to checking Certificate Trust Lists (CTL).
- **Trusted Locations** — Prevent security problems by allowing users to open documents only from trusted locations that you specify in the Trust Center.
- **Expanded Information Privacy Support** — Protect credit/debit card primary account numbers or other sensitive data that is entered or stored on host screens or in productivity features, such as Screen History.

To reinforce mainframe security, you can add a layer of protection in front of the host with secure token authorization, using the optional InfoConnect Security Gateway.

Automation and Developer Support
Using the InfoConnect object-oriented API model, add functionality to terminal sessions and Web pages using .NET API, Visual Basic for Applications (VBA), or HLLAPI programming. You can also create and run VBA scripts using functions provided by the VBA development environment. Documentation for the .NET API and VBA are provided from the Help button on the workspace frame.

Layout files give you the ability to access the InfoConnect .NET API in multiple instances of InfoConnect simultaneously. API security settings allow you to control access to the application through API or macro calls.

The SmartUx feature allows you to add functionality to IBM host applications. With SmartUx, you can highlight required fields and add buttons, date pickers, drop-down lists, and other controls to your sessions.

Legacy Support
InfoConnect 2014 protects the investment you've made in previous products.

You can run sessions you created in EXTRA!, KEA!, IBM Personal Communications, and Micro Focus RUMBA.

You can also still run and edit the macros and scripts you created in legacy Reflection and EXTRA!, including encrypted EXTRA! macros. And InfoConnect supports most types of macros created in Micro Focus RUMBA, OpenText HostExplorer, IBM PComm, and Brandon Systems/Jolly Giant QWS3270.

For a complete list of new features, see the InfoConnect 2014 Release Notes (http://support.attachmate.com/techdocs/2699.html).
Related Topics

- “The User Interface” on page 65
- “Productivity Tools” on page 190
- “Protecting Data and Information Privacy” on page 328
What's New?

InfoConnect 2014 includes two major new features:

- **TouchUx** allows InfoConnect to be configured for touchscreen user experiences. You can choose between Apple iOS, Android, or Windows 8 "skins." For iOS or Android devices, you must access InfoConnect through a Citrix XenApp server, with the Citrix Receiver client software installed on the device. InfoConnect only supports versions of Citrix software that Citrix currently supports.

- **SmartUx** allows you to modernize your legacy host applications with current-day application functionality. Developers can leverage a new set of programming interfaces to highlight fields and overlay controls, such as drop-down lists, buttons, and date-pickers on your legacy IBM host applications to make users more productive.

**TouchUx (Available for All Host Types)**

The TouchUx feature enables you to improve usability of terminal sessions on tablets and other mobile devices:

- A split pane window provides access to the same menu commands available on the ribbon and browser interfaces.
- An on-screen keyboard provides access to common host keys that are typically unavailable with standard tablet on-screen keyboards and can be configured for language, varying levels of transparency, and other properties.
- A gallery of open sessions allows you to switch sessions or quickly open recent sessions.

You can navigate with touch gestures, just as you do on other tablet applications. (Some of your device's gestures may not be supported on iPads or Android tablets.)

**SmartUx (Available for IBM 3270 and 5250 Terminals)**

The SmartUx feature enables you to modernize the host application user experience for easier, more productive use. With Reflection’s VBA or .NET API, you can:

- Highlight required fields and add tool tips to fields to help your users get over the difficult spots in your application.
- Replace old-style numbered option lists with more modern drop-down selection lists.
- Replace manual date entry with a graphical calendar date-picker.
- Add buttons to the host application's interface and program them to start macros or perform other actions.
Index Term
Primary: tech notes

You can find additional information about InfoConnect in the Attachmate Technical Note library (http://support.attachmate.com/techdocs).
3 Installation

You can install Reflection from a downloaded distribution, an administrative installation image, or from a CD. If you are an administrator looking for instructions on how to create a customized installer, see the Administrator’s Reference.

NOTE: Reflection is typically distributed electronically. If your installation requires a CD, you will need to request it when you place your order.

In this Chapter

- “System Requirements” on page 19
- “Upgrading from Previous Versions” on page 20
- “Install Reflection on a Workstation” on page 22
- “Features Selection Tab” on page 23
- “Set Your User Data Directory” on page 24
- “Advanced Tab” on page 24

System Requirements

Index Term
Primary: Vista

Index Term
Primary: system requirements

Index Term
Primary: supported platforms

Index Term
Primary: software requirements

Index Term
Primary: requirements

Index Term
Primary: platform support

Index Term
Primary: Office tools
Secondary: system requirements

Index Term
Primary: Microsoft
Secondary: Vista

Index Term
Primary: hardware requirements
Specific requirements for Attachmate InfoConnect 2014 vary based on your hardware and other software components present.

**NOTE:** Attachmate cannot confirm the accuracy of performance, or any other claims related to non-Attachmate products. For questions or concerns regarding the capabilities of non-Attachmate products, please contact the suppliers of those products.

### Processor
2 GHz, 32-bit or 64-bit (1.5 GHz or higher multi-core, 32-bit or 64-bit recommended)

### System memory (RAM)
1 GB (2 GB recommended)

### Recommended operating system and platform support
One of the following:

- Microsoft Windows 7 Enterprise 32-bit and 64-bit
- Microsoft Windows 7 Ultimate 32-bit and 64-bit
- Microsoft Windows Vista Enterprise, SP1 32-bit and 64-bit
- Microsoft Windows Vista Ultimate, SP1 32-bit and 64-bit
- Microsoft Windows 8.1 Pro, 32-bit and 64-bit
- Microsoft Windows Server 2003 R2 with Windows Terminal Server (for multi-user environments) 32-bit and 64-bit
- Microsoft Windows Server 2008 R1 or R2 with Windows Terminal Server (for multi-user environments) 32-bit and 64-bit for R1 (64-bit only for R2)
- Microsoft Windows Server 2012 R1 or R2 with Remote Desktop Services (for multi-user environments)

**NOTE:** For information about deploying InfoConnect in virtualized environments and other supported platforms, see Technical Note 2698: Reflection 2014 Supported Platforms (http://support.attachmate.com/techdocs/2698.html).

### Additional software requirements
Microsoft Office 2007 or later must be installed to use the Office integration features in InfoConnect.

### Related Topics
- "Install Reflection on a Workstation" on page 22
- "Features Selection Tab" on page 23
- "Upgrading from Previous Versions" on page 20

### Upgrading from Previous Versions
When you install InfoConnect 2014, it upgrades the following Attachmate products:

- Reflection for UNIX and OpenVMS 2008 and 2011
- Reflection for IBM v. 8.0 - 14.x
- Reflection for UNIX and OpenVMS v. 8.0 - 14.x
- Reflection for the Multi-Host Enterprise, Standard Edition v. 8.0 - 14.x
- EXTRA! X-treme v. 8.0 - 9.x
- myEXTRA! Enterprise v. 7.0
- myEXTRA! v. 7.x
- EXTRA! Enterprise 2000

**NOTE:** Reflection 2007, 2008, and 2011 are automatically removed when you upgrade. EXTRA! and the other Reflection products are automatically removed when you upgrade using setup.exe. If you upgrade these products by deploying the .msi file directly, you will get a message telling you to uninstall the older software first.

For detailed information about upgrading, see Technical Note 2702 (http://support.attachmate.com/techdocs/2702.html).

**Supported Reflection Configuration Files**

InfoConnect 2014 represents an upgrade over previous versions of both Reflection and EXTRA!. Most configuration files used with these products are supported by the new version.

For a complete list of legacy Reflection and EXTRA! files supported by InfoConnect 2014, see Technical Note 2193 (http://support.attachmate.com/techdocs/2193.html).

**Related Topics**

- “System Requirements” on page 19
- “Install Reflection on a Workstation” on page 22

**Install Reflection on a Workstation**

**Index Term**
- Primary: VPA numbers

**Index Term**
- Primary: personalizing, See also customizing

**Index Term**
- Primary: installation
  - Secondary: workstation

**Index Term**
- Primary: installation
  - Secondary: basic

**Index Term**
- Primary: workstation install

**NOTE:** You must log on with administrator privileges to install Reflection. If you do not have the necessary access rights, ask your system administrator to elevate your privileges.
To install on a workstation

1. Run the Attachmate Installation Program.

   If you install from                      Do This
   A download site                         Click the download link, and then run the download program. Select a location for the installer files, and then click Next. This extracts the files to the specified location and starts the Attachmate Installation Program.

   An administrative installation image   From the administrative installation point, double-click the setup.exe file.

2. From the Attachmate Installation Program, click Continue, and then accept a license.

3. (Optional) To change the default installation folder, click the File Location tab and browse to the folder in which you want to install Reflection.

4. (Optional) To select which features, components, or languages are installed, click the Feature Selection tab.

5. Click Install Now.

**NOTE:** Use the Advanced tab of the installer only if you want to modify the installer log settings, or if you are an administrator configuring a Reflection deployment. An administrative installation does not actually install the product — instead, it creates an installation image that administrators can use to customize and deploy Reflection to end users.

### Features Selection Tab

- **Index Term**
  - Primary: language
  - Secondary: installing

- **Index Term**
  - Primary: advertising
  - Secondary: feature installation

- **Index Term**
  - Primary: installation
  - Secondary: languages

- **Index Term**
  - Primary: Feature Selection tab

Use the Feature Selection tab to select which features you want to install.

Click the icon to the left of the feature name and select from the options below.
Set Your User Data Directory

You can specify any location as the user data directory. The default directory is My Documents (or Documents)\Attachmate\Reflection. The directory you specify will be added as a Trusted Location.

To set the user data directory

1. Run the Attachmate Installation Program as shown in “Install Reflection on a Workstation” on page 22.
2. On the Attachmate Installation Program, click File Location, and then under Default user data directory, browse to the directory you want to use.

**NOTE:** This change only affects those features that you include in your initial installation. If you add a feature later using Programs and Features (or Add/Remove Programs), that application will use the original default directory (Documents\Attachmate\Reflection), not the value you specified for Default user data directory.

Advanced Tab

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>🔄 Feature will be installed on local hard drive</td>
<td>Installs the selected feature. <strong>NOTE:</strong> Some features listed under a selected feature may not be included when you select to install the higher-level feature. The features that are included are the recommended defaults. If you select the higher level feature a second time, all sub-features will be included.</td>
</tr>
<tr>
<td>🔄 Feature will be installed when required</td>
<td>Installs the feature when you first use it (for example, when you click the Start menu shortcut for this feature).</td>
</tr>
<tr>
<td>❌ Feature will be unavailable</td>
<td>Leaves the feature uninstalled.</td>
</tr>
</tbody>
</table>

Index Term
Primary: Advanced tab (installer)

Index Term
Primary: administrative installation
Secondary: Advanced tab (installer)

Use the Advanced tab of the installer only if you want to modify the installer log settings or you are an administrator configuring a Reflection deployment.
**Install to this PC**

Installs Reflection to your computer.

**Create an Administrative install image on a server**

*NOTE:* An A2D unwrapped a broken link to: admin_install_image_pr in an excluded topic. Administrative install image does not actually install the product — instead, it creates an installation image that administrators can use to deploy Reflection to end users.

When you create an administrative install image, an image of Reflection is copied to a network location for later installation to multiple workstations. This network location can be used by deployment tools to access and create packages that are deployed to workstations. Also, end users can perform installations by running setup.exe from this location.

**Log file settings**

By default, an installation log file is created and then deleted after installation successfully completes. (This configuration avoids accumulation of large log files after successful installations.) To save a log file for all installations, including successful ones, select Create a log file for this installation, and clear Delete log file if install succeeds.

The installation log file, which provides details about the installation, is saved in the user's Windows temporary folder (%tmp%) with a generated name that begins with atm. To open this directory, launch the Start menu Run command and enter %tmp%. 
In this Chapter

- “Add a Button that Opens a Session Document” on page 28
- “Add Controls to the Ribbon” on page 28
- “Add a Keyboard Shortcut That Sends Special Character Data (VT)” on page 34
- “Configure Host Connection Options” on page 35
- “Configure Color Settings” on page 35
- “Configure non-FTP File Transfer” on page 36
- “Configure Workspace Arrangement” on page 37
- “Copy and Paste Host Data” on page 39
- “Create a Custom Context Menu” on page 40
- “Create a New Theme File” on page 41
- “Customize Microsoft Office Productivity Features” on page 42
- “Customize the Quick Access Toolbar” on page 42
- “Create or Modify a Layout” on page 43
- “Define Hot Spots” on page 45
- “Edit the Translation Table” on page 46
- “Edit or Move a Button on the Quick Access Toolbar” on page 47
- “Import Legacy VT Toolbars to the Ribbon” on page 47
- “Map a Sound to an Event” on page 48
- “Minimize the Ribbon” on page 49
- “Modify Existing Controls on the Ribbon” on page 49
- “Move Controls on the Ribbon” on page 50
- “Open a Layout” on page 51
- “Print More Than One Screen per Page” on page 52
- “Remove Controls from the Ribbon” on page 52
- “Restore the Default Ribbon” on page 53
- “Run Legacy Sessions” on page 53
- “Select a Cursor Style” on page 54
- “Select and Mark Text on a Terminal Screen” on page 54
- “Select the Interface Type (Ribbon, Browser, Classic, or TouchUx)” on page 56
- “Set Tab Colors” on page 56
- “Set Up a Default Windows Printer” on page 57
- “Start a Session From a Command Line” on page 58
- “Switch Between Tabs and Windows” on page 58
- “Switch to Windows Full Screen mode” on page 59
Add a Button that Opens a Session Document

You can add a button to the Quick Access Toolbar (QAT) that opens a session document. (You can also map this action to a Ribbon button or a keyboard shortcut.)

To add a QAT button that opens a session document

1. From the Quick Access Toolbar, select to add an action.

2. In the Add an Action dialog box, select Open Document.

3. Browse to the session document file you want to open when the button is clicked.

Add Controls to the Ribbon

With the UI Designer, you can add tabs, groups, buttons, and menus to the Ribbon. You can implement most tasks as a button control, a menu item, or as a combination of the two.

Button groups have the most flexibility of all controls because they can include both buttons and menus. If you need more space for controls, you may want to create a new tab, and add groups to it. A group is a structure to which you can add buttons, button groups, and menus.

To access the UI Designer, select the Appearance ribbon, and then, from the Menus group, click the UI Designer button.
To | Insert this type of control
---|---
Perform a single task or action | Button (page 29)
Run a macro | Button (page 76)
Add a group of three buttons | Button group (page 32)
Perform an action and open a menu | Split button (page 78)
Add a menu of options, thumbnails, or commands | Gallery (page 78)
Open a dialog box from a group | Dialog launcher (page 33)
Create a container to which you can add other controls, such as buttons, button groups, and split buttons | Group (page 32)
Create a new category on the Ribbon for custom controls | Tab (page 34)

NOTE: The UI Designer is just one way to create controls — the Context Menu Editor, Keyboard Mapper, Mouse Mapper, and Hotspots provide other ways for you to run favorite macros and actions.

Add a Button

Index Term
Primary: controls
Secondary: buttons

Index Term
Primary: button
Secondary: adding to UI

Index Term
Primary: actions
Secondary: creating buttons for

Use the Button control to add a button that performs a single task or action.

To add a button

1. On the Appearance tab, click UI Designer.
2. From the Design View pane, from the Ribbon simulation, select the tab and group to which you want to add the control.
   To select a group, click the group name. Create a new group, if needed.
3. From the Insert Controls pane, click Button.
4. From the Settings pane, set the action and other properties for the new button that appears on the Ribbon.
5. Click OK.

Related Topics
- “Add a Button to Run a Macro” on page 76
- “Add a Group” on page 32
Add a Button to Run a Macro

With the UI Designer, you can add a button or other control that runs a macro or a macro-related action to the Ribbon. All supported macros, including RCL scripts and legacy macro editors, are available as actions. Legacy compatibility features must be installed for these options to appear in the Actions list. For more information, see the InfoConnect Administrator's Reference.

NOTE: The UI Designer is just one way to create controls — the Context Menu Editor, Keyboard Mapper, Mouse Mapper, and Hotspots provide other ways for you to run favorite macros and actions.

To add a button that runs a macro-related action

1. On the Appearance tab, click UI Designer.
2. From the Design View pane, from the Ribbon simulation, select the tab and group to which you want to add the control.
   - To select a group, click the group name. Create a new group, if needed.
3. From the Insert Controls pane, click Button.
4. From the Settings pane, click the Select Action button.
5. From the Action category menu, choose Macro.
6. Select an action from the Action list.
   - If you selected an action that runs a macro, select the appropriate options:
     - Select a macro (or open a file that contains macros) each time you click the button
     - Specify a macro that runs automatically each time you click the button

7. From the Settings pane, set the properties for the new button that appears on the Ribbon.
8. Click OK.
9. If prompted, type a new filename for the custom ribbon and then save the file.
   - The button is saved to a custom ribbon file that you can use in other session documents.

Related Topics

- “Select Action Dialog Box” on page 161
- “Creating and Using Macros” on page 871
- “Add Controls to the Ribbon” on page 28
Add a Button with an Action and a Menu

A split button includes a functional button and a menu. Split buttons look like galleries except that they perform an action in addition to opening a menu. For an example of a split button, see the Screen History control — when clicked, the button opens an option pane and the menu shows a history of recorded screens.

To add a split button

1. On the Appearance tab, click UI Designer.
2. From the Design View pane, from the Ribbon simulation, select the tab and group to which you want to add the control.
   To select a group, click the group name. Create a new group, if needed.
3. From the Insert Controls pane, click Split Button.
4. From the Subitems Collection Editor dialog box, click Add, and then select Button.
5. Repeat the previous step to add as many buttons as you want to appear in the menu.
6. With a button selected in the list, set the action and other properties.
7. When you have finished adding and configuring buttons, click OK.
   The Subitems Collection Editor dialog box closes.
8. From the Settings pane, set the action and other properties for the new split button that appears on the Ribbon.
9. Click OK.

Related Topics

- “Subitems Collection Editor Dialog Box (UI Designer)” on page 87
- “Select Action Dialog Box” on page 161
- “Add Controls to the Ribbon” on page 28

Add a Menu that Holds Buttons

Use the Gallery control to add a menu of options to the Ribbon.

NOTE: To add a button that performs an action in addition to opening a menu, use the Split Button control.

To add a gallery

1. On the Appearance tab, click UI Designer.
2. From the Design View pane, from the Ribbon simulation, select the tab and group to which you want to add the control.
   To select a group, click the group name. Create a new group, if needed.
3. From the Insert Controls pane, click Gallery.
4. From the Subitems Collection Editor dialog box, click Add, and then select Button.
5. Repeat the previous step to add as many buttons as you want to appear in the menu.
6. With a button selected in the list, set the action and other properties.
7. When you have finished adding and configuring buttons, click OK.
The **Subitems Collection Editor** dialog box closes.

8 Specify the appearance of the gallery by doing one of the following:
   - Select **Change settings**, and then type the label, tooltip, and description you want.
   - or-
   - Click **Select Action**, and then select an action from which to use the label, tooltip, and description.

9 Click **OK**.

**Related Topics**

- “Add a Button with an Action and a Menu” on page 78
- “Subitems Collection Editor Dialog Box (UI Designer)” on page 87
- “Select Action Dialog Box” on page 161
- “Add Controls to the Ribbon” on page 28

**Add a Group**

**Index Term**

Primary: controls
Secondary: group

A group provides a container for controls on the Ribbon. For an example of a group, see **Host** or **Clipboard** on the **Session** ribbon.

**To add a group**

1 On the **Appearance** tab, click **UI Designer**.
2 From the **Design View** pane, from the Ribbon simulation, select the tab to which you want to add a new group of controls.
3 From the **Insert Controls** pane, click **Group**.
4 Enter a label for the group name.
5 Add controls to the group by clicking them in the **Insert Controls** pane.
6 Specify control settings, and then click **OK** to save your changes.

**Related Topics**

- “Add a Dialog Launcher to a Group” on page 33
- “Add Controls to the Ribbon” on page 28

**Add a Group of Buttons**

**Index Term**

Primary: button
Secondary: group

You can stack up to three controls — buttons, split buttons, and galleries — in a button group. For an example of a button group on the Ribbon, see the **Host** group on the **Session** ribbon: Connect, Disconnect, and Quick Keys are combined in a single button group.
To add a button group

1. On the **Appearance** tab, click **UI Designer**.
2. From the **Design View** pane, from the Ribbon simulation, select the tab and group to which you want to add the control.
   
   To select a group, click the group name. Create a new group, if needed.
3. From the **Insert Controls** pane, click **Button Group**.
4. From the **Subitems Collection Editor** dialog box, click **Add** and then select the item you want.
5. Repeat the previous step to add additional buttons, split buttons, or galleries (up to three items total).
6. With a button, split button, or gallery selected in the list, set the action and other properties.
   When you have finished adding and configuring items to the group, click **OK** to close the **Subitems Collection Editor** dialog box.
7. Click **OK**.

**Related Topics**

- “Subitems Collection Editor Dialog Box (UI Designer)” on page 87
- “Select Action Dialog Box” on page 161
- “Add Controls to the Ribbon” on page 28

### Add a Dialog Launcher to a Group

**Index Term**

Primary: dialog launcher

**Index Term**

Primary: controls
Secondary: dialog launcher

Groups can include a dialog launcher control in the lower-right corner. This control typically opens settings or performs other tasks relevant to the group.

To add a dialog launcher

1. On the **Appearance** tab, click **UI Designer**.
2. Do one of the following:
   - Create a new group by clicking **Group** in the **Insert Controls** pane.
   - or-
   - Select an existing group from the **Design View** by clicking the group name.
3. With the group selected, from the **Settings** pane, select **Show dialog launcher button** to enable the settings.
4. From the **Settings** pane, to set the action and other properties for the new dialog launcher that appears on the Ribbon, click **Select Action**.
5. Click **OK**.

**Related Topics**

- “Add a Group” on page 32
Add a Tab

Index Term
Primary: tabs
Secondary: adding to UI

Index Term
Primary: controls
Secondary: tab

Add a new tab to create a new category on the Ribbon for custom controls.

To add a tab

1. On the Appearance tab, click UI Designer.
2. In the Insert Controls pane, click Tab.
3. In the Settings pane, type a name for the tab in the Label box.
4. Click OK.

Related Topics

- “Add Controls to the Ribbon” on page 28

Add a Keyboard Shortcut That Sends Special Character Data (VT)

You can add an action that sends special characters to the host and then map it to a keyboard shortcut, a button, or another control.

To add a keyboard shortcut that sends special character data to the host

1. Open the Document Settings dialog box.
   The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ribbon or Reflection Browser</td>
<td>With a session open in Reflection, from the Quick Access Toolbar, click</td>
</tr>
<tr>
<td>TouchUx</td>
<td>Tap the Gear icon and then select Document Settings.</td>
</tr>
</tbody>
</table>

2. Select Manage Keyboard Map.
3. In the Keyboard map dialog box, select Modify the currently selected keyboard map file.
4. Press the key combination you want to map (for example, CTRL+Q).
5. Click Select Action and then select the Send Text action.
6. In the Select a special character list, choose the character data to send.
NOTE: If the Select a special character list doesn't have the character data you want to send, you can type in the string for the character data in the Text to send to host field. For example, type in `<ESC>`. Alternatively, you can hold down the ALT key and use the numeric keypad to enter the numeric code for the data. For example, to send `<ESC>`, enter 027.

Configure Host Connection Options

You can specify whether to automatically connect to the host when a session document is opened. You can also specify whether to reconnect to a host after disconnections occur that are not initiated from InfoConnect.

To set up Host connection options

1. Open the Document Settings dialog box.
   The steps depend on your user interface mode (page 120).

   User Interface Mode  Steps
   Ribbon or Reflection Browser  With a session open in Reflection, from the Quick Access Toolbar, click.
   TouchUx  Tap the Gear icon and then select Document Settings.

2. Under Host Connection, click Configure Connection Settings.
3. Under Host Connection Options (or Connection Options if you are using VT), specify how to connect and what to do when a connection is terminated:
   * To set up the session to establish a host connection as soon as the associated session document is opened, select Automatically connect to the host.
   * To specify whether to reconnect after any disconnection that is not initiated from InfoConnect, select an option in the When connection is terminated list.

Configure Color Settings

Index Term
Primary: color
Secondary: changing for the workspace

You can change the colors for the application frame and Ribbon or for the session.

To change the color of the application frame and Ribbon

1. Open the InfoConnect Workspace Settings dialog box.
   The steps depend on your user interface mode (page 120).
2 Under Workspace Settings, click **Configure User Interface**.
3 From the **Look and Feel / Color scheme** box, select the color scheme.

**To change the colors used in a terminal session**

1 Open the Document Settings dialog box.
   The steps depend on your **user interface mode** (page 120)]

2 Under **Terminal Appearance**, click **Manage Themes**.
3 Click **Select another theme file**.
4 Select a theme with the colors and sounds you prefer.
5 Click **OK**.

**Related Topics**

- “Configure Workspace Defaults Dialog Box” on page 125
- “Manage Themes Dialog Box” on page 132
- “Modify Theme Dialog Box (3270 Terminal Sessions)” on page 133
- “Modify Theme Dialog Box (5250 Terminal Sessions)” on page 136
- “Modify Theme Dialog Box (VT Terminal Sessions)” on page 139
- “Configure Workspace Arrangement” on page 37

## Configure non-FTP File Transfer

You can manually configure file transfer settings in the Transfer Settings dialog box. Any configuration you perform is saved with your session document.

However, using an automated preset configuration is recommended.

**To configure file transfer**

1 Open a terminal session.
2 Open the Transfer Settings dialog box.
   The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ribbon</td>
<td>On the Session ribbon, from the Transfer group, click the Transfer Settings launcher.</td>
</tr>
<tr>
<td>Reflection Browser</td>
<td>On the Reflection menu, choose Tools and then File Transfer. In the Transfer dialog box, click the Settings button.</td>
</tr>
<tr>
<td>TouchUx</td>
<td>Tap the Wrench icon and then under Tools, select File Transfer. In the Transfer dialog box, click the Settings button.</td>
</tr>
</tbody>
</table>

3 Configure the file transfer settings.
4 For most situations, you can configure for file transfers by selecting a preset configuration in the Protocol tab (For example, AS/400).

Configure Workspace Arrangement

Index Term
- Primary: workspace
- Secondary: expanding

Index Term
- Primary: window
- Secondary: tiling horizontal or vertical

Index Term
- Primary: window
- Secondary: cascading

Index Term
- Primary: window
- Secondary: arrangement

Index Term
- Primary: view options

Index Term
- Primary: tiling windows

Index Term
- Primary: tabs
- Secondary: arrange documents with

Index Term
- Primary: hiding the Ribbon

Index Term
- Primary: full screen mode

Index Term
- Primary: expanding the workspace
InfoConnect provides a variety of ways to customize the appearance of the workspace.

- Documents in the workspace are displayed in tabs by default. If you are using the InfoConnect Ribbon, you can choose to display them in windows that can be tiled or cascaded.
- You can enlarge the document window by using Full Screen mode or by hiding the Ribbon.

To choose tabs or windows

1. Open the InfoConnect Workspace Setting dialogs box. The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ribbon (Office 2007)</td>
<td>On the Reflection button <img src="image" alt="Reflection" />, choose <strong>Reflection Workspace Settings</strong>.</td>
</tr>
<tr>
<td>Ribbon (Office 2010)</td>
<td>On the File menu, choose <strong>Reflection Workspace Settings</strong>.</td>
</tr>
<tr>
<td>Reflection Browser</td>
<td>On the Reflection menu, choose <strong>Settings</strong> and then <strong>Reflection Workspace Settings</strong>.</td>
</tr>
<tr>
<td>TouchUx</td>
<td>Tap the Gear icon and then select <strong>Reflection Workspace Settings</strong>.</td>
</tr>
</tbody>
</table>

2. Under Workspace Settings, click **Configure User Interface**.
3. In the **Arrange documents as** box, select **Tabs** or **Windows**.
4. (Optional) If you have multiple windows open, you can arrange them as tiled or cascading windows, using the **Arrange Windows** menu, which is next to the **Full Screen** button in the status bar. You can also use this menu to switch the display between tabs and windows.

To enlarge the document window

- Do any of the following:

<table>
<thead>
<tr>
<th>To</th>
<th>Do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expand the workspace to fill the entire screen and hide the Ribbon</td>
<td>Click the <strong>Full Screen</strong> button from the status bar; click it again to return the workspace to its normal size and show the Ribbon.</td>
</tr>
<tr>
<td>Hide the Ribbon without expanding the workspace</td>
<td>Double-click any tab on the Ribbon; double-click again to show the Ribbon.</td>
</tr>
<tr>
<td>Expand the workspace to fill the entire screen without hiding the Ribbon</td>
<td>Double-click the workspace frame in the empty area to the right of the <strong>Quick Access</strong> toolbar; double-click again to return the workspace to its normal size.</td>
</tr>
</tbody>
</table>
Copy and Paste Host Data

Index Term
Primary: copying
Secondary: host data

You can copy entire host screens or selected data to the clipboard, then print the data, paste it to other host screens, Microsoft Office products installed on your computer, or other types of files.

To send host screens or data directly to Microsoft Office products, see “Integrate Host Data with Office Tools” on page 192.

To copy selected data from the current screen to other locations

1. Navigate to the host data you want to copy.
2. Select specific data to copy, then press CTRL+C.

**NOTE:** You can select a word in a field by double-clicking the word or select all of the words in a field by triple-clicking the field.

3. Navigate to the location where you want to paste the data. This can be on the same host screen, another host screen, or even in another application.

4. Press CTRL+V.

Copy data in a tabular format

You can copy data from the screen and paste it into an application that accepts tabular data (for example, a spreadsheet). By default, table columns are set by analyzing vertical space alignment. Optionally, you can configure InfoConnect so that columns are set by replacing multiple spaces or tabs with a single tab. (See Configure Clipboard Settings (page 167).)

To copy data from the current screen to a spreadsheet

1. Select the host data to copy.
2. Copy the data as follows:
   - The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ribbon</td>
<td>On the Sessionribbon <strong>Clipboard</strong> group, click the <strong>Copy</strong> drop-down menu and then select <strong>Copy Table</strong>.</td>
</tr>
<tr>
<td><strong>InfoConnect</strong> Browser</td>
<td>On the <strong>InfoConnect</strong> menu, choose <strong>Edit</strong> and then <strong>Copy Table</strong>.</td>
</tr>
</tbody>
</table>

3. Open the spreadsheet and press CTRL+V.
To copy host screens from Screen History to another location

1 Open the Screen History task pane.
   The steps depend on your user interface mode (page 120).

   User Interface Mode          Steps
   Ribbon                       On the Session ribbon, click the Screen History button.
   Reflection Browser          On the Reflection menu, choose View and then Screen History.
   TouchUx                      Tap the Wrench icon and then under View, select Screen History.

2 Select the screen that you want to copy.
   NOTE: Only text areas of the host screen are included in the recorded image; host graphics images are not included.

3 From the toolbar in the Screen History task pane, click the Copy button.
4 Choose Copy as Text or Copy as Bitmap.
5 Navigate to the location where you want to paste the host screen. This would typically be a file in another application (word-processing, e-mail, and so on).
6 Press CTRL+V.

Related Topics
- “Integrate Host Data with Office Tools” on page 192
- “Configure Clipboard Settings Dialog Box (3270 and 5250)” on page 165
- “Clear the Clipboard on Close” on page 155

Create a Custom Context Menu

You can create custom context menus for legacy hot lists or for other types of frequently used commands. After you create a custom context menu, you can map a mouse action to open the new menu.

1 Open the Context Menu Editor.
   The steps depend on your user interface mode (page 120).

   User Interface Mode          Steps
   Ribbon                       Click the Appearance tab and in the Menus group, select Context Menu.
   Reflection Browser          On the Reflection menu, choose View and then choose Context Menu.
   TouchUx                      Tap the Wrench icon and then under View, select Context Menu.

2 At the top of the Context Menu dialog box, click Add and enter the name of your context menu.
3 Add the menu items and separators for your new menu.
4 Under **Menu Item** settings, enter the label and select an action for each item.
5 Click **OK** to save the new menu.

Next, you'll want to make a right-click open the new custom context menu instead of the default.

1 **Open the Mouse Mapper dialog box.**
   
   The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ribbon</td>
<td>On the <strong>Tools</strong> tab, click <strong>Mouse Mapper</strong>.</td>
</tr>
<tr>
<td>Reflection Browser</td>
<td>On the <strong>Reflection</strong> menu, choose <strong>Tools</strong>, and then <strong>Mouse Mapper</strong>.</td>
</tr>
<tr>
<td>TouchUx</td>
<td>Tap the Gear icon and then select <strong>Document Settings</strong>. Under <strong>Input Devices</strong>, click <strong>Manage Mouse Map</strong>. Then choose whether to modify the current mouse map or create a new map.</td>
</tr>
</tbody>
</table>

2 Under **Mouse Mapper**, for **Key Combination**, select **Right** and then click **Modify**.
3 From the list of actions, select **Show Specific Context Menu**.
4 On the right, from the **Context Menu**, choose the name of the new custom context menu.

## Create a New Theme File

**Index Term**
Primary: themes
Secondary: new

**Index Term**
Primary: new
Secondary: theme

**To create a theme file**

1 **Open the Document Settings dialog box.**
   
   The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ribbon or Reflection Browser</td>
<td>With a session open in <strong>Reflection</strong>, from the Quick Access Toolbar, click ➕.</td>
</tr>
<tr>
<td>TouchUx</td>
<td>Tap the Gear icon and then select Document Settings.</td>
</tr>
</tbody>
</table>

2 Under **Terminal Appearance**, click **Manage Themes**.
3 Click **Create a new theme from an existing theme file** and then select the theme file to use as a template for creating a new theme file.
In the Modify Theme dialog box, select the settings for the theme file and then save the file.

**Customize Microsoft Office Productivity Features**

To customize productivity features

Open the Document Settings dialog box.

The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ribbon or Reflection Browser</td>
<td>With a session open in Reflection, from the Quick Access Toolbar, click.</td>
</tr>
<tr>
<td>TouchUX</td>
<td>Tap the Gear icon and then select Document Settings.</td>
</tr>
</tbody>
</table>

Select To

Productivity defaults Configure whether Recent Typing, Auto Complete, Auto Expand, and Spell Check are enabled by default.

Screen History Set the maximum screens to capture, whether to capture manually only, and whether to clear screen history when disconnected.

Office tools Specify PowerPoint presentation and Word templates.

NOTE: If you specify templates, you will need to deploy the template files.

Recent Typing Set the number of words to remember and whether to clear the list when disconnected.

Auto Complete Configure Suggestions and whether to overwrite or insert suggestions.

Auto Expand Set definitions for abbreviations you want to expand.

Spell Checking Specify a custom dictionary and other options.

**Customize the Quick Access Toolbar**

The Quick Access Toolbar contains a set of controls that you can use to perform common tasks and access document settings. It is located at the top of the InfoConnect window.
The Quick Access Toolbar

You can add button controls to the Quick Access Toolbar from the Ribbon interface or from the workspace menu. You can also add custom button controls that you have created.

**NOTE:** You can add only simple button controls to the Quick Access Toolbar. You cannot add complex buttons or other interface items.

**To add or remove Quick Access Toolbar buttons**

With a session open, add or remove Quick Access Toolbar button controls as follows:

<table>
<thead>
<tr>
<th>To</th>
<th>Do this...</th>
</tr>
</thead>
</table>
| Add a button control from the workspace menu. | 1. Open the InfoConnect Workspace menu.  
2. On the menu, right click on the button control you want to add, and then select Add to Quick Access Toolbar. |
| Add a button control from the Ribbon | On the InfoConnect Ribbon, right click on the button control you want to add, and then select Add to Quick Access Toolbar. |
| Add a custom button control | 1. Click the Quick Access Toolbar menu, and then select Add an Action.  
2. In the Select Action Dialog box, under Action, select an action and then specify action parameters (if required). |
| Remove a button control | On the Quick Access Toolbar, right-click the button control you want to remove and then select Remove from Quick Access Toolbar. |

The Quick Access Toolbar button controls that you add are automatically saved in your workspace file and are displayed the next time you open InfoConnect.

**Related Topics**

- “The User Interface” on page 65
- “Minimize the Ribbon” on page 49

**Create or Modify a Layout**

**Index Term**
Primary: workspace  
Secondary: saving

**Index Term**
Primary: sessions  
Secondary: opening multiple

**Index Term**
Primary: saving  
Secondary: layouts
In **InfoConnect**, the size, location, and arrangement of the workspace and any open terminal or Web session documents can be saved to a layout file. When opened, a layout automatically opens and arranges all documents saved to the layout, opens and positions any docked panes (such as Scratch Pad or Screen History), and connects session documents to configured hosts.

If the workspace is configured to display documents as tabs, you can create a name for each tab. This can be useful when you use two different applications on one host. You can create a session document that connects to that host, then open the document twice, add a different name to each tab, and then save your layout.

In addition, by using layout files, you can access the **InfoConnect** .NET API in multiple instances of **InfoConnect** simultaneously.

**NOTE:** If you already have terminal session or Web session documents open when you open a layout, the layout opens in a new workspace.

By saving terminal sessions you use regularly to a layout, you can open them all at once, arranged as you prefer, just by opening the layout.

**To create a layout**

1. Open the documents and any docked panes you want to include in the layout.
2. (Optional) To access multiple layouts using the **InfoConnect** .NET API, enter the necessary API settings as follows:

2a. **Open the Layout Settings dialog box.**
   The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ribbon (Office 2007)</td>
<td>On the Reflection button <img src="reflection.png" alt="Reflection Button" />, choose <strong>Settings</strong>, and then <strong>Layout Settings</strong>.</td>
</tr>
<tr>
<td>Ribbon (Office 2010)</td>
<td>On the <strong>File</strong> menu, choose <strong>Settings</strong>, and then <strong>Layout Settings</strong>.</td>
</tr>
<tr>
<td><strong>InfoConnect</strong> Browser</td>
<td>On the <strong>InfoConnect</strong> menu, choose <strong>Settings</strong> and then <strong>Layout Settings</strong>.</td>
</tr>
<tr>
<td><strong>touchUx</strong></td>
<td>Tap the Gear icon and then select <strong>Layout Settings</strong>.</td>
</tr>
</tbody>
</table>

2b. Enter the appropriate values for the server and channel name.
3 (Optional) If the workspace is configured to display documents as tabs, you can add a descriptive label to each document tab:

3a Right-click the session tab, and then choose Tab Properties.
3b In the Name box, type in the name that you want to appear on the tab, and then click OK.

4 Adjust the size and position of the workspace, as needed.

5 Save the layout.

The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Office 2007</td>
<td>On the Reflection button, choose Save Layout.</td>
</tr>
<tr>
<td>Microsoft Office 2010</td>
<td>On the File menu, choose Save Layout.</td>
</tr>
<tr>
<td>Reflection Browser</td>
<td>On the Reflection menu, choose Save Layout.</td>
</tr>
<tr>
<td>TouchUx</td>
<td>Tap the Folder icon and then select Save Layout.</td>
</tr>
</tbody>
</table>

6 Name and save the layout file to a trusted location, and then click Save.

If you haven’t saved the session documents, you are prompted to do so.

To modify a saved layout

- To save changes to a layout, save it again using the same name.

  
  NOTE: InfoConnect doesn't prompt you to save changes to a layout.

Related Topics

- “Open a Layout” on page 51
- “Tab Properties Dialog Box” on page 73
- “Layout Settings Dialog Box” on page 72

Define Hot Spots

Hotspots are virtual buttons that appear over text in terminal sessions. By using hotspots, you can control your terminal session with the mouse instead of the keyboard. Typically, clicking a hotspot transmits a terminal key or command to the host, but you can also configure hotspots to open a Web page, launch a macro, or perform a variety of other actions.

To create and configure a customized hotspots file

1 Open the Document Settings dialog box.

The steps depend on your user interface mode (page 120).
2 Under **Terminal Appearance**, click **Manage Hotspots**.

3 Click **Create a new hotspots file from an existing hotspots file**.

4 In the **Create a New Hotspots File** dialog box, select the type of hotspots file (built-in, Custom, or the new file for the current session) to use as a template for creating a new hotspots file.

5 In the Modify Hotspots dialog box, under **Hotspot text** enter the text for the hotspot.

6 Under **Select an action to map to the hotspot**, select an action to map to and configure the action.

7 When prompted, save the new hotspot file.

8 On the **Quick Access Toolbar**, click the **Save** button to save the session.

The session is automatically configured to point to the new hotspot file.

### Edit the Translation Table

Using the Translation Tables dialog box, you can:

- Edit the tables **InfoConnect** uses to translate the PC’s character set into the character set used by the host and vice versa.
- Use currently unsupported character sets.
- Customize **InfoConnect** for unique host environments.

Use the translation tables when:

- You need to edit how characters are translated from the host to the PC, and vice versa. Typically, you’ll use the tables to support a host character set that’s currently unavailable in **InfoConnect**. The characters in the table are hexadecimal.
  
  - or -

- You need to edit how EBCDIC characters are translated from the host to the PC, and vice versa for a Unisys T27 host. These translations are done in addition to the normal PC-to-host and host-to-PC translations performed by **InfoConnect**. The characters in the table are hexadecimal.

**NOTE:** To use the translation tables, the `DataStreamTranslation` VBA property must be set to `true` (the default is `false`). When **InfoConnect** is emulating a Unisys T27 host, the `DataStreamTranslation` property is automatically set to `true`.

### To open the Translation Tables dialog box

1 Launch a **InfoConnect** VT session.

2 From the Tools ribbon, select **Visual Basic**.

3 In the VBA editor, right-click on **Project Legacy** and choose **Insert** and then **Module**.

4 Copy and paste the following VBA code into the code window:
Sub Translation()

    With Session
        .DataStreamTranslation = True
        .ExecuteBuiltInFunction "TranslationTables"
    End With
End Sub

5 Close the VBA editor.

6 On the Tools ribbon, click Run Macro.

7 In the Run Macro dialog box, select Legacy Reflection Macro in This File.

8 Run the Translation Macro.

        The Translation Tables editor is displayed.

Edit or Move a Button on the Quick Access Toolbar

You can change the action that a button on the Quick Access Toolbar (QAT) is associated with. You can also move the button to change its position on the toolbar.

To edit a QAT button

    1 On the QAT, right click on the button you want to edit and select Modify.
    2 In the Select Action dialog box, select the action you want to associate with the button and click OK.

To move a QAT button

        • On the QAT, drag the button to the position you want to move it to.

Import Legacy VT Toolbars to the Ribbon

You can use the UI Designer to import legacy VT toolbars to the [InfoConnect] Ribbon. In Ribbon mode, you can import legacy VT toolbars from any legacy VT session file (*.r2w or *.r4w) or toolbar file (*.rtb) to the currently selected VT session. Once imported, the toolbars appear as buttons on the Ribbon.

NOTE: Importing legacy VT toolbar behavior depends on the user interface mode. The InfoConnect Classic user interface mode automatically imports toolbars for legacy VT sessions. However, when you open a legacy VT session in the Ribbon user interface mode, the session’s toolbars are not automatically imported.

In Ribbon Mode, Import Legacy VT Toolbars

    1 Open the VT session you want to import the toolbars from and select the session in the workspace.
    2 Right click the Ribbon and then select Customize the Ribbon.
    3 In the Ribbon UI Designer, in the Insert Controls group, click Import.
    4 From the Open dialog box, select the legacy VT session file or the toolbar file you want to import.
UI Designer displays all visible toolbars in the **Convert Legacy Toolbars** panel:

5 Select the Ribbon group you want to import the toolbars to. You can select an existing group or you can add a new tab and a new group.

6 To use small buttons that are grouped vertically in rows of three, select **Use small buttons**.

7 Select the toolbars you want to import and then click **Convert**.

The imported buttons are added to the Ribbon group.

If you checked the “Use small buttons” box, buttons are grouped vertically as follows:

8 Click **OK** and save the .map file.

## Map a Sound to an Event

**Index Term**

Primary: sounds  
Secondary: mapping to events

**Index Term**

Primary: mapping  
Secondary: sounds to events

**Index Term**

Primary: events  
Secondary: mapping sounds to

You can configure InfoConnect to play a sound when a session-level event occurs. This mapping is saved as a modification to your theme.

**To map a sound to an event**

1 Open the Document Settings dialog box.

   The steps depend on your **user interface mode** (page 120).
In the Settings dialog box, click Manage Themes.

Click Modify the currently selected theme file.

From the Modify Theme dialog box, under Sounds, select an item in the Events list.

Select a sound file to map to the selected event. (You can type the path and filename or click Browse to locate the file.)

**Related Topics**

- “Modify Theme Dialog Box (3270 Terminal Sessions)” on page 133
- “Modify Theme Dialog Box (5250 Terminal Sessions)” on page 136
- “Modify Theme Dialog Box (VT Terminal Sessions)” on page 139
- “Manage Themes Dialog Box” on page 132
- “Create a New Theme File” on page 41

### Minimize the Ribbon

You can minimize the Ribbon to provide more working area in the InfoConnect window.

**To minimize the Ribbon**

1. Click the Quick Access Toolbar menu button.

2. In the menu list, choose Minimize the Ribbon.

**NOTE:** You can restore the Ribbon by clicking the Quick Access Toolbar menu button and then choosing Maximize the Ribbon.

If you are using a default 3270 or 5250 keyboard map, you can press CTRL+F1 to permanently minimize or restore the Ribbon.

**Related Topics**

- “The User Interface” on page 65
- “Customize the Quick Access Toolbar” on page 42

### Modify Existing Controls on the Ribbon

You can change built-in controls or custom controls.
To modify an existing control

1. On the **Appearance** tab, click **UI Designer**.
2. In the **Design View** pane, from the Ribbon simulation, select the control that you want to modify.

   **NOTE:** To select a button group, click the bottom edge of the group, or, select one of its buttons, and then, under **Arrange Controls**, click **Select Parent**. To select a group, click the group name.

3. In the **Settings** pane, make your changes.
4. Click **OK**.

**Related Topics**

- “Move Controls on the Ribbon” on page 50
- “Select Action Dialog Box” on page 161
- “Subitems Collection Editor Dialog Box (UI Designer)” on page 87
- “Add Controls to the Ribbon” on page 28
- “Remove Controls from the Ribbon” on page 52

## Move Controls on the Ribbon

**Index Term**

- **Primary:** controls
- **Secondary:** rearranging

**Index Term**

- **Primary:** arrange
- **Secondary:** controls

From the **UI Designer**, you can reorganize or simplify your workspace by selecting a new location for the controls.

### To move a control within its parent control

- To move a control to a new location within its parent control (for example, to move a button within a group, or to move a group on a tab), use the **Move** buttons from the **Arrange Controls** pane in the **UI Designer**.

You can move a control from one group to a different group, move a group from one tab to a different tab, or delete a control from its current location and add it to the new location.

### To move a control outside its parent control

1. From the **Design View** pane, select the control that you want to move.
2. Write down the settings that appear in the **Settings** pane.
3. From the **Arrange Controls** pane, click **Delete**.
4. Select the tab and group where you want to place the control, or add a new tab and group.
5. From the **Insert Controls** pane:
<table>
<thead>
<tr>
<th>To insert</th>
<th>Do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>A Tab, Group, or Button</td>
<td>Click the control.</td>
</tr>
<tr>
<td>A Gallery, Split Button, or Button Group</td>
<td>Click the control, then from the Subitems Collector Editor dialog box, add subitems to the control, and then click OK.</td>
</tr>
<tr>
<td>A Built-In</td>
<td>Click the control, then from the Built-In Controls dialog box, choose a pre-defined gallery or group, and then click Insert.</td>
</tr>
</tbody>
</table>

6. Change the properties for the control in the Settings pane to match the settings you wrote down before you deleted the control from its original location.

7. Click OK.

Related Topics
- “Built-In Controls Dialog Box (UI Designer)” on page 88
- “Subitems Collection Editor Dialog Box (UI Designer)” on page 87

### Open a Layout

**Index Term**
- Primary: opening
- Secondary: layout

**Index Term**
- Primary: layouts
- Secondary: starting InfoConnect from

By saving terminal sessions you use regularly to a layout, you can open them all at once, arranged as you prefer, just by opening the layout.

**NOTE:** If you already have terminal session or Web session documents open when you open a layout, the layout opens in a new workspace.

#### To open a layout

1. Go to the Open dialog box.
   - The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ribbon or Reflection Browser</td>
<td>From the Quick Access Toolbar, click the Open button.</td>
</tr>
<tr>
<td>TouchUx</td>
<td>Tap the Folder icon and then select Open.</td>
</tr>
</tbody>
</table>

2. Select the layout file you want, and then click Open.

Layout files created in InfoConnect end with the extension .rwsp.

**Related Topics**
- “Open a Terminal Session” on page 148
Print More Than One Screen per Page

You can set up printing to send multiple screen prints to a spool file and then print them all at once. You also have the option of inserting a form feed between the screen prints or letting Reflection fill each page with the maximum amount of text (regardless of where one screen ends and the next begins).

To configure Reflection to print more than one screen per page

1 Open the Print dialog box.
   The steps depend on your user interface mode (page 120).
   • If you are using the Ribbon or Browser mode, click on the Quick Access Toolbar.
   • If you are using the TouchUx mode, tap the Folder icon and then under Print, select Print.
2 In the Print dialog box, click Setup.
3 At the bottom of the Print Setup dialog box, in the Multiple screens per page box, select Close printer manually.
4 (Optional) If you want Reflection to add a form feed between each screen print, select Auto formfeed.
5 For each screen you want to print, go to the screen, and then on the “Workspace Menu” on page 891, choose Print.
   After you print the first screen, the Close Printer button appears on the status bar.
6 When you are done printing, click Close Printer.

NOTE: Each screen print you send to the printer is spooled to a file until you click Close Printer.

Remove Controls from the Ribbon

Index Term
Primary: workspace
Secondary: simplify

Index Term
Primary: user interface
Secondary: simplify

Index Term
Primary: Ribbon
Secondary: simplify

Index Term
Primary: removing
Secondary: controls from the ribbon
To remove a control

1. With a session open in InfoConnect, select the Appearance tab.
2. From the Menus group, click the UI Designer button to open the UI Designer.
3. From the Design View pane of UI Designer, select the control you want to delete.
4. In the Arrange Controls pane, click Delete.
5. To view your changes before saving them, in the Review pane, click Preview.
6. Click OK.

Restore the Default Ribbon

You can reverse any changes you've made to the Ribbon in the UI Designer by selecting the default ribbon.

1. With a session open in InfoConnect, from the Quick Access Toolbar, click 🔄.
2. Under User Interface, click Manage Ribbon.
3. Click Select another Ribbon file.
4. Click Built-in and select a Ribbon from the list that best matches your session document; for example, for a 3270 session document, select Reflection 2014 Ribbon UI for 3270 Sessions.
5. Click OK.
6. To save the session document, on the Quick Access Toolbar, click 🔄.

   The session will use the Ribbon you selected until you select a different Ribbon.

Run Legacy Sessions

You can run the following types of legacy sessions on InfoConnect 2014:

- EXTRA!
- IBM Personal Communications
- Micro Focus RUMBA
- KEA!

To run a legacy session, you will need to install the compatibility feature that supports its session files. You will need administrative rights to install this feature.

To install a compatibility feature

1. Open the Attachmate Installation Program (setup.exe) from your administrative installation point or from the Control Panel.
2 On the Feature Selection tab, select **Reflection Workspace** and then **Emulation**.
3 Under **3270/5250** or **UNIX > and OpenVMS**, select **Compatibility**.
4 Choose the compatibility feature for your legacy product and then install the feature.

## Select a Cursor Style

Index Term  
Primary: cursor  
Secondary: select style

You can set the cursor style and save it as a modification to your theme.

**To select a cursor style**

1 **Open the Document Settings dialog box.**
   
   The steps depend on your [user interface mode](#page_120) (page 120).  

   **User Interface Mode**  
   
   **Ribbon or Reflection Browser**  
   With a session open in Reflection, from the [Quick Access Toolbar](#), click .

   **TouchUx**  
   Tap the Gear icon and then select [Document Settings](#).

2 **In the Settings dialog box, click Manage Themes.**
3 **Select Modify the currently selected theme file.**
4 **In the Modify Theme dialog box, under [Cursor Style](#), change the cursor settings and click OK.**

**Related Topics**

- “Modify Theme Dialog Box (3270 Terminal Sessions)” on page 133
- “Modify Theme Dialog Box (5250 Terminal Sessions)” on page 136
- “Modify Theme Dialog Box (VT Terminal Sessions)” on page 139
- “Manage Themes Dialog Box” on page 132
- “Create a New Theme File” on page 41

## Select and Mark Text on a Terminal Screen

Index Term  
Primary: text  
Secondary: selecting

Index Term  
Primary: selecting text

Index Term  
Primary: marking text

**InfoConnect** provides two different styles for selecting and marking text on the terminal screen, using either your keyboard or your mouse.
You can select and mark any rectangular area on the screen, or you can select and mark contiguous lines on the screen. You can also set the default behavior for your terminal sessions.

To set the default for selecting text on VT sessions

1. Open the Document Settings dialog box.
   The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ribbon or Reflection Browser</td>
<td>With a session open in Reflection, from the Quick Access Toolbar, click</td>
</tr>
<tr>
<td>TouchUx</td>
<td>Tap the Gear icon and then select Document Settings.</td>
</tr>
</tbody>
</table>

2. In the Settings dialog box, select Configure Terminal Settings.
3. In the Terminal Setup dialog box, select the Keyboard & Mouse tab.
4. To set text selection so that selected text forms a rectangle (instead of wrapping), select Rectangular selection.

To set the default for selecting text on IBM sessions

1. Open the Document Settings dialog box.
   The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ribbon or Reflection Browser</td>
<td>With a session open in Reflection, from the Quick Access Toolbar, click</td>
</tr>
<tr>
<td>TouchUx</td>
<td>Tap the Gear icon and then select Document Settings.</td>
</tr>
</tbody>
</table>

2. In the Settings dialog box, select Configure Terminal Settings.
3. To set text selection so that selected text forms a rectangle (instead of wrapping), select Rectangular selection (mouse).

To select text using the non-default behavior

- (IBM only) When using the mouse, to use the non-default behavior, hold down the CTRL key while dragging the mouse.
- (VT and IBM) When using a keyboard, to change the default behavior, select the Screen Selection (Keyboard) action in the Keyboard Mapper, and then choose either Rectangular Block or Contiguous Lines.

Related Topics

- “Specifying a Custom Keyboard Map” on page 177
- “Select Action Dialog Box” on page 161
- “Use a Keyboard to Interact with InfoConnect” on page 61
Select the Interface Type (Ribbon, Browser, Classic, or TouchUx)

You can choose from several user interface modes:
- Ribbon shares the look and feel of Microsoft Windows 7 and Office 2010.
- Browser has a look and feel that is similar to the latest Web browsers.
- Classic is similar to the legacy Attachmate InfoConnect and EXTRA! X-treme terminal emulation applications.
- TouchUx provides a touchscreen user experience.

To select the interface type
1. Open the InfoConnect Workspace Settings dialog box. The steps depend on your user interface mode (page 120).
2. Click Configure User Interface.
3. In the User interface mode list, select the type of interface you want to use.
4. To select a look and feel for the Ribbon or TouchUx interface modes, choose from the options in the Look and Feel / Color Scheme list.
5. Close and reopen the workspace.

Set Tab Colors

When you are running multiple sessions, color-coding session tabs can help identify which host application each session is connected to.

You can customize the text and background colors of a session tab. After you set the tab colors for your sessions, you can save them in a layout file so that the tab colors are used the next time you open the layout.

NOTE
- You can save session tab color settings only in layout files. These settings are not saved in session files.
- You can change only one tab at a time. You cannot globally change all tab colors.
To set tab background and text colors

You can set different colors for a session tab’s text and background. You can also set different colors for active and inactive states.

1. On the Session tab, right-click and then select **Customize Tab Colors** to open the Customize Tab Colors dialog box.
2. To set inactive tab colors, in the Inactive tab colors list, click **Change** and then select the foreground (text) color or background color.
3. Set the Active tab colors in the same way.
4. **Save the color settings in a layout.**

   The steps depend on your user interface mode (page 120).

   **User Interface Mode** | **Steps**
   --- | ---
   Microsoft Office 2007 | On the Reflection button , choose **Save Layout**.
   Microsoft Office 2010 | On the File menu, choose **Save Layout**.
   Reflection Browser | On the Reflection menu, choose **Save Layout**.
   TouchUx | Tap the Folder icon and then select **Save Layout**.

**TIP:** If you want to set only the tab background color, you can use an alternative approach. With a session open, click the Appearance tab and from the Color menu, choose a color. Then click on the session tab to set its background color. (The selected color is used as the tab’s background, for both active and inactive states.)

---

**Set Up a Default Windows Printer**

You can specify which Windows printer to use for the session.

To set up printing

1. **Open the Document Settings dialog box.**
   
   The steps depend on your user interface mode (page 120).

   **User Interface Mode** | **Steps**
   --- | ---
   Ribbon or Reflection Browser | With a session open in Reflection, from the Quick Access Toolbar, click .
   TouchUx | Tap the Gear icon and then select **Document Settings**.

2. Under Printer Settings, select **Configure Printer Settings**.
3. On the Print Setup dialog box, select the printer to use.
Start a Session From a Command Line

You can launch an InfoConnect session from a command line. You can also use command line options to specify InfoConnect startup behavior and appearance. These options override the workspace settings.

To start a session

- On a Windows command prompt, enter the following commands:

  "Attachmate.Emulation.Frame.exe" -f "<sessionPath><sessionName>"

InfoConnect Command Line Options

Options are case insensitive and are preceded by either a dash (-) or forward slash (/).

- **f**
  Open document (.rdox, .rd3x, .rd5x) or layout (.rwsp)

- **n**
  Suppress Reflection splash screen

- **uimode{classic|ribbon|browser|touch}**
  Set user interface mode

- **?, -help**
  Display this help topic

For example:

The following command opens mysession.rd3x in Browser mode with the splash screen suppressed:

```
Attachmate.Emulation.Frame.exe -f
"C:\Users\myUserName\Documents\Attachmate\Reflection\mysession.rd3x" -uimode browser -N
```

Switch Between Tabs and Windows

If you are using the InfoConnect Ribbon interface and have more than one session document open in a workspace, you can quickly change whether documents are displayed in tabs or in windows.

To quickly switch between a tabbed or windows display

- On the right side of the status bar, click the Arrange Windows menu and choose whether to display documents in tabs or in cascading or tiled windows.
Switch to Windows Full Screen mode

The Windows Full Screen Look and feel displays the workspace without the standard Windows title bar that includes the minimize, maximize, and close buttons. This Look and feel is available only in the TouchUX User interface mode.

To switch to Windows Full Screen Mode

1. Open the InfoConnect Workspace Settings dialog box. The steps depend on your user interface mode (page 120).

   **User Interface Mode** | **Steps**
   └───────────────────|───────────────────────────────────────────────────────────────────────────────────────────────────
   Reflection Browser  | On the Reflection menu, choose Settings and then Reflection Workspace Settings.
   TouchUX             | Tap the Gear icon and then select Reflection Workspace Settings.

2. Click Configure User Interface to open the User Interface dialog box.
3. In the User interface mode list, select TouchUX.
4. In the Look and Feel/ Color scheme list, select Windows Full Screen.
5. Restart the workspace to apply the changes.

Stop Showing the Create New Document Dialog Box

By default, the Create New Document dialog box is displayed when you open the InfoConnect workspace.

To stop showing the Create New Document dialog box

1. Open the InfoConnect Workspace Settings dialog box. The steps depend on your user interface mode (page 120).
### Turn off Screen History, Office Tools, and Productivity Features for Specific Fields

You can turn off Screen History, Office Tools, and productivity features for fields that contain sensitive information (like user accounts) by setting Field Security for these fields.

When Field Security is on for a field, Screen History, Office Tools, and all of the productivity features are disabled for that field. These features still work for other fields where Field Security is off. Field Security settings are saved when you save your session files.

**To Turn Field Security On**

- In the program field you want to set, right-click and choose Field Security.

**To Turn Field Security Off**

- In a program field that has Field Security set to On, right-click and choose Field Security.

### Undo a Cut or Paste

You can undo the latest cut or paste you make in an IBM terminal window.

**To undo a cut or paste**

On the InfoConnect Ribbon, click \(\text{undo}\).

**NOTE**

- When you undo a cut or paste, any data you have typed in since that cut or paste is removed.
- After you undo a cut or paste, you can choose to redo it by clicking \(\text{redo}\) again.
Underline Fields That Accept Input

For IBM 3270 and 5250 terminals, you can set InfoConnect to underline fields that accept input. You can choose to always underline these fields, to allow the host to control whether they should be underlined, or to never underline them.

To specify whether to underline fields that accept input

1. Open a 3270 or 5250 terminal session.
2. Open the Document Settings dialog box.
   - The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ribbon or Reflection Browser</td>
<td>With a session open in Reflection, from the Quick Access Toolbar, click</td>
</tr>
<tr>
<td>TouchUx</td>
<td>Tap the Gear icon and then select Document Settings.</td>
</tr>
</tbody>
</table>

3. Under Terminal Configuration, click Configure Terminal Attributes(3270) or Configure Terminal Settings(5250).
4. In the Input field underlining list, select whether to underline input fields.

Use a Keyboard to Interact with InfoConnect

Although it is more common to use a mouse to open dialog boxes, select documents, interact with the Ribbon, and to activate controls, InfoConnect also allows you to perform these actions using the keyboard.

By creating a custom keyboard map, you can assign a key or key combination to any task or control that you can access from the user interface. You can open a session, run a macro, create an e-mail message, or save a layout. You can also create a sequence of actions to perform with the stroke of a single key.

KeyTips provide another way to access to every command available on the Ribbon or the Quick Access toolbar. You can get to most commands with only two to four keystrokes, no matter where you are in InfoConnect.

When you press and release the ALT key, KeyTips are displayed over each feature that is available in the current view. At that point, you can press the letter shown in the KeyTip over the feature that you want to use.

Depending on which letter you pressed, you may be shown additional KeyTips. Continue pressing letters until you press the letter for the specific command or option that you want to use.
Other standard keyboard shortcuts are also supported. The following table includes common tasks you can perform with the keyboard:

<table>
<thead>
<tr>
<th>To</th>
<th>Press</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show or hide KeyTips</td>
<td>The ALT key.</td>
</tr>
<tr>
<td>Select or use a control on the Ribbon or the Quick Access toolbar</td>
<td>ALT, then the key associated with the KeyTip for that control.</td>
</tr>
<tr>
<td>Go to the next session document or Web page</td>
<td>CTRL+TAB.</td>
</tr>
<tr>
<td>Go to the previous session document or Web page</td>
<td>CTRL+SHIFT+TAB.</td>
</tr>
<tr>
<td>Go to the next pane in the current session document</td>
<td>CTRL+1.</td>
</tr>
<tr>
<td>Move between items in a dialog box</td>
<td>TAB and the ARROW keys.</td>
</tr>
<tr>
<td></td>
<td>-or-</td>
</tr>
<tr>
<td></td>
<td>ALT + the accelerator key (underlined letter) for that item.</td>
</tr>
</tbody>
</table>

Related Topics

- “Quick Keys” on page 156
- “Productivity Tools” on page 190
- “Specifying a Custom Keyboard Map” on page 177
- “Select and Mark Text on a Terminal Screen” on page 54

Use Customized Host Files

InfoConnect supports legacy Reflection custom host files. These files are used to specify the host names displayed in the Host name/IP address list in the Settings dialog box.

The path to the customized host file is specified in the value for the HKCU\Software\WRQReflection\Rwin\Global registry setting. This registry setting is only installed in legacy versions of Reflection. It is not part of the InfoConnect installation.

If the value of this setting is "" (the default) or if the setting is not in the registry, all of the names in the system local host file are displayed in the Host name/IP address list.

**NOTE:** Windows can resolve the host names in the custom host files only if these names are valid domain names or names that are in the local hosts file. Custom host files are not used by Windows to resolve IP addresses.

Host file format

The custom host file must have the following format:

```
<IPv4 or IPv6 address> <host name>
```

For Example:

```
127.0.0.1 localhost
:: localhost
```
The host name information is used to populate the Host name/IP address list in the Settings dialog box.

The IP address information is not relevant unless the specified host file also happens to be the Windows system hosts file.

Using the Clipboard (3270 and 5250)

In 3270 and 5250 sessions, the Clipboard has a few features that are only available from the InfoConnect menu: Paste Next, Cut and Append, Copy and Append.

Use Paste Next when you have more data in the Clipboard than will fit in a field, and you want to paste the remaining data into another field. Where the Paste command would start at the beginning of the data in the Clipboard, Paste Next starts at the beginning of the remaining data (that is, the Clipboard contents minus what was pasted in the previous field). Consecutive uses of Paste Next gradually empty the Clipboard.

To paste data into multiple fields

1 With data in the Clipboard, place the cursor in the first target field.

2 Select Paste.
   The steps depend on your user interface mode (page 120).

   **User Interface Mode** |  **Steps**
   --- | ---
   Ribbon | From the Clipboard group on the Session ribbon, click Paste.
   InfoConnect Browser | From the Reflection menu, choose Edit and then choose Paste.
   TouchUX | Tap the folder icon and then choose Paste.

3 Move the cursor to the next target field.
4 From the Ribbon Paste button menu (or the InfoConnect Browser Edit menu), click Paste Next.
5 (Optional) Repeat steps 2 and 3 as necessary.

Use Cut and Append or Copy and Append when you want to add to the Clipboard contents instead of replacing the Clipboard contents.
To append data to the Clipboard contents

1 Select the data you want to add to the Clipboard.

**NOTE:** You can select a word in a field by double-clicking the word or select all of the words in a field by triple-clicking the field.

2 From the Ribbon Cut or Copy buttons (or the InfoConnect Browser Edit menu), choose Cut and Append or Copy and Append.

Related Topics

- “Copy and Paste Host Data” on page 39
- “Select and Mark Text on a Terminal Screen” on page 54
- “Clear the Clipboard on Close” on page 155
- “Configure Clipboard Settings Dialog Box (3270 and 5250)” on page 165
With InfoConnect 2014, you can display sessions in four types of user interface modes: Ribbon, Browser, TouchUX, and Classic.
To select the interface type

1. Open the Reflection Workspace Settings dialog box. The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reflection Browser</td>
<td>On the Reflection menu, choose Settings and then Reflection Workspace Settings.</td>
</tr>
<tr>
<td>TouchUx</td>
<td>Tap the Gear icon and then select Reflection Workspace Settings.</td>
</tr>
</tbody>
</table>

2. Click Configure User Interface to open the User Interface dialog box.

3. In the User interface mode list, select the type of interface that you want to use.

4. To select a look and feel for the Ribbon or TouchUx interfaces, choose from the options in the Look and Feel / Color scheme list.

5. Close and reopen the workspace.

The Ribbon

The Ribbon interface shares the look and feel of Microsoft Windows 7 and Office 2010. In the area between the Quick Access toolbar (the toolbar in the upper-left corner) and the document window is the Ribbon, a dynamic, collapsible device that organizes commands, buttons, and other controls on tabs for each task area. Double-click any tab in the Ribbon to hide or show the Ribbon. Or, if you prefer, you can map a keyboard shortcut to show or hide the Ribbon with a keystroke. Sessions using the default 3270 or 5250 keyboard map already have this action mapped to CTRL+F1.

The Browser

The Browser interface has a look and feel that is similar to the latest Web browsers. You can access commands from the InfoConnect menu or from the Quick Access Toolbar. You can also access commands by searching for them in the search box and then clicking on the search results.
The **TouchUx** interface provides the **InfoConnect TouchUx** user experience. **InfoConnect** runs on Microsoft Windows devices or other devices (Apple iPad or Android) that are accessing sessions running on a Citrix server. This mode includes an on-screen terminal keyboard that can be set as a transparent overlay or docked in a separate pane.

### Classic

A Classic interface option provides an interface that is familiar to users of previous versions of **InfoConnect**. This mode is recommended only if you are upgrading from a previous version. When using the Classic UI, only one document can be open in a workspace, and other features may not be available.

### Workspace and Layouts

Most of your work in **InfoConnect** will be done in the application frame, which is called the workspace.

You can configure your workspace with several different types of "look and feel" settings that provide different ways to access the workspace menu, which contains layout options, application and document settings, and a list of recent documents.

The Steps to open your workspace settings dialog box depend on your User Interface Mode.

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ribbon (Office 2007)</td>
<td>On the Reflection button , choose <strong>Reflection Workspace Settings</strong>.</td>
</tr>
<tr>
<td>Ribbon (Office 2010)</td>
<td>On the <strong>File</strong> menu, choose <strong>Reflection Workspace Settings</strong>.</td>
</tr>
<tr>
<td><strong>InfoConnect</strong> Browser</td>
<td>On the <strong>InfoConnect</strong> menu, choose <strong>Settings</strong> and then <strong>Reflection Workspace Settings</strong>.</td>
</tr>
<tr>
<td><strong>TouchUx</strong></td>
<td>Tap the Gear icon and then select <strong>Reflection Workspace Settings</strong>.</td>
</tr>
</tbody>
</table>

The workspace incorporates these elements:

- **Quick Access toolbar**
  - From this toolbar, located in the upper-left corner, you can perform common tasks and access document settings.

- **Search**
  - Search the current document, or use the associated drop-down menu to search all open documents, screen history, your desktop, the **InfoConnect** Help system, or the Web.
  - From other locations in the product, you can also search settings pages, the Help system, or the Attachmate Support site.
  - When using the **InfoConnect** Browser, you can also search for commands (for example, Trace), and then choose a command from the search results. (In other words, you can use the search results like a menu.)
The size and location of the workspace, along with all open terminal sessions, Web pages, and task panes, is referred to as the layout. You can save the settings of a layout to a file. When reopened, a layout file automatically opens the saved documents and repositions the workspace to the specified size and location.

Documents

A document is a file that specifies the settings and behavior of a terminal session, a Web page, a printer session, or an FTP client session.

When you open a document, the related session or Web page is opened, either in the workspace (for terminal sessions and Web pages) or in a separate window (for printer sessions and FTP client sessions).

The document for a terminal session contains configuration settings for host-specific information. It also includes pointers to other files that are used to control the appearance of the session, such as the theme file, and to files that control input and text handling, such as the keyboard map file and the Ribbon file.

You can open any number of terminal sessions or Web pages in the workspace. The document name appears on the tab label unless a different name has been specified in a layout. The name of the selected document appears in the title bar of the workspace.

Appearance

You can control the appearance of documents in the workspace using themes, which combine color specifications for text and backgrounds, cursor types, and sounds for session-level events.
You can also select a color scheme for the workspace and ribbon background and sounds for workspace events.

In this Chapter

- “Using the Browser” on page 69
- “Configuring InfoConnect” on page 70
- “Using Layouts” on page 72
- “Customize the Ribbon” on page 74
- “The User Interface” on page 120
- “Create New Document Dialog Box” on page 122
- “Change the UI Language” on page 123
- “InfoConnect Workspace Settings Dialog Box” on page 124
- “Configure Workspace Defaults Dialog Box” on page 125
- “Configure Workspace Attributes Dialog Box” on page 128
- “Configure User Interface Dialog Box” on page 129
- “Manage On-Screen Keyboard Settings” on page 131
- “Manage Themes Dialog Box” on page 132
- “Select a Theme File Dialog Box” on page 133
- “Modify Theme Dialog Box (3270 Terminal Sessions)” on page 133
- “Modify Theme Dialog Box (5250 Terminal Sessions)” on page 136
- “Configure User Interface Dialog Box” on page 139
- “Manage QuickPads Dialog Box” on page 141
- “Workspace Settings Dialog Box” on page 143

Using the Browser

The Browser interface has a look and feel that is similar to the latest Web browsers. Although it requires less screen real estate than the Ribbon interface, it provides the same functionality as the Ribbon. It also provides additional ways to access commands and connect to hosts.

Accessing Commands

In much the same way that you access commands in the Ribbon interface, you can access commands through the InfoConnect menu or the Quick Access toolbar. The Browser also allows you to access commands by typing them into the search box. For example:

To access the Trace commands, enter \( \tau \) in the search box and then choose from the list of Trace commands.
Connecting to Hosts

Similar to the Ribbon, you can connect to a host automatically or from the InfoConnect menu. In addition, you can connect by entering the type of connection and the host name in the search box.

For example:

To open a telnet connection to a 3270 host named myMainFrame, enter `tn3270://myMainFrame`

**NOTE:** For IBM systems, you can open Telnet sessions for 3270 or 5250 terminals using the following format:

`tn3270://hostName`

`tn5250://hostName`

For Open Systems (VT) you can open Telnet, Secure Shell, or Rlogin sessions using the following format:

`telnet://hostName`

`ssh://hostName`

`rlogin://hostName`

---

**Configuring InfoConnect**

- Index Term
  - Primary: user interface
  - Secondary: User Account Control icon

- Index Term
  - Primary: user interface
  - Secondary: shield icon

- Index Term
  - Primary: User Account Control icon

- Index Term
  - Primary: shield icon

- Index Term
  - Primary: settings (InfoConnect)
  - Secondary: saving

- Index Term
  - Primary: settings (InfoConnect)
  - Secondary: global vs. session

- Index Term
  - Primary: settings (InfoConnect)
  - Secondary: disabled

- Index Term
  - Primary: saving
  - Secondary: settings

- Index Term
  - Primary: grayed-out settings
Index Term
Primary: disabled settings

Index Term
Primary: configuration files, See also session documents
Secondary: saving

Index Term
Primary: Change Currently Disabled Settings link

There are two types of configuration available in the InfoConnect workspace: session document and workspace configuration.

The document for a terminal session contains configuration settings for host-specific information. It also includes pointers to other files that are used to control the appearance of the session, such as the theme file, and to files that control input and text handling, such as the keyboard map file and the Ribbon file.

NOTE

- There are no document configuration settings for Web page documents.
- Printer sessions and FTP client sessions open in windows outside the InfoConnect workspace. They are configured from within those windows, instead of the workspace.

Workspace configuration settings affect all terminal session and Web page documents opened in InfoConnect. Workspace configuration settings include security, file locations, and other settings related to InfoConnect.

If any settings are unavailable, they may have been disabled by your administrator. If this is the case, on Vista and Windows 7 computers, the User Account Control icon appears in the upper left corner of the workspace.

Clicking the Change Currently Disabled Settings link next to this icon allows an administrator to enable settings.

When you navigate to multiple settings pages, all the settings on all the pages are saved when you click OK, or discarded when you click Cancel.

Related Topics

- “Terminal Sessions” on page 145
- “Session Documents and Related Files” on page 146
- “Open a Web Session” on page 315
- “Configure Workspace Arrangement” on page 37
- “Customize the Ribbon” on page 74
Using Layouts

Index Term
Primary: workspace
Secondary: RWSP files

In InfoConnect, the size, location, and arrangement of the workspace and any open terminal or Web session documents can be saved to a layout file. When opened, a layout automatically opens and arranges all documents saved to the layout, opens and positions any docked panes (such as Scratch Pad or Screen History), and connects session documents to configured hosts.

If the workspace is configured to display documents as tabs, you can create a name for each tab. This can be useful when you use two different applications on one host. You can create a session document that connects to that host, then open the document twice, add a different name to each tab, and then save your layout.

In addition, by using layout files, you can access the InfoConnect .NET API in multiple instances of InfoConnect simultaneously.

NOTE: If you already have terminal session or Web session documents open when you open a layout, the layout opens in a new workspace.

In this Section

- “Layout Settings Dialog Box” on page 72
- “Tab Properties Dialog Box” on page 73

Layout Settings Dialog Box

Index Term
Primary: layouts
Secondary: settings

Index Term
Primary: IPC Channel name

Index Term
Primary: automation server name

Index Term
Primary: API
Secondary: using IPC channels with

Getting there

The steps depend on your user interface mode (page 120).
By using layout files, you can access the InfoConnect .NET API in multiple instances of InfoConnect simultaneously. From this dialog box, define how to access the API in the instance of Reflection that starts when you open a layout file. (You must also enable the API in the Set Up API and Macro Security dialog box.)

NOTE: InfoConnect doesn't prompt you to save changes to a layout.

Set Up API

Automation server name Specify the name you'll use to access a particular InfoConnect instance. For example, you can specify this server name in VBA macros that use automation to get a running InfoConnect instance.

IPC channel name Specify a channel name. This setting overrides the IPC channel name specified in the Set Up API and Macro Security dialog box for the saved layout. In your custom application, use this name to access the API in the InfoConnect instance that starts when you open the layout file. (Use IPC must be selected in the Set Up API and Macro Security dialog box.)

Related Topics

- “Set Up API and Macro Security Dialog Box” on page 335
- “Using Layouts” on page 72
- “Create or Modify a Layout” on page 43

Tab Properties Dialog Box

Index Term
Primary: unique identifiers

Index Term
Primary: tabs
Secondary: Properties dialog box

Index Term
Primary: tabs
Secondary: labeling sessions

Index Term
Primary: sessions
Secondary: renaming tabs of
Getting there

1. Open a session document.
2. In the workspace, right-click the session document tab and choose Tab Properties.

Use this dialog box to add labels to tabbed documents saved with layouts. These labels appear on the tab in place of the actual filename when the document is viewed as part of a layout. This dialog box also provides a unique identifier for a document tab that you can reference in macros and scripts.

The location of the document tabs (top, bottom, left, or right) is selected on the Configure User Interface dialog box.

**NOTE:** Tab properties are lost if you close the associated document without saving a layout. These properties are used on the document tab only in the saved layout.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type a label to appear on the document tab in a saved layout. This text does not affect the filename of the document or the appearance of the tab when opening the document outside the layout.</td>
</tr>
<tr>
<td>Description</td>
<td>Type information relevant to the document or its use in the layout.</td>
</tr>
<tr>
<td>API tab identifier</td>
<td>Shows an alphanumeric identifier for the current instance of the tab. This number changes each time the document (tab) is opened. This read-only ID can be used to reference the tab through the API.</td>
</tr>
<tr>
<td>Document filename</td>
<td>Shows the full name, including the path, of the saved document file. The name of the document also appears in the title bar of the workspace. This value cannot be edited.</td>
</tr>
</tbody>
</table>

**Related Topics**
- “Create or Modify a Layout” on page 43
- “Configure Workspace Defaults Dialog Box” on page 125
- “Set Tab Colors” on page 56

**Customize the Ribbon**
In the area between the Quick Access Toolbar and the document window is the Ribbon, a dynamic, collapsible device that organizes commands, buttons, and other controls on tabs for each task area.

Whether you're a system administrator or user, you can customize the Ribbon interface to make InfoConnect more convenient to use. For example, since the Privacy Filters button affects the way data is handled by the productivity features, you could add it to the Productivity group on the Session tab.

Using the UI Designer, you determine which controls to include and what they do, from simple tasks to complex routines. In addition to creating new controls, you can modify existing controls, remove controls you don't use, or relocate controls to other tabs.

You can also use the InfoConnect VBA or .NET API to dynamically show or hide custom Ribbon controls, enable or disable the controls, and change the actions that are mapped to the controls. (See Dynamically Changing the User Interface in the VBA Guide or the .NET API Guide.)

In this Section

- “Add Controls to the Ribbon” on page 75
- “Remove Controls from the Ribbon” on page 81
- “Modify Existing Controls on the Ribbon” on page 81
- “Move Controls on the Ribbon” on page 82
- “Restore the Default Ribbon” on page 83
- “Manage Ribbon Dialog Box” on page 83
- “Select a Ribbon File Dialog Box” on page 84
- “UI Designer” on page 84
- “Create a New Ribbon File Dialog Box” on page 87
- “Subitems Collection Editor Dialog Box (UI Designer)” on page 87
- “Built-In Controls Dialog Box (UI Designer)” on page 88
- “Locking Down the User Interface” on page 89

Add Controls to the Ribbon

With the UI Designer, you can add tabs, groups, buttons, and menus to the Ribbon. You can implement most tasks as a button control, a menu item, or as a combination of the two.

Button groups have the most flexibility of all controls because they can include both buttons and menus. If you need more space for controls, you may want to create a new tab, and add groups to it. A group is a structure to which you can add buttons, button groups, and menus.
To access the UI Designer, select the Appearance ribbon, and then, from the Menus group, click the UI Designer button.

To insert a button

1. On the Appearance tab, click UI Designer.
2. From the Design View pane, from the Ribbon simulation, select the tab and group to which you want to add the control.
   To select a group, click the group name. Create a new group, if needed.
3. From the Insert Controls pane, click Button.
4. From the Settings pane, set the action and other properties for the new button that appears on the Ribbon.
5. Click OK.

**Related Topics**

- “Add a Button to Run a Macro” on page 76
- “Add a Group” on page 32
- “Select Action Dialog Box” on page 161
- “Add Controls to the Ribbon” on page 28

**Add a Button to Run a Macro**

**Index Term**
**Primary:** macros
**Secondary:** creating buttons for

NOTE: The UI Designer is just one way to create controls — the Context Menu Editor, Keyboard Mapper, Mouse Mapper, and Hotspots provide other ways for you to run favorite macros and actions.
With the UI Designer, you can add a button or other control that runs a macro or a macro-related action to the Ribbon. All supported macros, including RCL scripts and legacy macro editors, are available as actions. Legacy compatibility features must be installed for these options to appear in the Actions list. For more information, see the InfoConnect Administrator's Reference.

NOTE: The UI Designer is just one way to create controls — the Context Menu Editor, Keyboard Mapper, Mouse Mapper, and Hotspots provide other ways for you to run favorite macros and actions.

To add a button that runs a macro-related action

1. On the Appearance tab, click UI Designer.
2. From the Design View pane, from the Ribbon simulation, select the tab and group to which you want to add the control.
   To select a group, click the group name. Create a new group, if needed.
3. From the Insert Controls pane, click Button.
4. From the Settings pane, click the Select Action button.
5. From the Action category menu, choose Macro.
6. Select an action from the Action list.
   If you selected an action that runs a macro, select the appropriate options:

   To | Choose
   ---|----------------------
   Select a macro (or open a file that contains macros) each time you click the button | Select macro when action occurs
   Specify a macro that runs automatically each time you click the button | Select macro
   You can enter command-line arguments for the macro in the Macro data field

7. From the Settings pane, set the properties for the new button that appears on the Ribbon.
8. Click OK.
9. If prompted, type a new filename for the custom ribbon and then save the file.
   The button is saved to a custom ribbon file that you can use in other session documents.

Related Topics
- “Select Action Dialog Box” on page 161
- “Creating and Using Macros” on page 871
- “Add Controls to the Ribbon” on page 28
Add a Button with an Action and a Menu

A split button includes a functional button and a menu. Split buttons look like galleries except that they perform an action in addition to opening a menu. For an example of a split button, see the Screen History control — when clicked, the button opens an option pane and the menu shows a history of recorded screens.

To add a split button

1. On the Appearance tab, click UI Designer.
2. From the Design View pane, from the Ribbon simulation, select the tab and group to which you want to add the control.
   - To select a group, click the group name. Create a new group, if needed.
3. From the Insert Controls pane, click Split Button.
4. From the Subitems Collection Editor dialog box, click Add, and then select Button.
5. Repeat the previous step to add as many buttons as you want to appear in the menu.
6. With a button selected in the list, set the action and other properties.
7. When you have finished adding and configuring buttons, click OK.
   - The Subitems Collection Editor dialog box closes.
8. From the Settings pane, set the action and other properties for the new split button that appears on the Ribbon.
9. Click OK.

Related Topics

- “Subitems Collection Editor Dialog Box (UI Designer)” on page 87
- “Select Action Dialog Box” on page 161
- “Add Controls to the Ribbon” on page 28

Add a Menu that Holds Buttons
Use the **Gallery** control to add a menu of options to the Ribbon.

**NOTE:** To add a button that performs an action in addition to opening a menu, use the **Split Button** control.

**To add a gallery**

1. On the **Appearance** tab, click **UI Designer**.
2. From the **Design View** pane, from the Ribbon simulation, select the tab and group to which you want to add the control.
   - To select a group, click the group name. Create a new group, if needed.
3. From the **Insert Controls** pane, click **Gallery**.
4. From the **Subitems Collection Editor** dialog box, click **Add**, and then select **Button**.
5. Repeat the previous step to add as many buttons as you want to appear in the menu.
6. With a button selected in the list, set the action and other properties.
7. When you have finished adding and configuring buttons, click **OK**.
   - The **Subitems Collection Editor** dialog box closes.
8. Specify the appearance of the gallery by doing one of the following:
   - Select **Change settings**, and then type the label, tooltip, and description you want.
   - Click **Select Action**, and then select an action from which to use the label, tooltip, and description.
9. Click **OK**.

**Related Topics**

- “Add a Button with an Action and a Menu” on page 78
- “Subitems Collection Editor Dialog Box (UI Designer)” on page 87
- “Select Action Dialog Box” on page 161
- “Add Controls to the Ribbon” on page 28

**Add a Group**

A group provides a container for controls on the Ribbon. For an example of a group, see **Host** or **Clipboard** on the **Session** ribbon.

**To add a group**

1. On the **Appearance** tab, click **UI Designer**.
2. From the **Design View** pane, from the Ribbon simulation, select the tab to which you want to add a new group of controls.
3. From the **Insert Controls** pane, click **Group**.
4. Enter a label for the group name.
5. Add controls to the group by clicking them in the **Insert Controls** pane.
6. Specify control settings, and then click **OK** to save your changes.
Add a Group of Buttons

You can stack up to three controls — buttons, split buttons, and galleries — in a button group. For an example of a button group on the Ribbon, see the *Host* group on the *Session* ribbon: *Connect*, *Disconnect*, and *Quick Keys* are combined in a single button group.

**To add a button group**

1. On the **Appearance** tab, click **UI Designer**.
2. From the **Design View** pane, from the Ribbon simulation, select the tab and group to which you want to add the control.
   - To select a group, click the group name. Create a new group, if needed.
3. From the **Insert Controls** pane, click **Button Group**.
4. From the **Subitems Collection Editor** dialog box, click **Add** and then select the item you want.
5. Repeat the previous step to add additional buttons, split buttons, or galleries (up to three items total).
6. With a button, split button, or gallery selected in the list, set the action and other properties.
   - When you have finished adding and configuring items to the group, click **OK** to close the **Subitems Collection Editor** dialog box.
7. Click **OK**.

**Related Topics**

- “Subitems Collection Editor Dialog Box (UI Designer)” on page 87
- “Select Action Dialog Box” on page 161
- “Add Controls to the Ribbon” on page 28

Add a Dialog Launcher to a Group

Groups can include a dialog launcher control in the lower-right corner. This control typically opens settings or performs other tasks relevant to the group.

**To add a dialog launcher**

1. On the **Appearance** tab, click **UI Designer**.
2. Do one of the following:
   - Create a new group by clicking **Group** in the **Insert Controls** pane.
   - Select an existing group from the **Design View** by clicking the group name.
3. With the group selected, from the **Settings** pane, select **Show dialog launcher button** to enable the settings.
4. From the **Settings** pane, to set the action and other properties for the new dialog launcher that appears on the Ribbon, click **Select Action**.
5. Click **OK**.

**Related Topics**

- “Subitems Collection Editor Dialog Box (UI Designer)” on page 87
- “Add Controls to the Ribbon” on page 28
Add a Tab

Add a new tab to create a new category on the Ribbon for custom controls.

To add a tab

1. On the Appearance tab, click UI Designer.
2. In the Insert Controls pane, click Tab.
3. In the Settings pane, type a name for the tab in the Label box.
4. Click OK.

Remove Controls from the Ribbon

You can delete tabs, groups, and individual buttons from the Ribbon.

TIP: To simplify your workspace temporarily, hide the Ribbon by double-clicking any tab on the Ribbon, or by clicking the Full Screen button from the status bar.

To remove a control

1. On the Appearance tab, click UI Designer.
2. From the Design View pane of UI Designer, select the control you want to delete.
3. In the Arrange Controls pane, click Delete.
4. To view your changes before saving them, in the Review pane, click Preview.
5. Click OK.

Modify Existing Controls on the Ribbon

You can change built-in controls or custom controls.

To modify an existing control

1. On the Appearance tab, click UI Designer.
2. In the Design View pane, from the Ribbon simulation, select the control that you want to modify.

NOTE: To select a button group, click the bottom edge of the group, or, select one of its buttons, and then, under Arrange Controls, click Select Parent. To select a group, click the group name.

3. In the Settings pane, make your changes.
4. Click OK.
Related Topics

- “Move Controls on the Ribbon” on page 50
- “Select Action Dialog Box” on page 161
- “Subitems Collection Editor Dialog Box (UI Designer)” on page 87
- “Add Controls to the Ribbon” on page 28
- “Remove Controls from the Ribbon” on page 52

Move Controls on the Ribbon

From the **UI Designer**, you can reorganize or simplify your workspace by selecting a new location for the controls.

**To move a control within its parent control**

- To move a control to new location within its parent control (for example, to move a button within a group, or to move a group on a tab), use the **Move** buttons from the **Arrange Controls** pane in the **UI Designer**.

You can move a control from one group to a different group, move a group from one tab to a different tab, or delete a control from its current location and add it to the new location.

**To move a control outside its parent control**

1. From the **Design View** pane, select the control that you want to move.
2. Write down the settings that appear in the **Settings** pane.
3. From the **Arrange Controls** pane, click **Delete**.
4. Select the tab and group where you want to place the control, or add a new tab and group.
5. From the **Insert Controls** pane:

   To insert | Do this
   
   **A Tab, Group, or Button** | Click the control.
   
   **A Gallery, Split Button, or Button Group** | Click the control, then from the **Subitems Collector Editor** dialog box, add subitems to the control, and then click **OK**.
   
   **A Built-In** | Click the control, then from the **Built-In Controls** dialog box, choose a pre-defined gallery or group, and then click **Insert**.

6. Change the properties for the control in the **Settings** pane to match the settings you wrote down before you deleted the control from its original location.
7. Click **OK**.

Related Topics

- “Built-In Controls Dialog Box (UI Designer)” on page 88
- “Subitems Collection Editor Dialog Box (UI Designer)” on page 87
Restore the Default Ribbon

You can reverse any changes you've made to the Ribbon in the UI Designer by selecting the default ribbon.

1. With a session open in InfoConnect, from the Quick Access Toolbar, click ...
2. Under User Interface, click Manage Ribbon.
3. Click Select another Ribbon file.
4. Click Built-in and select a Ribbon from the list that best matches your session document; for example, for a 3270 session document, select Reflection 2014 Ribbon UI for 3270 Sessions.
5. Click OK.
6. To save the session document, on the Quick Access Toolbar, click ...
   The session will use the Ribbon you selected until you select a different Ribbon.

Manage Ribbon Dialog Box

The Ribbon contains tools that you use to complete tasks in the selected document. When you create a terminal session document, it includes a pointer to a default, built-in Ribbon file. For example, a new 5250 session document uses Reflection2007.5250.Ribbon.xuml (or Reflection2007.5250.Classic.xuml if you work in Classic mode). You can choose a different Ribbon file for each session, and you can create custom Ribbon files using the UI Designer.
Select another Ribbon file  
Click to choose a different Ribbon file from a list of existing Ribbon files. The file must be in a trusted location.

Modify the currently selected Ribbon file  
Select to open the UI Designer and modify the Ribbon file used by this session. Because built-in files are read-only, if the currently selected file is a built-in file, it will be saved as a custom file when you change it.

NOTE: If you select a Ribbon that doesn't match the current document type or user interface, the default Ribbon is used instead to ensure access to all features.

Create a new Ribbon from an existing file  
Click to create a custom Ribbon file based on an existing Ribbon file. To reopen the file later, it must be saved in a trusted location.

Related Topics

- “Customize the Ribbon” on page 74
- “UI Designer” on page 84

Select a Ribbon File Dialog Box

Getting there

1. With a session open in InfoConnect, from the Quick Access Toolbar, click .
2. Under User Interface, click Manage Ribbon.
3. Click Select another Ribbon file.

From this dialog box, select a Ribbon file to use with this session.

**Built-In**  
Select this option to show the Ribbon files distributed with InfoConnect.

**Custom**  
Select this option to show the Ribbon files that you've previously modified and saved. If the file you want doesn't appear in the list, click Browse to select it.

**NOTE:** The file must be in a trusted location.

UI Designer

**Index Term**
Primary: XUML files

**Index Term**
Primary: UI Designer

**Index Term**
Primary: Ribbon UI Designer

**Index Term**
Primary: labels
Secondary: on the Ribbon

**Index Term**
Primary: Design View
Getting there

1 Open a session document.
2 On the Appearance tab, in the Menus group, click UI Designer.

With the UI Designer, you can create new controls — including buttons, tabs, and menus — or modify existing controls on the Ribbon. Save your changes as a custom UI file (.xuml) that you can use with other session documents.

Design View

Displays a dynamic, graphical view of the Ribbon and tabs. Navigate to and select the controls you want to modify.

Insert Controls

Click the items you want to add to the Ribbon.

- **Tab**: Adds a Ribbon tab on which you can place additional controls.
- **Group**: Adds a container for controls.
- **Button**: Adds a single button control.
- **Gallery**: Adds a menu of buttons.
- **Split Button**: Adds a button and a menu.
- **Button Group**: Adds a button that contains three individual button controls, including split buttons and button menus (Galleries).
- **Built-ins**: Adds a control for built-in features, such as Quick Keys and Office Tools.

New items appear on the far right end of the Ribbon. If a button or group is selected in the Design View, new buttons appear in the same group as the selection.

Arrange Controls

- **Move Up**: Moves the selected control in the direction specified.
- **Move Down**: Moves the selected control in the opposite direction of **Move Up**.
- **Move Left**: Moves the selected control to the left.
- **Move Right**: Moves the selected control to the right.
- **Delete**: Removes the selected control from the Ribbon.
- **Select Parent**: Selects the parent control, or container, for the selected child or group control.

**NOTE**: To select a button group, click the bottom edge of the group, or, select one of its buttons, and then, under Arrange Controls, click Select Parent.

Review

- **Preview**: Displays, in a separate window, the way the Ribbon will appear with the options you selected.
Settings

This area of the UI Designer displays, for the selected control, the settings that allow or require additional input.

The specific items shown will vary, depending on the control that is selected.

Show dialog launcher button  Select to add a dialog launcher button next to the label on a Group.

Identifier  Use to identify the control when programming with the InfoConnect API.

NOTE: See "Dynamically Changing the User Interface" in the VBA Guide or the .NET API Guide.

Visible  Select to display the control. You can use the InfoConnect API to show or hide the control.

Enabled  Select to enable the control. You can use the InfoConnect API to enable or disable the control.

Action  Shows the action assigned to the control.

Select Action  Click to specify an action for the selected control in the Select Action dialog box.

Modify Subitems  Click to add subitems to a control. For example, if you add a gallery to a button group in the Subitems Collection Editor dialog box, click Modify Subitems to add buttons to the menu for that gallery.

Change settings  Select to allow changes to the label, image, tooltip, and description of the control.

NOTE: Changes to these settings overwrite the default properties of the selected action.

Label  Specifies the text that appears on the control.

NOTE: An ampersand (&) in front of a character in a label indicates that the character will function as a keyboard accelerator key.

Image  Shows the image that appears on the control. If you don't select an image, an orange circle with an exclamation point appears.

Select Image  Click to browse for a .PNG or .JPEG image to appear on the control.

Tooltip  Enter a heading that appears when the pointer is held over the control.

Description  Enter a description that appears (below the heading) when the pointer is held over the control.

Reset  Click to clear any of changes you've made and restore the default properties of the assigned action.

Related Topics

- “Add Controls to the Ribbon” on page 28
- “Remove Controls from the Ribbon” on page 52
- “Modify Existing Controls on the Ribbon” on page 49
- “Move Controls on the Ribbon” on page 50
- “Select Action Dialog Box” on page 161
- “Select a Ribbon File Dialog Box” on page 84
Create a New Ribbon File Dialog Box

Getting there

1. With a session open in InfoConnect, from the Quick Access Toolbar, click Open.
2. Under User Interface, click Manage Ribbon.
3. Click Create a new Ribbon from an existing Ribbon file.

From this dialog box, select the Ribbon file to use as a template for creating a new Ribbon file.

Built-In
Select this option to show the Ribbon files distributed with InfoConnect.

Custom
Select this option to show the Ribbon files that you've previously modified and saved. If the file you want doesn't appear in the list, click Browse to select it.

NOTE: The file must be in a trusted location.

Use the new file in the current session document
Select this option to use the file you are about to create with the current session.

Subitems Collection Editor Dialog Box (UI Designer)

Index Term
Primary: Subitems Collection Editor

Getting there

1. Open a session document.
2. On the Ribbon, click the Appearance tab.
3. From the Menus group, click UI Designer.
4. Under Insert Controls, click Gallery, Split Button, or Button Group.

-or-
Select an existing Gallery, Split Button, or Button Group, and then, under Settings, click the Modify Subitems button.

If you add a button group, split button, or gallery control to the Ribbon, you must specify subitems (buttons and menus) for that control.

Choose from the available subitems:

Subitems

Add
Add a Button, Split Button, or Gallery to a control. The control you select in the Insert Controls pane of the UI Designer determines the subitems you can add; for example, if you select Button Group, you can select any of the subitems.

Remove
Removes the selected control type from the list.

Move Up / Move Down
Moves the selected control up or down in the list.
### Subitem Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifier</td>
<td>Use to identify the control when programming with the InfoConnect API.</td>
</tr>
<tr>
<td><strong>NOTE:</strong></td>
<td>See &quot;Dynamically Changing the User Interface&quot; in the VBA Guide or the .NET API Guide.</td>
</tr>
<tr>
<td>Visible</td>
<td>Select to display the control. You can use the InfoConnect API to show or hide the control.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Select to enable the control. You can use the InfoConnect API to enable or disable the control.</td>
</tr>
<tr>
<td>Action</td>
<td>Shows the action assigned to the control.</td>
</tr>
<tr>
<td>Select Action</td>
<td>Click to specify an action for the selected control in the Select Action dialog box.</td>
</tr>
<tr>
<td>Modify Subitems</td>
<td>Click to add subitems to a control. For example, if you add a gallery to a button group in the Subitems Collection Editor dialog box, click Modify Subitems to add buttons to the menu for that gallery.</td>
</tr>
<tr>
<td>Change settings</td>
<td>Select to allow changes to the label, image, tooltip, and description of the control.</td>
</tr>
<tr>
<td><strong>NOTE:</strong></td>
<td>Changes to these settings overwrite the default properties of the selected action.</td>
</tr>
<tr>
<td>Label</td>
<td>Specifies the text that appears on the control.</td>
</tr>
<tr>
<td><strong>NOTE:</strong></td>
<td>An ampersand (&amp;) in front of a character in a label indicates that the character will function as a keyboard accelerator key.</td>
</tr>
<tr>
<td>Image</td>
<td>Shows the image that appears on the control. If you don't select an image, an orange circle with an exclamation point appears.</td>
</tr>
<tr>
<td>Select Image</td>
<td>Click to browse for a .PNG or .JPEG image to appear on the control.</td>
</tr>
<tr>
<td>Tooltip</td>
<td>Enter a heading that appears when the pointer is held over the control.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description that appears (below the heading) when the pointer is held over the control.</td>
</tr>
<tr>
<td>Reset</td>
<td>Click to clear any of changes you've made and restore the default properties of the assigned action.</td>
</tr>
</tbody>
</table>

### Related Topics

- “Select Action Dialog Box” on page 161
- “Add Controls to the Ribbon” on page 28

### Built-In Controls Dialog Box (UI Designer)

Index Term
Primary: controls
Secondary: colorpicker

Index Term
Primary: controls
Secondary: built-in
InfoConnect includes several controls that you can customize. With UI Designer, you can change the default location and settings of these controls to better suit your needs.

Click Built-Ins in the Insert Controls pane of UI Designer to choose from the following options:

- **Quick Keys Gallery**: Add keyboard shortcuts that let you send program function keys, program attention keys, and other commands to the host.
- **Office Tools Gallery**: Use Microsoft Word and Outlook application features with data from your host: create Word documents, send e-mail, schedule appointments, add notes and tasks, and create new contacts.
- **Recent Typing Gallery**: Quickly view and select from a list of recently typed items, and send the selected string to the active document, eliminating the need to re-enter information. This saves time and reduces errors when entering commonly-typed commands or field data.
- **Scratch Pad Gallery**: Keep notes associated with a session using the Scratch Pad, and print or save them as .rtf or .txt files.
- **Screen History Gallery**: View and/or verify the information from Screen History recordings of host screens as you navigate them, and send multiple host screens to Microsoft Word, PowerPoint, and Outlook (Email Message and Note only), if they're installed on your computer.
- **Colorpicker Control**: Add a control for standard and custom colors for host sessions.
- **VBA / Macro Group**: Provide the Visual Basic editor, and macro recording and playback tools.
- **Themes Group**: Set the appearance of host sessions, including text and background colors, sounds, and cursor properties.

## Locking Down the User Interface

Use Permissions Manager to restrict access to InfoConnect features. After you select the features you want to disable, your specifications are saved in .access files that you can deploy to users.
Permissions Manager displays groups of configurable items. The following reference topics provide a brief description for each item.

**Actions Group (page 91)**

**Workspace Groups (page 113)**
- Api Security (page 114)
- Application Options (page 114)
- Application Sounds (page 115)
- PCI DSS (page 115)
- Privacy Filter (page 116)
- Trusted Locations (page 116)
- UX Configuration (page 116)

**Document Groups**
- Classic (page 110)
- Hotspots (page 109)
- Keyboard (page 110)
- Mouse (page 110)
- Ribbon (page 110)
- Theme (page 110)

**3270 terminal Groups**
- Clipboard (page 108)
- Connection\TN3270 Advanced (page 96)
- Connection\TN3270 Basic (page 98)
- Terminal\Configuration\3270 (page 98)

**Productivity Groups**
- Productivity (page 111)
- AutoComplete (page 113)
- AutoExpand (page 113)
- Office (page 112)

**5250 terminal Groups**
- Clipboard (page 108)
- Connection\TN5250 Advanced (page 102)
- Connection\TN5250 Basic (page 104)
- Terminal\Configuration\5250 (page 104)

**VT terminal Groups**
- Clipboard (page 117)
- Connection (page 117)
- Safeguards (page 120)
- Terminal (page 119)

**Related Topics**
- “How the Permissions Manager Items are Organized” on page 91
How the Permissions Manager Items are Organized

<table>
<thead>
<tr>
<th>Groups</th>
<th>The feature group to configure.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Items</td>
<td>Lists the configurable items within the selected group.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>This column</th>
<th>Indicates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Item</td>
<td>The name of the item.</td>
</tr>
<tr>
<td>Accessibility</td>
<td>The security level of the item. <strong>Full</strong> means that the user can configure the item; <strong>Restricted</strong> means that the user cannot configure the item without administrator assistance.</td>
</tr>
</tbody>
</table>

Permissions Manager Additional security options

**Session File Encryption**

Session files may be encrypted from the **Save As** dialog box, by selecting the encrypted option from the **Save As Type** box.

**User Can Only Open Encrypted Session Files**
Select to prevent the user from opening unencrypted session files.

**User Can Only Save Encrypted Session Files**
Select to prevent the user from saving unencrypted session files.

Restrict Actions (actions.access)

**Index Term**
**Primary:** Permissions Manager
**Secondary:** additional security options

**Index Term**
**Primary:** actions
**Secondary:** reference table

**Index Term**
**Primary:** Permissions Manager
**Secondary:** actions

In many cases, an action can be accessed multiple ways. For example, you can restrict access to the Clipboard Settings action (clipboardSettingsAction). However, if the user has access to the Document Settings action (settingsAction), Clipboard settings will still be accessible.

<table>
<thead>
<tr>
<th>Item Name</th>
<th>UI Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>appointmentAction</td>
<td>Create an Outlook appointment that includes the selected host data in the message field.</td>
</tr>
<tr>
<td>backHistoryAction</td>
<td>View the previous host screen in ready-only mode.</td>
</tr>
<tr>
<td>clearAllAction</td>
<td>Remove all text from the display memory, including what's on the screen.</td>
</tr>
<tr>
<td>clearDisplayAction</td>
<td>Remove all text from the screen. By default, InfoConnect saves this text to the display memory.</td>
</tr>
<tr>
<td>Item Name</td>
<td>UI Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>clearSelectionAction</td>
<td>Clear the selection by clicking somewhere.</td>
</tr>
<tr>
<td>clipboardSettingsAction</td>
<td>Open the <strong>Clipboard Settings</strong> dialog box to configure settings that control how the Cut, Copy, and Paste functions work.</td>
</tr>
<tr>
<td>closeAction</td>
<td>Close the current document.</td>
</tr>
<tr>
<td>codePageSettingsAction</td>
<td>Open the <strong>Select Host Code Page</strong> dialog box to specify the host code page for your display session.</td>
</tr>
<tr>
<td>connectAction</td>
<td>Connect to the host for the current session document.</td>
</tr>
<tr>
<td>connectDisconnectAction</td>
<td>Connect to the host for the current session document, and then invoke again to disconnect.</td>
</tr>
<tr>
<td>contactAction</td>
<td>Create a new contact in Outlook that includes the selected host data in the Notes field.</td>
</tr>
<tr>
<td>contextMenuEditorAction</td>
<td>Open the Context Menu Editor.</td>
</tr>
<tr>
<td>copyAction</td>
<td>Copy the selected text to the Clipboard.</td>
</tr>
<tr>
<td>copyAppendAction</td>
<td>Add the selected text to the Clipboard.</td>
</tr>
<tr>
<td>cutAction</td>
<td>Delete the selected text and copy it to the Clipboard.</td>
</tr>
<tr>
<td>cutAppendAction</td>
<td>Delete the selected text and add it to the Clipboard.</td>
</tr>
<tr>
<td>disconnectAction</td>
<td>Disconnect from the host for the current session document.</td>
</tr>
<tr>
<td>emailMessageAction</td>
<td>Create an Outlook e-mail message that includes the selected host data.</td>
</tr>
<tr>
<td>exitAction</td>
<td>Quit the application.</td>
</tr>
<tr>
<td>fileTransferAction</td>
<td>Open the <strong>Transfer</strong> dialog box.</td>
</tr>
<tr>
<td>forwardHistoryAction</td>
<td>View the next screen in your screen history sequence.</td>
</tr>
<tr>
<td>ftpFileTransferAction</td>
<td>Open <strong>InfoConnect FTP Client</strong>.</td>
</tr>
<tr>
<td>fullScreenViewAction</td>
<td>Hide the Ribbon, and expand the workspace to fill your computer screen.</td>
</tr>
<tr>
<td>globalSettingsAction</td>
<td>Open the <strong>InfoConnect</strong> workspace configuration settings.</td>
</tr>
<tr>
<td>holdAction</td>
<td>Workspace configuration settings affect all terminal session and Web page documents opened in <strong>InfoConnect</strong>.  Workspace configuration settings include security, file locations, and other settings related to <strong>InfoConnect</strong>.</td>
</tr>
<tr>
<td>helpAction</td>
<td>Open Help from the main workspace <strong>Help</strong> button.</td>
</tr>
<tr>
<td>hostConnectionSettingsAction</td>
<td>Configure the host connection for the current session document.</td>
</tr>
<tr>
<td>hotspotsSettingsAction</td>
<td>Open the <strong>Set Up Hotspot Display Settings</strong> dialog box.</td>
</tr>
<tr>
<td>keyboardExtendSelection</td>
<td>Extend the screen selection using the keyboard.</td>
</tr>
<tr>
<td>keyboardMapperAction</td>
<td>Display the keyboard map.</td>
</tr>
<tr>
<td>launchApplicationAction</td>
<td>Launch an external application from the <strong>InfoConnect</strong> workspace using a customized UI element.</td>
</tr>
<tr>
<td>launchSupportWebsiteAction</td>
<td>Open the Attachmate Support site from the <strong>Help</strong> menu.</td>
</tr>
<tr>
<td>Item Name</td>
<td>UI Description</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>launchVbaAction</td>
<td>Open the Visual Basic editor to create a VBA macro based on objects defined by the active session.</td>
</tr>
<tr>
<td>layoutCascadeAction</td>
<td>Arrange all open document windows in a cascade. The title bar of each window remains visible.</td>
</tr>
<tr>
<td>layoutHorizontalAction</td>
<td>Arrange all open document windows horizontally.</td>
</tr>
<tr>
<td>layoutSettingsAction</td>
<td>Open the <strong>Layout Settings</strong> dialog box.</td>
</tr>
<tr>
<td>layoutVerticalAction</td>
<td>Arrange all open document windows vertically.</td>
</tr>
<tr>
<td>lightPenAction</td>
<td>Simulate a light pen selection with your mouse or keyboard.</td>
</tr>
<tr>
<td>macroSecurityAction</td>
<td>Set macro security options to protect a macro from accidental changes.</td>
</tr>
<tr>
<td>mainframeTransferChunkAction</td>
<td>Open the <strong>Transfer Settings</strong> dialog box.</td>
</tr>
<tr>
<td>manualCaptureAction</td>
<td>Manually capture the current screen.</td>
</tr>
<tr>
<td>mapKeystrokeAction</td>
<td>Open the <strong>Keyboard Mapper</strong> to associate a keystroke with a host terminal key or to create a keyboard shortcut.</td>
</tr>
<tr>
<td>modelSettingsAction</td>
<td>Open the basic host connection settings page to specify the terminal model you want to emulate.</td>
</tr>
<tr>
<td>moveCursorAction</td>
<td>Move the cursor with a mouse click.</td>
</tr>
<tr>
<td>moveHostCursorAction</td>
<td>Move the cursor by sending the correct arrow keys to the host so that it moves the cursor relative to its current position.</td>
</tr>
<tr>
<td>newDocumentAction</td>
<td>Create a new document of any kind from the &quot;Workspace Menu&quot; on page 891 or the <strong>Quick Access</strong> toolbar.</td>
</tr>
<tr>
<td>nextWindowAction</td>
<td>Make the next document or task pane active.</td>
</tr>
<tr>
<td>noteAction</td>
<td>Create an Outlook &quot;sticky&quot; note that includes the selected host data.</td>
</tr>
<tr>
<td>officeToolsPaneAction</td>
<td>Open the <strong>Office Tools</strong> task pane.</td>
</tr>
<tr>
<td>openAction</td>
<td>Open any kind of document from the &quot;Workspace Menu&quot; on page 891 or the <strong>Quick Access</strong> toolbar.</td>
</tr>
<tr>
<td>openURLAction</td>
<td>Open a Web page from within <strong>InfoConnect</strong>.</td>
</tr>
<tr>
<td>pageSetupAction</td>
<td>Open the <strong>Page Setup</strong> dialog box.</td>
</tr>
<tr>
<td>pasteAction</td>
<td>Paste data from the Clipboard to the current cursor location.</td>
</tr>
<tr>
<td>pasteNextAction</td>
<td>Insert the remaining text in the paste next buffer within the host application.</td>
</tr>
<tr>
<td>pauseMacroAction</td>
<td>Pause a recording macro.</td>
</tr>
<tr>
<td>playBackTraceAction</td>
<td>Select a trace file to play back.</td>
</tr>
<tr>
<td>playNextTraceRecordAction</td>
<td>Play the next record in the current trace file.</td>
</tr>
<tr>
<td>playPreviousTraceRecordAction</td>
<td>Play the previous record in the current trace file.</td>
</tr>
<tr>
<td>printAction</td>
<td>Print the current document from the &quot;Workspace Menu&quot; on page 891 or the <strong>Quick Access</strong> toolbar.</td>
</tr>
<tr>
<td>printSetupAction</td>
<td>Open the <strong>Print Setup</strong> dialog box.</td>
</tr>
<tr>
<td>Item Name</td>
<td>UI Description</td>
</tr>
<tr>
<td>-----------</td>
<td>----------------</td>
</tr>
<tr>
<td>processRUOTraceAction</td>
<td>Process a trace file to generate a Reflection Basic script file, or to add system details to the text format report.</td>
</tr>
<tr>
<td>quickKeysAction</td>
<td>Open a gallery of buttons that you can click to send PA keys, PF keys, or other commands to the host.</td>
</tr>
<tr>
<td>quickPrintAction</td>
<td>Print the current document without opening the Print dialog box.</td>
</tr>
<tr>
<td>recentTypingPaneAction</td>
<td>Open the Recent Typing task pane.</td>
</tr>
<tr>
<td>recordMacroAction</td>
<td>Record a macro.</td>
</tr>
<tr>
<td>runEBEditAction</td>
<td>Run EXTRA! Basic Editor.</td>
</tr>
<tr>
<td>runHostExplorerMacro</td>
<td>Run a macro that contains Hummingbird Basic commands.</td>
</tr>
<tr>
<td>runLegacyExtraMacroAction</td>
<td>Open an EXRAI file that contains macros, and select one to run.</td>
</tr>
<tr>
<td>runLegacyMacroAction</td>
<td>Run an embedded legacy InfoConnect macro.</td>
</tr>
<tr>
<td>runLegacyMacroWithDataAction</td>
<td>Run an embedded legacy InfoConnect macro with data. (This allows the user to type parameters to execute with the macro.)</td>
</tr>
<tr>
<td>runLegacyRBEditAction</td>
<td>Run InfoConnect Basic Editor.</td>
</tr>
<tr>
<td>runLegacyRBMacroAction</td>
<td>Run a legacy InfoConnect Basic macro.</td>
</tr>
<tr>
<td>runLegacyReflectionMacroAction</td>
<td>Run an external legacy InfoConnect macro.</td>
</tr>
<tr>
<td>runMacroAction</td>
<td>Run an InfoConnect Workspace macro.</td>
</tr>
<tr>
<td>runPCommMacroAction</td>
<td>Open an IBM Personal Communications file that contains a macro.</td>
</tr>
<tr>
<td>RunQWSMacroAction</td>
<td>Open a QWS3270 file that contains a macro.</td>
</tr>
<tr>
<td>runRCLScriptAction</td>
<td>Run an RCL script.</td>
</tr>
<tr>
<td>runRumbaMacroAction</td>
<td>Open a RUMBA file that contains macros, and select one to run.</td>
</tr>
<tr>
<td>runSupportToolAction</td>
<td>Runs a utility to help Attachmate Support collect InfoConnect application data.</td>
</tr>
<tr>
<td>saveAction</td>
<td>Save the current document from the Workspace Menu on page 891 or the Quick Access toolbar.</td>
</tr>
<tr>
<td>saveAsAction</td>
<td>Save the current document with a new name or location.</td>
</tr>
<tr>
<td>saveLayoutAction</td>
<td>Save the current layout.</td>
</tr>
<tr>
<td>saveRSFTAction</td>
<td>Save the current document configuration as a template.</td>
</tr>
<tr>
<td>scratchPadPaneAction</td>
<td>Open the Scratch Pad task pane.</td>
</tr>
<tr>
<td>screenHistoryPaneAction</td>
<td>Open the Screen History task pane.</td>
</tr>
<tr>
<td>selectAllAction</td>
<td>Select all data on the screen.</td>
</tr>
<tr>
<td>sendHostKeyAction</td>
<td>Send a preconfigured key to the host.</td>
</tr>
<tr>
<td>sendHostTextAction</td>
<td>Send some preconfigured text to the host.</td>
</tr>
<tr>
<td>sendWordAction</td>
<td>Send the word at the current cursor location to the host, followed by a Return (VT) or an Enter (3270/5250) key. This is typically mapped to a mouse button.</td>
</tr>
</tbody>
</table>
settingsAction
Open the document settings from the “Workspace Menu” on page 891 or the Quick Access toolbar.

setupLoggingAction
Open the Logging Settings dialog box.

showAPIGuideAction
Open the .NET API Guide.

showAPIHelpAction
Open the .NET API Help.

showAutoCompleteSettingsAction
Open the Configure Auto Complete dialog box.

showAutoExpandAction
Open the Configure Auto Expand dialog box.

showContextMenuAction
Open the context menu. This is the default action of the right mouse button.

showHelpAboutAction
Show the About dialog from the Help menu.

showLiveScreenAction
Return to the current host screen for your session from anywhere in the screen history sequence.

showMouseMapperAction
Open the Mouse Mapper.

showPrivacyFilterAction
Open the Set Up Privacy Filters dialog box.

showProductivitySettingsAction
Open the Configure Productivity Defaults dialog box.

showRecentTypingSettingsAction
Open the Configure Recent Typing dialog box.

showScreenHistorySettingAction
Open the Configure Screen History dialog box.

showSpecificContextMenuAction
Specifies the context menu to open when the action is performed.

showSpellCheckAction
Open the Configure Spell Checking dialog box.

showUIDesignerAction
Open the UI Designer to customize your Ribbon.

showVBAGuideAction
Open the VBA Guide.

showVBAHelpAction
Open the VBA Help.

spellCheckFieldAction
Check spelling in the currently active host field.

spellCheckScreenAction
Check spelling in the current host screen.

startLoggingAction
Turn logging on for a VT session.

startTraceAction
Create a new trace and begin the trace process.

stopLoggingAction
Turn logging off for a VT session.

stopMacroAction
Stop the currently running macro.

stopTraceAction
Stop the currently active trace.

taskAction
Create an unscheduled Outlook task that includes the selected host data in the task body field.

terminalAppearanceSettingsAction
Open the Configure Terminal Settings dialog box.

themeSettingsAction
Open the Manage Themes dialog box.

toggleMacroRecordAction
Record your actions in a VBA macro.

togglePauseMacroAction
Pause the macro recording process.
Permissions Manager Items: TN3270 Advanced

Index Term
Primary: Permissions Manager
Secondary: TN3270 items

TN3270 Advanced

<table>
<thead>
<tr>
<th>Item Name</th>
<th>Sub-group</th>
<th>UI Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AssociatedPrinterSession</td>
<td></td>
<td>The associated 3270 printer session filename.</td>
</tr>
<tr>
<td>AssociatePrinterBy</td>
<td>TN3270 Enhanced Protocol</td>
<td>The associated 3270 printer session, or Association string.</td>
</tr>
<tr>
<td>AsyncTransportEnabled</td>
<td></td>
<td>Revert to polling mode for host interactions. This is mainly used for diagnostic purposes.</td>
</tr>
<tr>
<td>AttentionKey</td>
<td>TN3270-specific</td>
<td>Treat ATTN key as TelnetAbortOutput, TelnetBreak, or TelnetIntProcess.</td>
</tr>
<tr>
<td>AutoReconnect</td>
<td></td>
<td>Reconnect after a disconnection that is not initiated by InfoConnect.</td>
</tr>
<tr>
<td>BackSpaceKeyAsDelete</td>
<td></td>
<td>Treat Backspace key as Delete key.</td>
</tr>
<tr>
<td>BeforeConnectStartupMacro</td>
<td></td>
<td>Run a macro or other action before the initial connection.</td>
</tr>
<tr>
<td>ConnectMacro</td>
<td>Connection Action</td>
<td>Run a macro or other action after the initial connection.</td>
</tr>
<tr>
<td>ConnectMacroData</td>
<td></td>
<td>The name of a macro that is run automatically after a connection is established.</td>
</tr>
<tr>
<td>ConnectScript</td>
<td></td>
<td>The InfoConnect script that runs automatically after a connection is established.</td>
</tr>
<tr>
<td>ConnectScriptArguments</td>
<td></td>
<td>The parameter string to pass to the connect script after a connection is established.</td>
</tr>
<tr>
<td>Item Name</td>
<td>Sub-group</td>
<td>UI Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DBCSUnmappedChar</td>
<td></td>
<td>Allow user to choose how to translate double-byte host characters that are not available in the Shift-JIS double-byte character translation table.</td>
</tr>
<tr>
<td>EnableAssociatedPrinter</td>
<td></td>
<td>Enable the associated printer. (See AssociatePrinterBy, AssociatedPrinterSession, and TNAssociation.)</td>
</tr>
<tr>
<td>ExpressLogonFeature AppID</td>
<td>Security</td>
<td>The application ID to use for Express Logon Feature (ELF) support.</td>
</tr>
<tr>
<td>FileSystem</td>
<td></td>
<td>Allow users to specify whether to use the ANSI character set or the ASCII character set for ASCII transfers from the host.</td>
</tr>
<tr>
<td>HLLAPI.LongName</td>
<td>HLLAPI Options</td>
<td>The HLLAPI application associated with a particular session.</td>
</tr>
<tr>
<td>HLLAPI.ShortName</td>
<td>HLLAPI Options</td>
<td>An identifier that a HLLAPI application uses to link to a session.</td>
</tr>
<tr>
<td>HLLAPI.Style</td>
<td>HLLAPI Options</td>
<td>The HLLAPI configuration. This can be a numeric value or a predefined constant.</td>
</tr>
<tr>
<td>KeepAlive</td>
<td>Misc.</td>
<td>Periodically poll the host to determine if Telnet connections remain active during intervals when you are not sending data to the host.</td>
</tr>
<tr>
<td>KeepAlive.Timeout</td>
<td>Misc.</td>
<td>The interval, measured in seconds, between keep alive requests sent by InfoConnect.</td>
</tr>
<tr>
<td>ReuseMSSNAPoolName</td>
<td></td>
<td>Allow users to choose how to handle MS SNA pool names. When unselected (the default), administrators must assign the pool to each user for the number of connections the user needs. When selected, administrators can assign the pool once to each user.</td>
</tr>
<tr>
<td>RunMacroAtReconnect</td>
<td>Connection Action</td>
<td>Run macro when reconnecting.</td>
</tr>
<tr>
<td>SameModel</td>
<td>TN3270-specific</td>
<td>Specify to use the same model for primary and alternate screens.</td>
</tr>
<tr>
<td>Support3270Partitions</td>
<td></td>
<td>Send partition-related information from the terminal to the host in response to a host query request.</td>
</tr>
<tr>
<td>SysReqKey</td>
<td>TN3270-specific</td>
<td>Specifies what happens when you transmit the SysReq function. The definition of this key varies by host application.</td>
</tr>
<tr>
<td>TelnetLocation</td>
<td>Misc.</td>
<td>The location where the connection originated. This can also be used to provide informational messages to the host from the PC.</td>
</tr>
<tr>
<td>TelnetResponseMode</td>
<td>TN3270Advanced</td>
<td>Return a message to the host from the PC after each message sent by the host.</td>
</tr>
<tr>
<td>TNAssociation</td>
<td></td>
<td>A 3270 terminal session on the host. Use this to associate a 3270 terminal session with a specific 3270 printer session.</td>
</tr>
</tbody>
</table>
### Permissions Manager Items: TN3270 Basic

<table>
<thead>
<tr>
<th>Item Name</th>
<th>Sub-group</th>
<th>UI Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UserDataDirectory</td>
<td></td>
<td>The folder where user-created files, like settings files and trace files, are saved by default.</td>
</tr>
</tbody>
</table>

**Related Topics**
- “Permissions Manager Items: TN3270 Basic” on page 98

### Permissions Manager Items: 3270 Terminal Configuration

<table>
<thead>
<tr>
<th>Item Name</th>
<th>Sub-group</th>
<th>UI Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AllowInvalidThaiInput</td>
<td></td>
<td>Turn off validity checking for Thai characters. (By default, when you enter Thai characters in a host application, InfoConnect determines whether the input is legal according to the rules of Thai character composition.)</td>
</tr>
</tbody>
</table>

**Related Topics**
- “Permissions Manager Items: TN3270 Advanced” on page 96
<table>
<thead>
<tr>
<th>Item Name</th>
<th>Sub-group</th>
<th>UI Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AutoIME</td>
<td></td>
<td>Automatically turn the Input Method Editor (IME) on when the cursor is in a double-byte input field, and off when the cursor is in a single-byte input field. When it is not specified, the state of the IME does not change in response to the cursor's location.</td>
</tr>
<tr>
<td>BDTIgnoreScrollLock</td>
<td></td>
<td>Ignore the state of Scroll Lock.</td>
</tr>
<tr>
<td>C370CharSet</td>
<td></td>
<td>Use the C/370 code page. The C/370 code page provides support for square brackets (&quot;[&quot; and &quot;]&quot;).</td>
</tr>
<tr>
<td>CmdPrompt</td>
<td></td>
<td>The character or characters in the terminal window, after which InfoConnect attempts to insert Quick Text.</td>
</tr>
<tr>
<td>CMSFileListCommand</td>
<td></td>
<td>The file list command to issue on the CMS host to list files. When the Show host files button in the Transfer dialog box is clicked, InfoConnect issues the specified file list command.</td>
</tr>
<tr>
<td>CommandLineEnabled</td>
<td></td>
<td>Enable the InfoConnect command line. This allows users to activate the command line (for example, with the Alt-L keystroke).</td>
</tr>
<tr>
<td>CursorMovementStyle</td>
<td></td>
<td>Specifies how the cursor moves between composed Thai characters.</td>
</tr>
<tr>
<td>CursorProgressionIndicator</td>
<td></td>
<td>Specifies how InfoConnect responds when the host queries to determine if End User Interface (EUI) enhancements are supported by the terminal. Use only for host applications that use cursor progression and queries to determine if EUI is supported.</td>
</tr>
<tr>
<td>DelayAfterAID</td>
<td></td>
<td>The amount of time, measured in milliseconds, to wait before processing keystrokes after an AID key (PF1-PF24, Enter, or Clear) is pressed.</td>
</tr>
<tr>
<td>DisplayMargins</td>
<td></td>
<td>Display margins around the terminal window.</td>
</tr>
<tr>
<td>EnableHotspots</td>
<td>Display</td>
<td>Enable all defined hotspots</td>
</tr>
<tr>
<td>EnableQuickText</td>
<td></td>
<td>Use the Quick Text feature.</td>
</tr>
<tr>
<td>EnterKeyRepeat</td>
<td></td>
<td>Specifies whether holding down the Enter key is equivalent to pressing it multiple times.</td>
</tr>
<tr>
<td>ExtendHotSpots</td>
<td></td>
<td>Treat a region to the right of a hotspot as part of the hotspot.</td>
</tr>
<tr>
<td>GraphicsExtendedColors</td>
<td></td>
<td>Use the set of extended graphics colors (black, white, dark blue, orange, purple, dark green, dark turquoise, mustard, gray, and brown).</td>
</tr>
<tr>
<td>HostBeep</td>
<td></td>
<td>Enable host beep.</td>
</tr>
<tr>
<td>HostCodePage</td>
<td></td>
<td>Host Code page.</td>
</tr>
<tr>
<td>Item Name</td>
<td>Sub-group</td>
<td>UI Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>------------</td>
<td>----------------</td>
</tr>
<tr>
<td>HostKeyboardType</td>
<td>Input</td>
<td>The keyboard type.</td>
</tr>
<tr>
<td>HostNumlockControl</td>
<td></td>
<td>Allows the host to turn NumLock on.</td>
</tr>
<tr>
<td>HotspotsAltKey</td>
<td>Activation</td>
<td>Under <strong>Choose key(s) to press in combination with mouse click</strong>, activate the Alt key.</td>
</tr>
<tr>
<td>HotspotsCtrlKey</td>
<td>Activation</td>
<td>Under <strong>Choose key(s) to press in combination with mouse click</strong>, activate the Ctrl key.</td>
</tr>
<tr>
<td>HotspotsDoubleClick</td>
<td>Activation</td>
<td>Under <strong>Choose key(s) to press in combination with mouse click</strong>, activate the double-click action.</td>
</tr>
<tr>
<td>HotspotsMouseButton</td>
<td>Activation</td>
<td>Choose the mouse button to activate hotspots.</td>
</tr>
<tr>
<td>HotspotsShiftKey</td>
<td>Activation</td>
<td>Under <strong>Choose key(s) to press in combination with mouse click</strong>, activate the Shift key.</td>
</tr>
<tr>
<td>IgnoreHostPrintreq</td>
<td></td>
<td>Ignore print commands in host data streams.</td>
</tr>
<tr>
<td>InputFieldUnderlines</td>
<td></td>
<td>Specify how InfoConnect underlines input fields on host screens.</td>
</tr>
<tr>
<td>InsertArena</td>
<td></td>
<td>Specify the extent to which the InsertProtocol property applies — to a single field, across multiple local fields, or to all unprotected fields.</td>
</tr>
<tr>
<td>InsertProtocol</td>
<td></td>
<td>Specify how a character will be inserted.</td>
</tr>
<tr>
<td>KanaLockState</td>
<td></td>
<td>Specify the current Kana mode of the keyboard. When the keyboard is in Kana mode, it is capable of producing half-width Katakana characters. When it is not in Kana mode, the keyboard is in Latin character mode.</td>
</tr>
<tr>
<td>KeyboardErrorReset</td>
<td>Input</td>
<td>Keyboard error.</td>
</tr>
<tr>
<td>KeysDuringWait</td>
<td></td>
<td>Allow the user to use the keyboard during a synchronous command. A synchronous command (such as <strong>Wait</strong> or <strong>WaitEvent</strong>) causes a procedure to pause until a defined waiting period expires.</td>
</tr>
<tr>
<td>MappedNumlockPreservesNumlock</td>
<td></td>
<td>Specify how InfoConnect behaves if a user presses the PC NumLock key when it has been mapped to emulate the action of a terminal key.</td>
</tr>
<tr>
<td>MouseShape</td>
<td></td>
<td>Specify the appearance of the mouse pointer in the terminal window.</td>
</tr>
<tr>
<td>NumberMouseButtons</td>
<td></td>
<td>Specify how many buttons InfoConnect assumes the mouse has. Changing this property changes the mouse shown in the <strong>Mouse Setup</strong> dialog box.</td>
</tr>
<tr>
<td>Preserve3270insertState</td>
<td></td>
<td>Specify whether pressing Enter resets the Insert mode.</td>
</tr>
<tr>
<td>Item Name</td>
<td>Sub-group</td>
<td>UI Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>PreserveEntryMode</td>
<td></td>
<td>Remain in Extended Graphics or Hexadecimal mode indefinitely after either mode is entered. From Extended Graphics mode users can enter multiple graphics; from Hexadecimal mode users can enter hexadecimal characters.</td>
</tr>
<tr>
<td>QuickText</td>
<td></td>
<td>Specify the contents of the Quick Text buffer.</td>
</tr>
<tr>
<td>RightControlKeyRepeat</td>
<td></td>
<td>Designates the right Ctrl key as a modifier key. (A modifier key is used in combination with another key to send a function. For example, Ctrl-F1 is mapped to the Attention key in 3270 sessions).</td>
</tr>
<tr>
<td>ShowBytesRemaining</td>
<td></td>
<td>Display the Show Bytes Remaining indicator on the host status line. This indicator displays the number of bytes remaining in the current field.</td>
</tr>
<tr>
<td>ShowDisplayCharsInUppercase</td>
<td></td>
<td>Display characters in uppercase.</td>
</tr>
<tr>
<td>ShowHotsspots</td>
<td>Display</td>
<td>Show all defined HotSpots.</td>
</tr>
<tr>
<td>ShowOIA</td>
<td></td>
<td>Show operation and status messages in the Operator Information Area (OIA) at the bottom of the terminal window.</td>
</tr>
<tr>
<td>ShowSOSICChars</td>
<td></td>
<td>Show shift-out and shift-in (SO/SI) control characters on the terminal screen. (This helps to determine where double-byte characters or fields begin and end.)</td>
</tr>
<tr>
<td>SubstituteDisplayChars</td>
<td></td>
<td>Specify whether zeroes should be displayed with a slash (Ø) or without a slash (0).</td>
</tr>
<tr>
<td>SupportDBCSFeatures</td>
<td>Misc.</td>
<td>Support double-byte character sets.</td>
</tr>
<tr>
<td>TelnetXSystem</td>
<td></td>
<td>Support the X SYSTEM in 3270 sessions. X SYSTEM is a keyboard locked state that occurs when the host ends a transmission to the workstation without unlocking the keyboard. Some applications use this to notify you of a message written to the display, requiring you to reset the keyboard before you can type again. Other applications rely on SNA to unlock the keyboard.</td>
</tr>
<tr>
<td>TextBlinkRate</td>
<td></td>
<td>The rate at which blinking text blinks.</td>
</tr>
<tr>
<td>TSOFileListCommand</td>
<td></td>
<td>The name of the host executable to run when, from the Transfer dialog box, the Show host files button is clicked.</td>
</tr>
<tr>
<td>TSOMemberListCommand</td>
<td></td>
<td>The name of the host executable to run when, from the Transfer dialog box, a member that is expanded is clicked.</td>
</tr>
</tbody>
</table>
Permissions Manager Items: TN5250 Advanced

**TN5250 Advanced**

<table>
<thead>
<tr>
<th>Item Name</th>
<th>Sub-group</th>
<th>UI Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TypeAhead</td>
<td>Input</td>
<td>Select to buffer characters that are typed in the terminal window. When characters are buffered, they are sent to the host as soon as possible. When characters are not buffered, anything typed while the host is not ready is lost.</td>
</tr>
<tr>
<td>UseCtrlZ</td>
<td></td>
<td>Interprets the Ctrl-Z character as an end-of-file character (when reading a file) or appends the character at the end of a file (when saving a file).</td>
</tr>
<tr>
<td>WordWrap</td>
<td>Input</td>
<td>Enable word wrap.</td>
</tr>
<tr>
<td>WordWrap3270MinimumFieldLength</td>
<td></td>
<td>Wrap text to the next available field when entered text is too long to fit in a text entry field.</td>
</tr>
</tbody>
</table>

**5250 Items**

**Index Term**

Primary: Permissions Manager
Secondary: 5250 items

**In this Section**

- “Permissions Manager Items: TN5250 Advanced” on page 102
- “Permissions Manager Items: TN5250 Basic” on page 104
- “Permissions Manager Items: 5250 Terminal Configuration” on page 104

**Permissions Manager Items: TN5250 Advanced**

**TN5250 Advanced**

<table>
<thead>
<tr>
<th>Item Name</th>
<th>Sub-group</th>
<th>UI Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS400Host</td>
<td></td>
<td>The name of the AS/400 host to connect to when Service Location Protocol (SLP) is enabled.</td>
</tr>
<tr>
<td>Async TransportEnabled</td>
<td></td>
<td>Revert to polling mode for host interactions. This is mainly used for diagnostic purposes.</td>
</tr>
<tr>
<td>AutoReconnect</td>
<td></td>
<td>Reconnect after a disconnection that is not initiated by InfoConnect.</td>
</tr>
<tr>
<td>AutoSignon</td>
<td>Sign-on Options</td>
<td>Sign-on options (all options).</td>
</tr>
<tr>
<td>BackSpaceKeyAsDelete</td>
<td></td>
<td>Treat Backspace key as Delete key.</td>
</tr>
<tr>
<td>BeforeConnectStartupMacro</td>
<td></td>
<td>Run a macro or other action before the initial connection.</td>
</tr>
<tr>
<td>ConnectMacro</td>
<td>Connection Action</td>
<td>Run a macro or other action after the initial connection.</td>
</tr>
<tr>
<td>ConnectMacroData</td>
<td></td>
<td>The name of a macro that is run automatically after a connection is established.</td>
</tr>
<tr>
<td>ConnectScript</td>
<td></td>
<td>A InfoConnect script that is run automatically after a connection is established.</td>
</tr>
<tr>
<td>Item Name</td>
<td>Sub-group</td>
<td>UI Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ConnectScriptArguments</td>
<td></td>
<td>A parameter string to pass to the connect script after a connection is established.</td>
</tr>
<tr>
<td>DBCSU unmapped Char</td>
<td></td>
<td>Allows user to choose how to translate double-byte host characters that are not available in the Shift-JIS double-byte character translation table.</td>
</tr>
<tr>
<td>DefaultPorts</td>
<td></td>
<td>Attempt to communicate with the host transaction programs using the default port numbers (as defined by IBM).</td>
</tr>
<tr>
<td>FileSystem</td>
<td></td>
<td>Allow users to choose whether to use the ANSI character set or the ASCII character set for ASCII transfers from the host.</td>
</tr>
<tr>
<td>HLLAPI Long Name</td>
<td>HLLAPI Options</td>
<td>The HLLAPI application associated with a particular InfoConnect session.</td>
</tr>
<tr>
<td>HLLAPI Short Name</td>
<td></td>
<td>An identifier that a HLLAPI application uses to link to a InfoConnect session.</td>
</tr>
<tr>
<td>HLLAPI Style</td>
<td>HLLAPI Options</td>
<td>The HLLAPI configuration. This can be a numeric value or a predefined constant.</td>
</tr>
<tr>
<td>KeepAlive</td>
<td>Misc.</td>
<td>Periodically poll the host to determine if Telnet connections remain active during intervals when you are not sending data to the host.</td>
</tr>
<tr>
<td>KeepAlive Timeout</td>
<td>Misc.</td>
<td>The interval, measured in seconds, between keep alive requests sent by InfoConnect.</td>
</tr>
<tr>
<td>Mode Name</td>
<td></td>
<td>The properties of your application. The default value is &quot;QPCSUPP&quot;, which is the common mode name defined on the AS/400 for 5250 applications.</td>
</tr>
<tr>
<td>MPTN IP Address</td>
<td></td>
<td>A suffix for a fully qualified host name, with an SNA domain name suffix, either in your Hosts file or in your TCP/IP Domain Name Server.</td>
</tr>
<tr>
<td>Password</td>
<td>Sign-on Options</td>
<td>A Password (under Automatically sign on using specified user ID and password).</td>
</tr>
<tr>
<td>Reuse MSSNAPool Name</td>
<td></td>
<td>Allow users to specify how InfoConnect handles MS SNA pool names. When cleared (the default), administrators must assign the pool to each user for the number of connections the user needs. When selected, administrators can assign the pool once to each user.</td>
</tr>
<tr>
<td>Run Macro At Reconnect</td>
<td>Connection Action</td>
<td>Run when reconnecting.</td>
</tr>
<tr>
<td>Single Sign On</td>
<td></td>
<td>Use a single user name and password for multiple log on procedures.</td>
</tr>
<tr>
<td>Telnet Environment</td>
<td></td>
<td>Automatically log on to the host as soon as a connection with InfoConnect is established.</td>
</tr>
<tr>
<td>Telnet Location</td>
<td>Misc.</td>
<td>The location where the connection originated. This can also be used to provide informational messages to the host from the PC.</td>
</tr>
</tbody>
</table>
## Permissions Manager Items: TN5250 Basic

### TN5250 Basic

<table>
<thead>
<tr>
<th>Item Name</th>
<th>Sub-group</th>
<th>UI Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TNAPPNGateway</td>
<td></td>
<td>Adds the third PC Support header to the Telnet pass-through header for a save screen command, and removes it for a restore screen command. This is valid for 5250 connections over Telnet to an Apertus gateway only.</td>
</tr>
<tr>
<td>UserDataDirectory</td>
<td></td>
<td>The folder where user-created files, like settings files and trace files, are saved by default.</td>
</tr>
<tr>
<td>UserID</td>
<td>Sign-on Options</td>
<td>The user ID (under Automatically sign on using specified user ID and password).</td>
</tr>
</tbody>
</table>

**Related Topics**

- "Permissions Manager Items: TN5250 Advanced" on page 102

## Permissions Manager Items: 5250 Terminal Configuration

<table>
<thead>
<tr>
<th>Item Name</th>
<th>Sub-group</th>
<th>UI Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TNAPPNGateway</td>
<td></td>
<td>Adds the third PC Support header to the Telnet pass-through header for a save screen command, and removes it for a restore screen command. This is valid for 5250 connections over Telnet to an Apertus gateway only.</td>
</tr>
<tr>
<td>UserDataDirectory</td>
<td></td>
<td>The folder where user-created files, like settings files and trace files, are saved by default.</td>
</tr>
<tr>
<td>UserID</td>
<td>Sign-on Options</td>
<td>The user ID (under Automatically sign on using specified user ID and password).</td>
</tr>
</tbody>
</table>

**Related Topics**

- “Permissions Manager Items: TN5250 Advanced” on page 102

## Permissions Manager Items: 5250 Terminal Configuration

<table>
<thead>
<tr>
<th>Item Name</th>
<th>Sub-group</th>
<th>UI Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIDFieldExitMode</td>
<td>Misc.</td>
<td>Enables AID field exit mode</td>
</tr>
<tr>
<td>AllowValidThaiInput</td>
<td></td>
<td>Turn off validity checking for Thai characters. (By default, when you enter Thai characters in a host application, InfoConnect determines whether the input is legal according to the rules of Thai character composition.)</td>
</tr>
</tbody>
</table>

**Related Topics**

- “Permissions Manager Items: TN5250 Advanced” on page 102

---

104  InfoConnect 2014 User’s Guide
<table>
<thead>
<tr>
<th>Item Name</th>
<th>Sub-group</th>
<th>UI Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AutoIME</td>
<td></td>
<td>Automatically turn the Input Method Editor (IME) on when the cursor is in a double-byte input field, and off when the cursor is in a single-byte input field. When it is not specified, the state of the IME does not change in response to the cursor's location.</td>
</tr>
<tr>
<td>BDTIgnoreScrollLock</td>
<td></td>
<td>Ignore the state of Scroll Lock.</td>
</tr>
<tr>
<td>C370CharSet</td>
<td></td>
<td>Use the C/370 code page. The C/370 code page provides support for square brackets (&quot;[&quot; and &quot;]&quot;).</td>
</tr>
<tr>
<td>CmdPrompt</td>
<td></td>
<td>The character or characters in the terminal window, after which InfoConnect attempts to insert Quick Text.</td>
</tr>
<tr>
<td>ColumnSeparator</td>
<td>Display</td>
<td>Select to use either dots or vertical lines to separate columns.</td>
</tr>
<tr>
<td>CommandLineEnabled</td>
<td></td>
<td>Specify whether the InfoConnect command line can be activated (for example, with the Alt-L keystroke).</td>
</tr>
<tr>
<td>CursorMovementStyle</td>
<td></td>
<td>Specifies how the cursor moves between composed Thai characters.</td>
</tr>
<tr>
<td>CursorProgressionIndicator</td>
<td></td>
<td>Specifies how InfoConnect responds when the host queries to determine if End User Interface (EUI) enhancements are supported by the terminal. Use only for host applications that use cursor progression and queries to determine if EUI is supported.</td>
</tr>
<tr>
<td>DBCSUserDefinedCharacterSource</td>
<td></td>
<td>The location of user-defined character fonts.</td>
</tr>
<tr>
<td>DisplayMargins</td>
<td></td>
<td>Display margins around the terminal window.</td>
</tr>
<tr>
<td>EnableHotspots</td>
<td>Display</td>
<td>Enable all defined hotspots</td>
</tr>
<tr>
<td>EnableQuickText</td>
<td></td>
<td>Use the Quick Text feature.</td>
</tr>
<tr>
<td>EnterKeyRepeat</td>
<td></td>
<td>Specifies whether holding down the Enter key is equivalent to pressing it multiple times.</td>
</tr>
<tr>
<td>ExtendHotSpots</td>
<td></td>
<td>Treat a region to the right of a hotspot as part of the hotspot.</td>
</tr>
<tr>
<td>HorizontalCursorSpeed</td>
<td></td>
<td>Specify how many character spaces to move the cursor, either to the left (on Left Double function), or to the right (on a Right Double function).</td>
</tr>
<tr>
<td>HostBeep</td>
<td></td>
<td>Enable host beep.</td>
</tr>
<tr>
<td>HostCodePage</td>
<td></td>
<td>Host Code page.</td>
</tr>
<tr>
<td>HostControlsOutlineColor</td>
<td></td>
<td>Set the session so that the host determines the color of field outline characters. When cleared, the color of field outline characters can be configured in the Modify Theme dialog box.</td>
</tr>
<tr>
<td>Item Name</td>
<td>Sub-group</td>
<td>UI Description</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>HostCursorBlinkControl</td>
<td></td>
<td>Set a session so that the host controls the cursor blink rate.</td>
</tr>
<tr>
<td>HostNumlockControl</td>
<td></td>
<td>Allows the host to turn NumLock on.</td>
</tr>
<tr>
<td>HostTypeAheadControl</td>
<td></td>
<td>Honor the keyboard buffering control setting in the user AS/400 user profile.</td>
</tr>
<tr>
<td>HotspotsAltKey</td>
<td>Activation</td>
<td>Under Choose key(s) to press in combination with mouse click, activate the Alt key.</td>
</tr>
<tr>
<td>HotspotsCtrlKey</td>
<td>Activation</td>
<td>Under Choose key(s) to press in combination with mouse click, activate the Ctrl key.</td>
</tr>
<tr>
<td>HotspotsDoubleClick</td>
<td>Activation</td>
<td>Under Choose key(s) to press in combination with mouse click, activate the double-click action.</td>
</tr>
<tr>
<td>HotspotsMouseButton</td>
<td>Activation</td>
<td>Choose the mouse button to activate hotspots.</td>
</tr>
<tr>
<td>HotspotsShiftKey</td>
<td>Activation</td>
<td>Under Choose key(s) to press in combination with mouse click, activate the Shift key.</td>
</tr>
<tr>
<td>InputFieldUnderlines</td>
<td></td>
<td>Specify how InfoConnect underlines input fields on host screens.</td>
</tr>
<tr>
<td>InsertArena</td>
<td></td>
<td>Specify the extent to which the InsertProtocol property applies — to a single field, across multiple local fields, or to all unprotected fields.</td>
</tr>
<tr>
<td>InsertProtocol</td>
<td></td>
<td>Specify how a character will be inserted.</td>
</tr>
<tr>
<td>KeyboardAlarmError</td>
<td>Input</td>
<td>Beep when keyboard error is detected.</td>
</tr>
<tr>
<td>KeyboardErrorReset</td>
<td>Input</td>
<td>Keyboard error.</td>
</tr>
<tr>
<td>KeysDuringWait</td>
<td></td>
<td>Specifies whether the user can use the keyboard during a synchronous command. A synchronous command (such as Wait or WaitEvent) causes a procedure to pause until a defined waiting period expires.</td>
</tr>
<tr>
<td>MappedNumlockPreservesNumlock</td>
<td></td>
<td>Specifies how InfoConnect behaves if a user presses the PC NumLock key when it has been mapped to emulate the action of a terminal key.</td>
</tr>
<tr>
<td>MouseShape</td>
<td></td>
<td>Specifies the appearance of the mouse pointer in the terminal window.</td>
</tr>
<tr>
<td>NumberMouseButtons</td>
<td></td>
<td>Specifies the number of buttons in the Mouse Mapper list.</td>
</tr>
<tr>
<td>Item Name</td>
<td>Sub-group</td>
<td>UI Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>PreserveEntryMode</td>
<td></td>
<td>Specifies whether InfoConnect remains in Extended Graphics or Hexadecimal mode indefinitely after you enter either mode. From Extended Graphics mode, you can enter multiple graphics; from Hexadecimal mode, you can enter hexadecimal characters.</td>
</tr>
<tr>
<td>QuickText</td>
<td></td>
<td>The contents of the quick text buffer.</td>
</tr>
<tr>
<td>RestrictedCursor</td>
<td></td>
<td>Restrict the cursor to input fields in the terminal window.</td>
</tr>
<tr>
<td>RightControlKeyRepeat</td>
<td></td>
<td>Designate the right Ctrl key as a modifier key. (A modifier key is used in combination with another key to send a function. For example, Ctrl-F1 is mapped to the Attention key in 3270 sessions).</td>
</tr>
<tr>
<td>ShowAttributesAsHex</td>
<td></td>
<td>Display field attributes in Hexadecimal format.</td>
</tr>
<tr>
<td>ShowBytesRemaining</td>
<td></td>
<td>Display the Show Bytes Remaining indicator on the host status line. This indicator displays the number of bytes remaining in the current field.</td>
</tr>
<tr>
<td>ShowHotspots</td>
<td>Display</td>
<td>Show all defined hotspots.</td>
</tr>
<tr>
<td>ShowOIA</td>
<td></td>
<td>Specifies whether InfoConnect shows operation and status messages in the Operator Information Area (OIA) at the bottom of the terminal window.</td>
</tr>
<tr>
<td>ShowSOSICChars</td>
<td></td>
<td>Specifies whether to show shift-out and shift-in (SO/SI) control characters on the terminal screen. (This helps to determine where double-byte characters or fields begin and end.)</td>
</tr>
<tr>
<td>StatusLine</td>
<td></td>
<td>Specifies the type of host status line for AS/400 terminals.</td>
</tr>
<tr>
<td>SubstituteDisplayChars</td>
<td></td>
<td>Specify whether zeroes should be displayed with a slash (Ø) or without a slash (0).</td>
</tr>
<tr>
<td>SupportDBCSFeatures</td>
<td>Misc.</td>
<td>Support double-byte character sets.</td>
</tr>
<tr>
<td>TextBlinkRate</td>
<td></td>
<td>The rate at which blinking text blinks.</td>
</tr>
<tr>
<td>TypeAhead</td>
<td>Input</td>
<td>Select to buffer characters that are typed in the terminal window. When characters are buffered, they are sent to the host as soon as possible. When characters are not buffered, anything typed while the host is not ready is lost.</td>
</tr>
<tr>
<td>UseCtrlZ</td>
<td></td>
<td>Interprets the Ctrl-Z character as an end-of-file character (when reading a file) or appends the character at the end of a file (when saving a file).</td>
</tr>
</tbody>
</table>
Permissions Manager Items: Clipboard

<table>
<thead>
<tr>
<th>Item Name</th>
<th>Sub-group</th>
<th>UI Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UserDefinedCharactersViatelnet</td>
<td></td>
<td>Send User Defined Character (UDC) requests to the AS/400 host when you are connected through Telnet.</td>
</tr>
<tr>
<td>WordWrapAS400</td>
<td>Input</td>
<td>Enable word wrap.</td>
</tr>
</tbody>
</table>

### Clipboard

<table>
<thead>
<tr>
<th>Item Name</th>
<th>Sub-group</th>
<th>UI Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AutoCopyOnSelect</td>
<td>Copy</td>
<td>Automatically copy selected text.</td>
</tr>
<tr>
<td>BlanksBetweenFields</td>
<td>Copy</td>
<td>Insert blanks between fields (under Use table format).</td>
</tr>
<tr>
<td>ClearSelectionOnCopy</td>
<td>Copy</td>
<td>Clear selection after copying.</td>
</tr>
<tr>
<td>ClipboardPrologue</td>
<td></td>
<td>Configure the macro recorder to add additional, language-specific code to recorded actions placed on the Clipboard.</td>
</tr>
<tr>
<td>ClipboardSyntax</td>
<td></td>
<td>The programming language used when recorded actions are placed on the Clipboard.</td>
</tr>
<tr>
<td>CopyDataSeparation</td>
<td></td>
<td>Specify whether the data copied from InfoConnect should be separated by delimiters at field boundaries or at word boundaries.</td>
</tr>
<tr>
<td>CopyFormatOptions</td>
<td></td>
<td>Specify which file formats to copy from InfoConnect to the clipboard.</td>
</tr>
<tr>
<td>CopyInputFieldsOnly</td>
<td>Copy</td>
<td>Copy input fields only.</td>
</tr>
<tr>
<td>CopyTrailingSpaces</td>
<td>Copy</td>
<td>Copy trailing spaces.</td>
</tr>
<tr>
<td>CutFillCharacter</td>
<td>Cut</td>
<td>Select how you want to fill cut area — with spaces or nulls.</td>
</tr>
<tr>
<td>PasteClearField</td>
<td></td>
<td>Clear all of the previous data remaining in a field after pasting new data into it.</td>
</tr>
<tr>
<td>PasteLineBreak</td>
<td></td>
<td>The character that is actually inserted in a field on the terminal screen when data containing line breaks is copied from the Clipboard.</td>
</tr>
<tr>
<td>PasteMaskProtectedFields</td>
<td></td>
<td>Paste text into unprotected fields.</td>
</tr>
<tr>
<td>PasteReplaceTabs</td>
<td>Paste</td>
<td>The Replace tabs with option that enables the text box used to provide tab replacement.</td>
</tr>
<tr>
<td>PasteTabReplacement</td>
<td>Paste</td>
<td>The text box used to provide tab replacement.</td>
</tr>
<tr>
<td>PasteUsingFieldDelimiters</td>
<td>Paste</td>
<td>Use field delimiters.</td>
</tr>
<tr>
<td>PasteWrapText</td>
<td>Paste</td>
<td>Wrap text to the next input field.</td>
</tr>
<tr>
<td>RectangularSelection</td>
<td></td>
<td>Set text selection so that selected text forms a rectangle (instead of wrapping).</td>
</tr>
</tbody>
</table>
Permissions Manager Items: Hotspots

Index Term
Primary: Permissions Manager
Secondary: hotspots items

Index Term
Primary: Permissions Manager
Secondary: Clipboard items

Hotspots

<table>
<thead>
<tr>
<th>Item Name</th>
<th>Sub-group</th>
<th>UI Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RetainSelection</td>
<td>Copy</td>
<td>Retain selection.</td>
</tr>
<tr>
<td>UseTableFormat</td>
<td>Copy</td>
<td>Use table format.</td>
</tr>
<tr>
<td>HotspotMatchCase</td>
<td></td>
<td>Specifies the case sensitivity for identifying hotspots.</td>
</tr>
<tr>
<td>HotspotOtherDelimiters</td>
<td></td>
<td>Allows uses of additional characters to delineate hotspots. See UseOtherDelimiters.</td>
</tr>
<tr>
<td>HotspotSpaceDelimiter</td>
<td></td>
<td>Delimits hotspots with the space character.</td>
</tr>
<tr>
<td>HotspotStyle</td>
<td></td>
<td>Defines how hotspots are displayed.</td>
</tr>
<tr>
<td>MapFile</td>
<td></td>
<td>The name of the file containing hotspots mappings.</td>
</tr>
<tr>
<td>UseOtherDelimiters</td>
<td></td>
<td>Enables the use of characters defined in setting HotspotOtherDelimiters to delineate hotspots.</td>
</tr>
</tbody>
</table>

Permissions Manager Items: Document Map files

Index Term
Primary: Permissions Manager
Secondary: mapper items

In this Section

- "Permissions Manager Items: Document\Classic" on page 110
- "Permissions Manager Items: Document\Keyboard" on page 110
- "Permissions Manager Items: Document\Mouse" on page 110
- "Permissions Manager Items: Document\Ribbon" on page 110
- "Permissions Manager Items: Document\Theme" on page 110
- "Permissions Manager Items: Productivity\SpellCheck" on page 110
Permissions Manager Items: Document\Classic

Classic

<table>
<thead>
<tr>
<th>Item Name</th>
<th>UI Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MapFile</td>
<td>Restrict the ability of users to modify their UI in the Manage Ribbon dialog box, (when operating in Classic mode).</td>
</tr>
</tbody>
</table>

Permissions Manager Items: Document\Keyboard

Keyboard

<table>
<thead>
<tr>
<th>Item Name</th>
<th>UI Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MapFile</td>
<td>Restrict the ability of users to select or modify a keyboard map.</td>
</tr>
</tbody>
</table>

Permissions Manager Items: Document\Mouse

Mouse

<table>
<thead>
<tr>
<th>Item Name</th>
<th>UI Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MapFile</td>
<td>Restrict the ability of users to select or modify a mouse map.</td>
</tr>
</tbody>
</table>

Permissions Manager Items: Document\Ribbon

Ribbon

<table>
<thead>
<tr>
<th>Item Name</th>
<th>UI Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MapFile</td>
<td>Restrict the ability of users to select or modify a Ribbon.</td>
</tr>
</tbody>
</table>

Permissions Manager Items: Document\Theme

Theme

<table>
<thead>
<tr>
<th>Item Name</th>
<th>UI Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MapFile</td>
<td>Restrict the ability of users to select or modify a theme.</td>
</tr>
</tbody>
</table>

Permissions Manager Items: Productivity\SpellCheck

Spell Check

<table>
<thead>
<tr>
<th>Item Name</th>
<th>UI Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AutoCorrect</td>
<td>Commonly misspelled words are corrected without prompt or indication as you type.</td>
</tr>
<tr>
<td></td>
<td>NOTE: This feature is available only for English.</td>
</tr>
<tr>
<td>CheckSpellingAsType</td>
<td>Spell Check marks possible errors with wavy underlines.</td>
</tr>
<tr>
<td>Item Name</td>
<td>UI Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CorrectCapsLock</td>
<td>If you accidentally type a word in Title Case with the CAPS LOCK key turned on, Spell Check corrects the capitalization; for example, eNTER kEY changes to Enter Key.</td>
</tr>
<tr>
<td>CorrectTwoInitialCaps</td>
<td>If you type two consecutive uppercase letters at the beginning of a word, Spell Check changes the second uppercase letter to a lowercase letter; for example, ENTER changes to Enter.</td>
</tr>
<tr>
<td>CustomDictionary</td>
<td>The path to the custom dictionary file.</td>
</tr>
<tr>
<td>IgnoreAllUppercase</td>
<td>If you are typing in UPPERCASE letters, Spell Check does not attempt to correct spelling.</td>
</tr>
<tr>
<td>IgnoreWordsWithNumbers</td>
<td>If you are typing a word with a number in it, like UrsaMajorM51, Spell Check does not attempt to correct the spelling.</td>
</tr>
<tr>
<td>MaxSuggestions</td>
<td>The number of suggested spellings to offer when a misspelled word is encountered.</td>
</tr>
<tr>
<td>MaxWordLength</td>
<td>The longest word checked for spelling. Longer words are ignored by the spell checker.</td>
</tr>
<tr>
<td>MinimumMatch</td>
<td>The shortest field in which to check spelling.</td>
</tr>
</tbody>
</table>

The User Interface

Permissions Manager Items: Productivity

Index Term
Primary: Permissions Manager
Secondary: productivity tool items

Productivity

<table>
<thead>
<tr>
<th>Item Name</th>
<th>Sub-group</th>
<th>UI Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AutoCompleteEnabled</td>
<td></td>
<td>Enable or disable the Auto Complete feature.</td>
</tr>
<tr>
<td>AutoExpandEnabled</td>
<td></td>
<td>Enable or disable the Auto Expand feature.</td>
</tr>
<tr>
<td>RecentTypingEnabled</td>
<td></td>
<td>Enable or disable the Recent Typing feature.</td>
</tr>
<tr>
<td>SpellCheckEnabled</td>
<td></td>
<td>Enable or disable the Spell Check feature.</td>
</tr>
</tbody>
</table>
Permissions Manager Items: Productivity\ScreenHistory

<table>
<thead>
<tr>
<th>Item Name</th>
<th>Sub-group</th>
<th>UI Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ClearHistoryOnClose</td>
<td></td>
<td>Delete when the session is disconnected for any reason.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>NOTE:</strong> If the screen history has been saved to a file, the screen history file is not affected.</td>
</tr>
<tr>
<td>ManualCaptureOnly</td>
<td></td>
<td>Capture screens only when manual captures are performed.</td>
</tr>
<tr>
<td>MaxScreen</td>
<td></td>
<td>The maximum number of screens to record and keep at any one time in the current session's screen history.</td>
</tr>
</tbody>
</table>

Permissions Manager Items: Productivity\RecentTyping

<table>
<thead>
<tr>
<th>Item Name</th>
<th>Sub-group</th>
<th>UI Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ClearListOnClose</td>
<td></td>
<td>The Recent Typing list is deleted when the session is disconnected for any reason.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>NOTE:</strong> If the Recent Typing list has been saved to a file, the recent typing file is not affected.</td>
</tr>
<tr>
<td>MaxListItems</td>
<td></td>
<td>The maximum number of words to remember.</td>
</tr>
<tr>
<td>MinimumMatch</td>
<td></td>
<td>The number of characters that InfoConnect considers a word.</td>
</tr>
</tbody>
</table>

Permissions Manager Items: Productivity\Office

<table>
<thead>
<tr>
<th>Item Name</th>
<th>Sub-group</th>
<th>UI Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CloseOfficeDocs</td>
<td></td>
<td>Close Office documents when exiting InfoConnect. If the documents are not saved, Office prompts you to save them before closing.</td>
</tr>
<tr>
<td>PresentationTemplateFile</td>
<td></td>
<td>The default presentation template file.</td>
</tr>
<tr>
<td>WordProcessingTemplateFile</td>
<td></td>
<td>The default word-processing template file.</td>
</tr>
</tbody>
</table>
Permissions Manager Items: Productivity\AutoExpand

Productivity\AutoExpand

<table>
<thead>
<tr>
<th>Item Name</th>
<th>Sub-group</th>
<th>UI Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AutoExpandOverwrite</td>
<td></td>
<td>Overwrite only the data that exists where the Auto Expand definition is being placed — other data in the field is not affected.</td>
</tr>
<tr>
<td>CaseSensitive</td>
<td></td>
<td>Use case sensitivity when expanding.</td>
</tr>
<tr>
<td>ExpandAndContinue</td>
<td></td>
<td>Wrap text into next field.</td>
</tr>
</tbody>
</table>

Permissions Manager Items: Productivity\AutoComplete

Productivity\AutoComplete

<table>
<thead>
<tr>
<th>Item Name</th>
<th>Sub-group</th>
<th>UI Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AllScreenData</td>
<td></td>
<td>Make suggestions based on all user data that has been entered into any field used during the session.</td>
</tr>
<tr>
<td>AutoCompleteOverwrite</td>
<td></td>
<td>Overwrite only the data that exists where the Auto Complete suggestion is being placed. Other data in the field is not affected.</td>
</tr>
<tr>
<td>CaseSensitive</td>
<td></td>
<td>Use case sensitivity for suggestions.</td>
</tr>
<tr>
<td>CompleteAndContinue</td>
<td></td>
<td>If the Auto Complete suggestion pushes existing data past the end of the field, the additional data is added at the beginning of the next available field.</td>
</tr>
<tr>
<td>MaxSuggestions</td>
<td></td>
<td>The maximum number of items you want Auto Complete to suggest for any word.</td>
</tr>
<tr>
<td>MaxWordLength</td>
<td></td>
<td>The longest word on which to apply Auto Complete. Longer words are ignored.</td>
</tr>
<tr>
<td>MinimumMatch</td>
<td></td>
<td>The number of characters typed before suggestions are made.</td>
</tr>
<tr>
<td>PersistData</td>
<td></td>
<td>Auto Complete &quot;remembers&quot; the data entered during the current session, so that if the session is closed, and then reopened, suggestions will still be available.</td>
</tr>
</tbody>
</table>

Permissions Manager Items: Application Workspace

Index Term
Primary: Permissions Manager
Secondary: application workspace items

In this Section
- “Permissions Manager Items: Application Access\API Security” on page 114
- “Permissions Manager Items: Application Access\Application Options” on page 114
- “Permissions Manager Items: Application Access\Application Sounds” on page 115
Permissions Manager Items: Application Access\API Security

API Security

<table>
<thead>
<tr>
<th>Item Name</th>
<th>Sub-group</th>
<th>UI Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ChannelType</td>
<td></td>
<td>Prevent custom applications from accessing InfoConnect.</td>
</tr>
<tr>
<td>LegacyCOM</td>
<td></td>
<td>The legacy API used for the GetObject() method to retrieve API COM objects — No Legacy API, InfoConnect, or EXTRA!.</td>
</tr>
<tr>
<td>RequiredUACForRestrictedAction</td>
<td></td>
<td>Require UAC elevation when a restricted action is invoked by a macro or API call.</td>
</tr>
</tbody>
</table>

Permissions Manager Items: Application Access\Application Options

Application Options

<table>
<thead>
<tr>
<th>Item Name</th>
<th>Sub-group</th>
<th>UI Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ApplicationStartup</td>
<td></td>
<td>Specifies which dialog box, if any, to display when InfoConnect starts.</td>
</tr>
<tr>
<td>ClearClipboardOnExit</td>
<td></td>
<td>Any data that may have been copied to the Clipboard is cleared when the workspace is closed.</td>
</tr>
<tr>
<td>CustomHelpSystemURL</td>
<td></td>
<td>The URL to use for Help.</td>
</tr>
<tr>
<td>DefaultSettingsLocalPath</td>
<td></td>
<td>The path for the default directory in which session and other documents are saved.</td>
</tr>
<tr>
<td>HelpSystem</td>
<td></td>
<td>Specify whether to use the product Help as it appears on the Attachmate Web site or the Help installed on your local machine.</td>
</tr>
<tr>
<td>HideBuiltInTemplates</td>
<td></td>
<td>Display only user-defined templates from the Create New Document dialog box.</td>
</tr>
<tr>
<td>Logging</td>
<td></td>
<td>Send error information to the Windows logging service.</td>
</tr>
<tr>
<td>OptimizeRemoteSession</td>
<td></td>
<td>Turn off cursor blinking and disable the splash screen when running InfoConnect under Citrix or WTS.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NOTE: This setting is ignored if you are not running under Citrix or WTS;</td>
</tr>
<tr>
<td>SessionShutdown</td>
<td></td>
<td>Specify what you want done with any changed settings when you close a document.</td>
</tr>
</tbody>
</table>
### Permissions Manager: Application Access\Application Sounds

<table>
<thead>
<tr>
<th>Item Name</th>
<th>Sub-group</th>
<th>UI Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Events</td>
<td></td>
<td>Map events to sound files.</td>
</tr>
</tbody>
</table>

### Permissions Manager: Application Access\PCI DSS

**PCI DSS**

<table>
<thead>
<tr>
<th>Item Name</th>
<th>Sub-group</th>
<th>UI Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ConnectionToUseSecureProtocol</td>
<td></td>
<td>Specify whether to require secure connections. Security can be required for all connections or for only wireless connections.</td>
</tr>
<tr>
<td>ExceptionRegularExpressions</td>
<td></td>
<td>Define exception expressions that filter out false PAN detections. These only apply when the Reflection PAN detection method is used.</td>
</tr>
<tr>
<td>NeedRaiseEvent</td>
<td></td>
<td>Specify whether API events occur when a user views a credit card Primary Account Number (PAN).</td>
</tr>
<tr>
<td>PrecedingKnownStrings</td>
<td></td>
<td>Define a list of text keywords that precede PANs. These only apply when the Detect PANs based on preceding text method is selected.</td>
</tr>
<tr>
<td>RecognitionStyle</td>
<td></td>
<td>Specify which type of PAN Detection to use.</td>
</tr>
<tr>
<td>RedactionRules</td>
<td></td>
<td>Choose to redact data on the screen after it is entered or as it is typed.</td>
</tr>
<tr>
<td>RedactStyle</td>
<td></td>
<td>Specify how many digits of the PAN to redact.</td>
</tr>
<tr>
<td>RegularExpressions</td>
<td></td>
<td>Define additional detection rules with regular expressions. These only apply when the Reflection PAN detection method is used.</td>
</tr>
<tr>
<td>StoreTypedPANs</td>
<td></td>
<td>Determine whether or not PAN data are stored.</td>
</tr>
</tbody>
</table>
## Permissions Manager Items: Application Access\Privacy Filter

**Privacy Filter**

<table>
<thead>
<tr>
<th>Item Name</th>
<th>Sub-group</th>
<th>UI Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MapFile</td>
<td></td>
<td>The list of privacy filters.</td>
</tr>
<tr>
<td>Redaction Rules</td>
<td></td>
<td>Specify how data affected by Privacy Filters will be redacted.</td>
</tr>
</tbody>
</table>

## Permissions Manager Items: Application Access\TrustedLocations

**TrustedLocations**

<table>
<thead>
<tr>
<th>Item Name</th>
<th>Sub-group</th>
<th>UI Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AllowNetwork</td>
<td></td>
<td>Permit network paths to be included in the list of trusted locations.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>NOTE:</strong> This is not recommended.</td>
</tr>
<tr>
<td>TrustAllLocations</td>
<td></td>
<td>Open files only from trusted locations.</td>
</tr>
<tr>
<td>TrustedLocations</td>
<td></td>
<td>The list of trusted locations.</td>
</tr>
</tbody>
</table>

## Permissions Manager Items: Application Access\UX Configuration

**UX Configuration**

<table>
<thead>
<tr>
<th>Item Name</th>
<th>Sub-group</th>
<th>UI Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CloseButtonOnTab</td>
<td></td>
<td>Specifies to display a Close button on each document tab.</td>
</tr>
<tr>
<td>DocumentLayout</td>
<td></td>
<td>Specifies how to display documents in the workspace — using tabs (the default), or as windows that you can tile or cascade.</td>
</tr>
<tr>
<td>Language</td>
<td></td>
<td>The language you want to use for the UI — the menus, dialog boxes, and Help when you start a new session.</td>
</tr>
<tr>
<td>MaxRecentDocuments</td>
<td></td>
<td>The maximum number of recently used documents to display in the Recent Documents list on the &quot;Workspace Menu&quot; on page 891.</td>
</tr>
<tr>
<td>ShowDocumentSwitcher</td>
<td></td>
<td>When selected, pressing the Ctr+Tab displays a document switcher that can be used to tab through the open documents.</td>
</tr>
<tr>
<td>ShowHelp</td>
<td></td>
<td>Displays the Help icon and menu on the Ribbon.</td>
</tr>
<tr>
<td>ShowQuickAccessToolbar</td>
<td></td>
<td>Displays the Quick Access Toolbar on the Ribbon or Browser.</td>
</tr>
<tr>
<td>ShowSearch</td>
<td></td>
<td>Displays the Search box on the Ribbon.</td>
</tr>
<tr>
<td>ShowStartPage</td>
<td></td>
<td>Displays a gallery of recent documents.</td>
</tr>
</tbody>
</table>
Permissions Manager Items: VT terminal

Index Term
Primary: Permissions Manager
Secondary: VT items

In this Section

- “Permissions Manager Items: VT terminal\Document\Clipboard” on page 117
- “Permissions Manager Items: VT terminal\Document\Connection” on page 117
- “Permissions Manager Items: VT terminal\Document\Terminal” on page 119
- “Permissions Manager Items: VT terminal\Document\Safeguards” on page 120

Permissions Manager Items: VT terminal\Document\Clipboard

Document\Clipboard

<table>
<thead>
<tr>
<th>Item Name</th>
<th>Sub-group</th>
<th>UI Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PasteBufferSize</td>
<td></td>
<td>The size of a &quot;paste block,&quot; which is the number of characters pasted from the Clipboard to the terminal window before a pause occurs.</td>
</tr>
<tr>
<td>PasteDelay</td>
<td></td>
<td>The time interval (in tenths of a second) that InfoConnect waits between &quot;paste blocks&quot; when pasting data from the Clipboard into display memory.</td>
</tr>
</tbody>
</table>

Permissions Manager Items: VT terminal\Document\Connection

Document\Connection

<table>
<thead>
<tr>
<th>Item Name</th>
<th>Sub-group</th>
<th>UI Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baud</td>
<td></td>
<td>The rate at which InfoConnect transmits and receives data through the selected serial port.</td>
</tr>
<tr>
<td>ConnectionMethod</td>
<td></td>
<td>Determines how the session connects to the host (Network, Serial Port, Modem). This setting is used in conjunction with ConnectionType.</td>
</tr>
</tbody>
</table>

ShowSuggestion
Displays search suggestions when you type in the Search box. (This applies only to Browser mode.)

TabStripLocation
Where to display the document tabs — at the top (default), bottom, left, or right.

WindowLookAndFeel
The user interface mode— Ribbon, (the default), Browser, Classic, or TouchUx.

WindowTheme
The color scheme to use.
### Item Name | Sub-group | UI Description
---|---|---
ConnectionType |  | Determines how the session connects to the host (Telnet, Secure Shell, Rlogin). This setting is used in conjunction with ConnectionMethod.
ConnectMacro |  | Run the connection action when the session initially connects to a host.
Host |  | The name of the host to which to connect.
ModemAdvancedSettingsDialog |  | The More Settings Modem dialog box. Restricting access to this setting limits user access to this dialog box when a session is configured for a modem connection.
ModemAreaCode |  | The area code (or city code) of the number being dialed.
ModemCountryName |  | The country of the number being dialed.
ModemDialingPropertiesDialog |  | The Phone and Modem Options dialog box. Restricting access to this setting limits user access to this dialog box when a session is configured for a modem connection.
ModemLocation |  | The current modem location. Modem locations are configured using the Control Panel tool.
ModemName |  | The type of modem being used.
ModemPhoneNumber |  | The phone number you want the modem to dial when connecting. The number must adhere to the rules of your modem.
ModemUserDialingRules |  | Set the TAPI modem dialer to add appropriate dialing prefixes to the number you are dialing, based on the current values of ModemAreaCode, ModemCountryName, and ModemLocation. When cleared, the modem dialer dials the phone number exactly as specified by ModemPhoneNumber.
NetworkAdvancedSettingsDialog |  | The More Settings - Network dialog box. Restricting access to this setting limits user access to this dialog box when a session is configured for a network connection.
NetworkSecurityDialog |  | The Security Properties dialog box. Restricting access to this setting limits user access to this dialog box when a session is configured for a network connection.
Parity |  | The parity for data transmission to and from the serial device on this port.

To use the multinational character set or 8-bit controls, Parity must be set to one of the values that offers 8-bit controls. If your communications link generates parity, and you set Parity to 8/None, multinational characters appear on your screen. In this case, set Parity to either 8/Even or 8/Odd.
Permissions Manager Items: VT terminal\Document\Terminal

<table>
<thead>
<tr>
<th>Item Name</th>
<th>Sub-group</th>
<th>UI Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AutoResizeScreen</td>
<td></td>
<td>Automatically resize the terminal window to accommodate the data being displayed.</td>
</tr>
<tr>
<td>CompressBlankLines</td>
<td></td>
<td>Specify whether to save room in display memory by compressing multiple blank lines into a single blank line.</td>
</tr>
<tr>
<td>DisplayColumns</td>
<td></td>
<td>Display the number of columns in the complete terminal display.</td>
</tr>
<tr>
<td>DisplayMemoryBlocks</td>
<td></td>
<td>The number of 8K memory blocks to allocate for display memory.</td>
</tr>
<tr>
<td>DisplayRows</td>
<td></td>
<td>Display the number of rows in the complete terminal display.</td>
</tr>
<tr>
<td>EnableHotspots</td>
<td></td>
<td>Enable all defined hotspots.</td>
</tr>
<tr>
<td>GraphicsTerminal</td>
<td></td>
<td>Emulate a graphics terminal.</td>
</tr>
<tr>
<td>HotspotsAltKey</td>
<td>Activation</td>
<td>Under <strong>Choose key(s) to press in combination with mouse click</strong>, activate the Alt key.</td>
</tr>
<tr>
<td>HotspotsCtrlKey</td>
<td>Activation</td>
<td>Under <strong>Choose key(s) to press in combination with mouse click</strong>, activate the Ctrl key.</td>
</tr>
<tr>
<td>HotspotsDoubleClick</td>
<td>Activation</td>
<td>Under <strong>Choose key(s) to press in combination with mouse click</strong>, activate the double-click action.</td>
</tr>
<tr>
<td>HotspotsMouseButton</td>
<td>Activation</td>
<td>Choose the mouse button to activate hotspots.</td>
</tr>
</tbody>
</table>

The communications port to which your target serial device is connected.
Run the macro when the session initially connects to a host, and every time it reconnects to the host.

The **More Settings - Serial Port** dialog box. Restricting access to this setting limits user access to this dialog box when a session is configured for a Serial Port connection.

The serial port to use when connecting to the host via a serial port connection.

The SSH configuration scheme settings to use to make a Secure Shell connection.

A name that identifies you or your PC to the host.
Permissions Manager Items: VT terminal\Document\Safeguards

Document\Safeguards

<table>
<thead>
<tr>
<th>Item Name</th>
<th>Sub-group</th>
<th>UI Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CacheSecureShellUserName</td>
<td></td>
<td>Temporarily stores the user name entered for a Secure Shell session until the Reflection workspace is closed. (When selected, users are not prompted for a user name when they reconnect unless they reopen the workspace.)</td>
</tr>
<tr>
<td>ClearDisplayOnDisconnect</td>
<td></td>
<td>Delete all data from display memory when a session is disconnected from the host.</td>
</tr>
<tr>
<td>SaveSecureShellUserName</td>
<td></td>
<td>Save the user name when users save their settings files, or record a macro.</td>
</tr>
</tbody>
</table>

The User Interface

With InfoConnect 2014, you can display sessions in four types of user interface modes: Ribbon, Browser, TouchUx, and Classic.
To select the interface type

1. Open the Reflection Workspace Settings dialog box. The steps depend on your user interface mode (page 120).

User Interface Mode | Steps
--- | ---
Reflection Browser | On the Reflection menu, choose Settings and then Reflection Workspace Settings.
TouchUx | Tap the Gear icon and then select Reflection Workspace Settings.

2. Click Configure User Interface to open the User Interface dialog box.
3. In the User interface mode list, select the type of interface that you want to use.
4. To select a look and feel for the Ribbon or TouchUx interfaces, choose from the options in the Look and Feel / Color scheme list.
5. Close and reopen the workspace.

The Ribbon

The Ribbon interface shares the look and feel of Microsoft Windows 7 and Office 2010. In the area between the Quick Access toolbar (the toolbar in the upper-left corner) and the document window is the Ribbon, a dynamic, collapsible device that organizes commands, buttons, and other controls on tabs for each task area. Double-click any tab in the Ribbon to hide or show the Ribbon. Or, if you prefer, you can map a keyboard shortcut to show or hide the Ribbon with a keystroke. Sessions using the default 3270 or 5250 keyboard map already have this action mapped to CTRL+F1.

The Browser

The Browser interface has a look and feel that is similar to the latest Web browsers. You can access commands from the InfoConnect menu or from the Quick Access Toolbar. You can also access commands by searching for them in the search box and then clicking on the search results.
**TouchUx**

The TouchUx interface provides the InfoConnect TouchUx user experience. InfoConnect runs on Microsoft Windows devices or other devices (Apple iPad or Android) that are accessing sessions running on a Citrix server. This mode includes an on-screen terminal keyboard that can be set as a transparent overlay or docked in a separate pane.

**Classic**

A Classic interface option provides an interface that is familiar to users of previous versions of InfoConnect. This mode is recommended only if you are upgrading from a previous version. When using the Classic UI, only one document can be open in a workspace, and other features may not be available.

## Create New Document Dialog Box

Index Term  
Primary: user-defined session templates

Index Term  
Primary: sessions  
Secondary: user-defined

Index Term  
Primary: new  
Secondary: Create New Document dialog box

Index Term  
Primary: Create New Document dialog box  
Secondary: Create New Document dialog box

Index Term  
Primary: compatibility setting

### Getting there

The steps depend on your user interface mode (page 120).

**User Interface Mode**  
**Steps**

Ribbon or InfoConnect Browser  
From the Quick Access Toolbar, click the New Document button.

TouchUx  
Tap the Folder icon and then under File, select New.

InfoConnect provides several templates to help you start sessions and create Web page and other documents. Terminal session documents and Web page documents open in a tab in the workspace. Printer session documents open in a separate window.
**Built-in templates**

Built-in templates are provided with InfoConnect.

- **3270 terminal**: Select to create a mainframe terminal session.
- **5250 terminal**: Select to create an AS/400 terminal session.
- **3270 printer**: Select to create a mainframe printer session.
- **5250 printer**: Select to create an AS/400 printer session.
- **VT terminal**: Select to create a UNIX, OpenVMS, or Regis Graphics terminal session.
- **Web**: Select to access a Web page using the default browser.

**User defined**

User-defined templates are created when you save a document as a template.

**Compatibility**

Select the set of default settings to use when creating a terminal session document. The compatibility settings include keyboard maps and themes similar to those of other emulation products. The default InfoConnect compatibility setting is optimized for this product.

**Related Topics**

- “Create a Session Document File” on page 147
- “Stop Showing the Create New Document Dialog Box” on page 59
- “Share Sessions as Templates” on page 149
- “Open a Web Session” on page 315

---

**Change the UI Language**

**Index Term**

Primary: user interface  
Secondary: language

**Index Term**

Primary: localized UI

**Index Term**

Primary: language  
Secondary: setting for the UI

By default, InfoConnect uses the same language as the operating system to display text within the Ribbon user interface, dialog boxes, and the workspace. You can change the language for this text if you installed additional languages with InfoConnect, and if your operating system supports it.

**To select a different language**

1. Open the InfoConnect Workspace Settings dialog box.  
   The steps depend on your user interface mode (page 120).
Under Workspace Settings, click **Configure User Interface**.

In the **User interface language** list, choose the language to which you want to change.

**NOTE:** Changes you make to the Ribbon are specific to the language selected when changes are made; for example, if you create a custom Ribbon when Spanish is selected for the user interface, that Ribbon is available only when the user interface is viewed in Spanish.

**Related Topics**
- “Configure Workspace Defaults Dialog Box” on page 125

**InfoConnect Workspace Settings Dialog Box**

**Getting there**
- Open the InfoConnect Workspace Settings dialog box.

The steps depend on your **user interface mode** (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reflection Browser</td>
<td>On the Reflection menu, choose Settings and then Reflection Workspace Settings.</td>
</tr>
<tr>
<td>TouchUx</td>
<td>Tap the Gear icon and then select Reflection Workspace Settings.</td>
</tr>
</tbody>
</table>

Workspace configuration settings affect all terminal session and Web page documents opened in InfoConnect. These settings include security, user interface options, file locations, and other settings related to InfoConnect.

**NOTE:** These settings are applied only after the workspace is closed and reopened.
Trust Center

Specify Trusted Locations Set up trusted locations (directories that are designated as secure sources for opening files). By default, InfoConnect allows you to open documents only in directories that are specified as trusted locations in the InfoConnect settings.

Set Up Information Privacy Configure Information Privacy features to protect sensitive data so that it is not displayed on the screen or in productivity features, such as Screen History.

Set Up API and Macro Security Enable the InfoConnect .NET API, and specify corresponding settings.

Workspace Settings

Configure Workspace Defaults Configure the actions to perform when the InfoConnect workspace opens or closes and preferences for automatically saving session document files.

Configure Workspace Attributes Configure options for logging, running remote sessions, and displaying Help. You can also specify the user data directory, in which session documents and other related files are saved.

Configure User Interface Configure which type of user interface to use (InfoConnect provides four interfaces), its look and feel, and other user interface options.

Configure Workspace Defaults Dialog Box

Index Term
Primary: workspace
Secondary: configuring

Index Term
Primary: Windows Terminal Server (WTS)

Index Term
Primary: Windows logging service

Index Term
Primary: user interface
Secondary: global preferences

Index Term
Primary: user interface
Secondary: classic mode

Index Term
Primary: user data directory

Index Term
Primary: tabs
Secondary: location in UI window

Index Term
Primary: startup settings

Index Term
Primary: Ribbon
Secondary: UI setting
Getting there

1. Open the Reflection Workspace Settings dialog box. The steps depend on your user interface mode (page 120).

   **User Interface Mode** | **Steps**
   --- | ---
   Reflection Browser | On the Reflection menu, choose Settings and then Reflection Workspace Settings.
   TouchUx | Tap the Gear icon and then select Reflection Workspace Settings.

2. Click Configure Workspace Attributes.

Configure the actions to perform when the InfoConnect workspace opens or closes and preferences for automatically saving session document files.
## Workspace

### When starting workspace
Specify whether to display the New or Open dialog box or to run an action when InfoConnect starts.

**NOTE:** When a workspace is opened by double-clicking on a session document file, this setting is not applied. (The workspace opens without displaying a dialog box or running an action.)

<table>
<thead>
<tr>
<th>Select this</th>
<th>To do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show New dialog</td>
<td>Display the New dialog box used to choose which type of session to configure.</td>
</tr>
<tr>
<td>Show Open dialog</td>
<td>Display the Open dialog box used to choose a session document file.</td>
</tr>
<tr>
<td>Show nothing</td>
<td>Open the workspace without displaying a dialog box.</td>
</tr>
<tr>
<td>Run Startup action</td>
<td>Set up an action (for example, a startup macro) that is performed when InfoConnect starts.</td>
</tr>
</tbody>
</table>

### Select Action
Open the Select Action dialog box used to specify actions (available only when Run Startup Action is selected).

### When closing a document
Specify what you want done with any changed settings when you close a document.

<table>
<thead>
<tr>
<th>Select this</th>
<th>To do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save document settings automatically</td>
<td>Save the modified version of the session document and any related files without any additional prompt. If one of the modified files is a built-in file, a copy of the built-in file is saved in your user data directory.</td>
</tr>
<tr>
<td>Ask me to save document settings</td>
<td>Specify where to save the modified version of the session document and any related files at the time you choose to create it.</td>
</tr>
<tr>
<td>Discard document settings</td>
<td>Discard any changes to the session document and any related files.</td>
</tr>
</tbody>
</table>

### Show Start Page after workspace opens
Displays a gallery of recent documents.

### Exit workspace when last document closed
Automatically exit InfoConnect after the last document (session or Web page) in the workspace is closed.

### Clear clipboard when closing workspace
When selected, any data that may have been copied to the Clipboard is cleared when the workspace is closed.

### Hide built-in templates for new documents
When selected, only user-defined templates are available from the Create New Document dialog box.

### Show Document Switcher with Ctr+Tab
When selected, pressing the Ctr+Tab displays a document switcher that can be used to tab through the open documents.

### Open documents in same workspace
When sessions are opened by double-clicking on session document files, the sessions all open in the same workspace.
Recent Documents

Maximum number of Recent Documents to show  Specify the maximum number of recently used documents to display in the Recent Documents list on the "Workspace Menu" on page 891.
Clear Recent Documents List  Click to remove all documents from the list.

Related Topics

- “Configure Color Settings” on page 35
- “Change the UI Language” on page 123
- “The User Interface” on page 65
- “Manage Themes Dialog Box” on page 132

Configure Workspace Attributes Dialog Box

Getting there

1. Open the Reflection Workspace Settings dialog box.
   The steps depend on your user interface mode (page 120).

   User Interface Mode  Steps
   Reflection Browser  On the Reflection menu, choose Settings and then Reflection Workspace Settings.
   TouchUX  Tap the Gear icon and then select Reflection Workspace Settings.

2. Click Configure Workspace Attributes.

You can configure options for logging, running remote sessions, and displaying Help. You can also specify the user data directory, in which session documents and other related files are saved.

Logging

Enable event logging  Select to send error information to the Windows logging service.

Remote Session

Optimize Citrix and WTS sessions  Select to turn off cursor blinking and disable the splash screen when running InfoConnect under Citrix or WTS.

NOTE: This setting is ignored if you are not running under Citrix or WTS.
Help System

When displaying help
Specify whether to use the product Help as it appears on the Attachmate Web site or the Help installed on your local computer.

If the Help system you specify is not available, InfoConnect will use the other one.

Show Help on Ribbon
Displays the Help icon and menu on the Ribbon.

Directories

Default user data directory
Type the path for the default directory in which session and other documents are saved, or click Browse to locate it. All Open and Save As dialog boxes default to this directory (including, for example, screen history and scratch pad files).

NOTE: To reopen the file later, it must be saved in a trusted location.

Default legacy EXTRA! directory
Type or browse to the default directory in which to save legacy EXTRA! macros or other legacy files, such as quickpads.

Configure User Interface Dialog Box

Getting there

1. Open the InfoConnect Workspace Settings dialog box.
   The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reflection Browser</td>
<td>On the Reflection menu, choose Settings and then Reflection Workspace Settings.</td>
</tr>
<tr>
<td>TouchUx</td>
<td>Tap the Gear icon and then select Reflection Workspace Settings.</td>
</tr>
</tbody>
</table>

2. Click Configure User Interface.

You can configure which type of user interface to use (InfoConnect provides four interfaces), its look and feel, and other user interface options. You can also specify sounds to play when InfoConnect opens or closes.
UI Preferences

**NOTE:** If you change this setting after configuring a session, the appearance of that session may be unpredictable.

**User interface mode**

**Ribbon** is the default UI for InfoConnect. It provides a user experience similar to the most recent Office applications, including features such as super ToolTips and Ribbon galleries.

When using the Ribbon, you can have more than one document open in the same workspace. Tabs allow you to see which documents are open, and to change between documents.

**Classic** provides the familiar menu and toolbar interface. When using the Classic UI, only one document can be open in a workspace, and other features may not be available.

**NOTE:** All of the Help procedures are written for the Ribbon, the Browser, or TouchUX.

**Browser** provides a "minimalist" look and feel that is similar to the latest Web browsers. Multiple documents are displayed in tabs.

**TouchUX** provides a touchscreen user experience. (You can run InfoConnect natively on Microsoft Windows 8 devices. For iOS or Android devices, you must access InfoConnect through a Citrix XenApp server, with the Citrix Receiver client software installed on the device. InfoConnect only supports versions of Citrix software that Citrix currently supports.

**Look and Feel / Color scheme**

Select the base color for the application and Ribbon background. The color scheme does not affect your host screen, only the frame around it. To change the colors of the host screen, choose a different theme.

When the Ribbon mode is selected, you can configure your workspace with two different types of "look and feel" settings that provide different ways to access the “Workspace Menu” on page 891.

With the "Office 2007" look and feel, you use the Reflection button  to access the workspace menu.

![Reflection button](image)

With the "Office 2010" look and feel, you use the Reflection File menu to access the workspace menu.

![Reflection File menu](image)

When TouchUX mode is selected, you can choose an operating system look and feel (iOS, Android, or Windows). This look and feel changes only the colors and style of the display. It does not affect functionality.

For the Windows look and feel, you can select whether to to open InfoConnect in Full Screen mode.
Documents in the workspace are displayed in tabs by default. If you are using the InfoConnect Ribbon, you can choose to display them in windows that can be tiled or cascaded.

Specify whether to display document tabs at the top (default), bottom, left, or right.

Select to display the Help button and menus on the Ribbon.

Clear to remove the Close button from the document tabs. Individual document tabs can still be closed using the Close button at the end of the tab strip.

Select to display the Search box on the Ribbon.

Select to display the Quick Access Toolbar on the Ribbon or the Browser.

Select to display search suggestions when you type in the Search box. (This applies only to Browser mode.)

Select to hide the F1 Help link that is displayed on tooltips by default.

Select the language you want to use for the InfoConnect UI.

Select the application event with which to associate a sound.

The sound file played when the associated application event occurs.

Click to locate a sound file to associate with application events.

Play the sound file associated with the selected application event.

Manage On-Screen Keyboard Settings

Getting there

1. On the InfoConnect menu, tap the Gear icon and then select Document Settings.
2. Under Input Devices, click Manage On-Screen Keyboard.

Use the Manage On-Screen Keyboard dialog box to set up the keyboard options for the TouchUx user interface mode:

- Under Keyboard Options, you can set different keyboard mode options for portrait and landscape orientations.
- Transparent displays the keyboard as a transparent overlay on the session window. You can set the transparency level.
- Docked displays the keyboard in a separate pane at the bottom of the screen. The session window pane is resized to allow for the additional pane.

You can also select whether to use the device keyboard or the built-in InfoConnect terminal keyboard provided for the type of session you are running.
Manage Themes Dialog Box

Getting there

1. Open a terminal session.
   - The steps depend on your user interface mode (page 120).

2. Under Terminal Appearance, click Manage Themes.

Theme files control the colors, shape of the cursor, and other details about the appearance of your terminal sessions. When you create a terminal session document, it includes a pointer to a default, built-in theme file. You can choose a different theme file for each session, and create custom theme files with the settings you prefer.

Select another theme file
   - Click to choose a different theme file from a list of existing theme files. The file must be in a trusted location.

Modify the currently selected theme file
   - Select to modify the theme file used by this session. Because built-in files are read-only, if the currently selected file is a built-in file, it will be saved as a custom file when you change it.

Create a new theme from an existing file
   - Click to create a custom theme file based on an existing theme file. To reopen the file later, it must be saved in a trusted location.

Related Topics

- “Modify Theme Dialog Box (3270 Terminal Sessions)” on page 133
- “Modify Theme Dialog Box (5250 Terminal Sessions)” on page 136
- “Modify Theme Dialog Box (VT Terminal Sessions)” on page 139
- “Select a Cursor Style” on page 54
- “Map a Sound to an Event” on page 48
- “Configure Color Settings” on page 35
Select a Theme File Dialog Box

Getting there

1. Open the Document Settings dialog box. The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ribbon or Reflection Browser</td>
<td>With a session open in Reflection, from the Quick Access Toolbar, click.</td>
</tr>
<tr>
<td>TouchUx</td>
<td>Tap the Gear icon and then select Document Settings.</td>
</tr>
</tbody>
</table>

2. Under Terminal Appearance, click Manage Themes.
3. Click Select another theme file.

From this dialog box, select a theme file to use with this session.

   - Built-In: Select this option to show the theme files distributed with InfoConnect.
   - Custom: Select this option to show the theme files that you've previously modified and saved. If the file you want doesn't appear in the list, click Browse to select it.

   **NOTE:** The file must be in a trusted location.

Modify Theme Dialog Box (3270 Terminal Sessions)

Index Term
Primary: variable-width fonts
Secondary: in 3270 sessions

Index Term
Primary: Unicode zero character
Secondary: settings, 3270 sessions

Index Term
Primary: themes
Secondary: settings, 3270 sessions

Index Term
Primary: text
Secondary: host formatting settings (3270)

Index Term
Primary: text
Secondary: color mapping (3270)

Index Term
Primary: sounds
Secondary: settings, 3270 sessions
Getting there

1 **Open a terminal session.**
   The steps depend on your [user interface mode](page 120).\
   \[User Interface Mode\] \[Steps\]
   Ribbon or Reflection Browser With a session open in Reflection, from the [Quick Access Toolbar](#), click [ ].
   TouchUx Tap the Gear icon and then select [Document Settings].

2 **Under Terminal Appearance, click Manage Themes.**
3 **Click Modify the currently selected theme file.**

Create your own custom theme by modifying and saving an existing theme.
Theme Information
This information is displayed, along with a thumbnail, in the list of themes that appears on the Select a Theme File dialog box.

Title
Specify a title for this theme.

Description
Describe this theme.

Sounds
Make sure any sound file you want to include is saved in a trusted location. InfoConnect uses the sound files installed with Windows.

Events
Select the event that will trigger a sound.

Sound
Click Browse to specify a sound that plays when the selected event occurs. Click Play to hear the sound.

Font

Font Settings

Font
Select a font from the drop-down box.

Bold
Select to apply bold formatting to the specified font.

Include variable-width fonts
Select to increase your font choices.

Unicode zero character setting
Select a different style of zero, if supported by the specified font.

Automatically adjust font size to fit window
When selected, InfoConnect adjusts the font to fit the session screen. To specify a particular font size, select Specify font size instead.

Specify font size
Specify the point size for fonts.

Preview

Preview box
Displays the specified font and text effects.

Cursor Style

Cursor

Shape
Specify the shape for the cursor.

Blink rate
Specify the speed at which the cursor blinks.

Graphics Cursor

Shape
Specify the shape for the graphics cursor.

Crosshair color
Specify the color of the graphics cursor crosshair.
Rule Line

Show rule lines
Select to display rule lines, which provide a visual cue to your location on the screen.

Appearance
Specify the type of rule lines: a vertical line, a horizontal line, or crosshair lines.

Text Color Mapping

Terminal color
Click Change to specify the foreground (text) and background colors for all terminal session screens.

Terminal item
Click Change to specify foreground and background colors for terminal items. You can specify different colors for different types of fields: protected (read-only) and unprotected, highlighted and normal, and alpha and numeric.

Graphics Color Mapping

Terminal graphics color
Click Change to specify the foreground (text) colors for all terminal graphics screens.

Background
Click Change to specify the background color for terminal graphics screens.

Related Topics

• “Manage Themes Dialog Box” on page 132
• “Specify Trusted Locations Dialog Box” on page 329

Modify Theme Dialog Box (5250 Terminal Sessions)

Index Term
Primary: variable-width fonts
Secondary: in 5250 sessions

Index Term
Primary: Unicode zero character
Secondary: settings, 5250 sessions

Index Term
Primary: themes
Secondary: settings, 5250 sessions

Index Term
Primary: text
Secondary: host formatting settings (5250)

Index Term
Primary: text
Secondary: color mapping (5250)
Index Term
Primary: sounds
Secondary: settings, 5250 sessions

Index Term
Primary: rule line
Secondary: settings, 5250 sessions

Index Term
Primary: mapping
Secondary: text color (5250)

Index Term
Primary: fonts
Secondary: settings, 5250 sessions

Index Term
Primary: events
Secondary: sounds (5250 sessions)

Index Term
Primary: cursor
Secondary: settings, 5250 sessions

Index Term
Primary: bold
Secondary: font settings, 5250 sessions

Index Term
Primary: blink rate
Secondary: cursor (5250 sessions)

Getting there

1. **Open a terminal session.**
   The steps depend on your user interface mode (page 120).

   **User Interface Mode** | **Steps**
   --- | ---
   Ribbon or Reflection Browser | With a session open in Reflection, from the Quick Access Toolbar, click .
   TouchUx | Tap the Gear icon and then select Document Settings.

2. **Under Terminal Appearance, click Manage Themes.**
3. **Click Modify the currently selected theme file.**

Create your own custom theme by modifying and saving an existing theme.

**Theme Information**
This information is displayed, along with a thumbnail, in the list of themes that appears on the Select a Theme File dialog box.

**Title** Specify a title for this theme.

**Description** Describe this theme.
Sounds
Make sure any sound file you want to include is saved in a trusted location. InfoConnect uses the sound files installed with Windows.

Events
Select the event that will trigger a sound.

Sound
Click Browse to specify a sound that plays when the selected event occurs. Click Play to hear the sound.

Font
Font Settings

Font
Select a font from the drop-down box.

Bold
Select to apply bold formatting to the specified font.

Include variable-width fonts
Select to increase your font choices.

Unicode zero character setting
Select a different style of zero, if supported by the specified font.

Automatically adjust font size to fit window
When selected, InfoConnect adjusts the font to fit the session screen. To specify a particular font size, select Specify font size instead.

Specify font size
Specify the point size for fonts.

Preview
Preview box
Displays the specified font and text effects.

Cursor Style
Cursor

Shape
Specify the shape for the cursor.

Blink rate
Specify the speed at which the cursor blinks.

Restrict cursor movement
When selected, cursor movement is restricted to protected fields. Selecting this option helps users navigate within the terminal screen more efficiently.

Horizontal speed
Set the horizontal cursor speed. The number indicates the number of character spaces the cursor moves with each "Left Double" or "Right Double" key press. Increase the numeric value to increase the speed.

Vertical speed
Set the vertical cursor speed. The number indicates the number of character spaces the cursor moves with each "Up Double" or "Down Double" key press. Increase the numeric value to increase the speed.

Rule Line
Show rule lines
Select to display rule lines, which provide a visual cue to your location on the screen.

Appearance
Specify the type of rule lines: a vertical line, a horizontal line, or crosshair lines.
Text Color Mapping

**Terminal color**
Click **Change** to specify the foreground (text) and background colors for all terminal session screens.

**Terminal item**
Click **Change** to specify foreground (text) and background colors for the Status Line, Field Outlines, Message Line, Error Line, and System Request terminal items.

Related Topics

- “Manage Themes Dialog Box” on page 132
- “Specify Trusted Locations Dialog Box” on page 329

**Modify Theme Dialog Box (VT Terminal Sessions)**

Index Term
- Primary: themes
- Secondary: settings, VT sessions

Index Term
- Primary: text
- Secondary: host formatting settings (VT)

Index Term
- Primary: mapping
- Secondary: text color (VT)

Index Term
- Primary: fonts
- Secondary: settings, VT sessions

Index Term
- Primary: cursor
- Secondary: settings, VT sessions

Index Term
- Primary: color
- Secondary: cursor (VT)

Index Term
- Primary: color
- Secondary: ANSI color, configuring in VT

Index Term
- Primary: ANSI
- Secondary: color mapping (VT)

**Getting there**

1. Open a terminal session.

   The steps depend on your [user interface mode](#) (page 120).
Under Terminal Appearance, click Manage Themes.

3 Click Modify the currently selected theme file.

Create your own custom theme by modifying and saving an existing theme.

Theme Information

This information is displayed, along with a thumbnail, in the list of themes that appears on the Select a Theme File dialog box.

- **Title**: Specify a title for this theme.
- **Description**: Describe this theme.

Sounds

Make sure any sound file you want to include is saved in a trusted location. InfoConnect uses the sound files installed with Windows.

- **Events**: Select the event that will trigger a sound.
- **Sound**: Click Browse to specify a sound that plays when the selected event occurs. Click Play to hear the sound.

Font

**Font Settings**

- **Font**: Select a font from the drop-down box.
- **Bold**: Select to apply bold formatting to the specified font.
- **Automatically adjust font size to fit window**: When selected, InfoConnect adjusts the font to fit the session screen. To specify a particular font size, select Specify font size instead.
- **Specify font size**: Specify the point size for fonts.

Preview

- **Preview box**: Displays the specified font and text effects.

Cursor Style

- **Shape**: Specify the shape for the cursor.
- **Enable cursor blink**: Select to allow the cursor to blink.
**Display Enhancements**

These settings control whether display enhancements specified by the host are used by your computer.

- **Enable blink**: Select to allow text to blink.
- **Enable underline**: Select to allow underlined text.
- **Enable bold**: Select to allow bold text.
- **Inverse video**: Select to allow inverse video.
- **Color cursor**: Select to allow changes to the color of your cursor.

**Text Color Mapping**

These colors are not available for all terminal types.

- **Terminal item**: Click Change to specify foreground and background colors for terminal items. You can specify different colors for different types of fields, such as Normal, Blink, Bold, Underline, and Inverse.

**ANSI Color Mapping**

These colors are not available for all terminal types.

- **Terminal graphics color**: Click Change to replace standard ANSI colors with the specified colors for all terminal session screens.

**Related Topics**

- “Manage Themes Dialog Box” on page 132
- “Specify Trusted Locations Dialog Box” on page 329

---

## Manage QuickPads Dialog Box

**Getting to the Manage QuickPads dialog box**

**IMPORTANT**: The Manage QuickPads dialog box is available only if you installed the Legacy EXTRA! feature when you installed InfoConnect. (This feature is available on the Attachmate Installation Program Features tab, under 3270/5250 | Compatibility or UNIX and OpenVMS | Compatibility.)

1. Open the Document Settings dialog box.
   - The steps depend on your user interface mode (page 120).
In the Settings dialog box, under **User Interface**, click **Manage QuickPads**.

2 You can use quickpads and toolbars that were created in EXTRA! in your **InfoConnect** sessions.

**IMPORTANT**

- The Manage QuickPads dialog box is available only if you installed the Legacy EXTRA! feature when you installed **InfoConnect**. (This feature is available on the Attachmate Installation Program Features tab, under 3270/5250 | Compatibility or UNIX and OpenVMS | Compatibility.)

- To create or edit a quickpad, you must use the Attachmate EXTRA! product. You cannot use **InfoConnect** to create or edit quickpads.

To add a quickpad or toolbar to your session

- In the **Available QuickPads** list, select the quickpad and click **OK**.

The quickpad is displayed in the existing session and the session document is set to display the quickpad in new sessions.

**NOTE**

- If the quickpad is closed during the session, it is not displayed in new sessions.

- Toolbars are imported as quickpads that open in a quickpad window docked on the top of the session window.

**Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Available QuickPads</strong></td>
<td>Displays the list of quickpads that are available for the session. This list includes all of the quickpad (.eqp) files and toolbar (.etb) files in the EXTRA!\Schemes directory and in the Default Legacy EXTRA! directory specified in the “Configure Workspace Attributes Dialog Box” on page 128 (the default path is: My Documents\Attachmate\Reflection). It also includes all of the .eqp and .etb files that you have added. (These files must be in trusted locations.)</td>
</tr>
<tr>
<td><strong>Add</strong></td>
<td>Opens a dialog box that you can use to add quickpad (.eqp) files or toolbar (.etb) files from any trusted location to the Available QuickPads list.</td>
</tr>
<tr>
<td><strong>Remove</strong></td>
<td>Removes the selected quickpad from the Available QuickPads list.</td>
</tr>
<tr>
<td><strong>Show ToolTips</strong></td>
<td>Displays the quickpad tooltips.</td>
</tr>
</tbody>
</table>
Workspace Settings Dialog Box

Getting there

1. Open the InfoConnect Workspace Settings dialog box.
   The steps depend on your user interface mode (page 120).

   **User Interface Mode**  |  **Steps**
   ------------------------|----------------------------
   InfoConnect Browser     |  On the InfoConnect menu, choose Settings and then Reflection Workspace Settings.
   TouchUX                 |  Tap the Gear icon and then select Reflection Workspace Settings.

2. Click **Workspace Settings**.

   You can configure actions to perform when Reflection opens or closes, set workspace attributes such as the user data directory, and select which type of interface to use.

**Group Box Title**

- **Configure Workspace Defaults**  Configure the actions to perform when the Reflection workspace opens or closes and preferences for automatically saving session document files.
- **Configure Workspace Attributes**  Configure options for logging, running remote sessions, and displaying Help. You can also specify the user data directory, in which session documents and other related files are saved.
- **Configure User Interface**  Configure which type of user interface to use (Reflection provides four interfaces), its look and feel, and other user interface options.
6 Terminal Sessions

The document for a terminal session contains configuration settings for host-specific information. It also includes pointers to other files that are used to control the appearance of the session, such as the theme file, and to files that control input and text handling, such as the keyboard map file and the Ribbon file.

Terminal sessions are pre-configured to use built-in Ribbon, theme, keyboard map, and mouse map files. If you choose, you can create custom versions of these files to modify the appearance and capabilities of each session.

**CAUTION:** If you specify a custom file for a session, be sure to maintain the same file name and file path (relative to the session document file) when you deploy the files. If InfoConnect cannot find the custom file when it starts a session, it prompts to use a built-in file.

**NOTE:** You must have a session open to configure it.

Access individual settings pages from specific buttons on the Ribbon. Or, click the Document Settings button from the Quick Access toolbar to select settings pages from a list of links.

Settings pages open in a separate window that includes:

- The address path, which you can select with the click of a mouse
- Related Topics links in a pane on the left
- Back and Forward buttons, for navigation between settings pages you've visited

In this Chapter

- “Session Documents and Related Files” on page 146
- “Create a Session Document File” on page 147
- “Open a Terminal Session” on page 148
- “Share Sessions as Templates” on page 149
- “Encrypt a Session File” on page 151
- “Connecting to the Host” on page 152
- “Context Menu Editor Dialog Box” on page 153
- “Terminal Settings” on page 155
New documents include default, built-in choices for configuration settings. These settings are saved in configuration files such as Ribbon, theme, keyboard map, and mouse map files. If you choose, you can create custom versions of these files to modify the appearance and capabilities of each session. If you choose a different built-in setting or create a custom setting, you must save the document to apply the new setting. Custom settings files are saved separately from the document.

Macro files are also saved as separate files external to the session document.

**CAUTION:** If you specify a custom file for a session, be sure to maintain the same file name and file path (relative to the session document file) when you deploy the files. If InfoConnect cannot find the custom file when it starts a session, it prompts to use a built-in file.

**NOTE:** Always save documents and templates to a trusted location — InfoConnect won’t open documents from nontrusted locations.

You can open saved documents in any of the user interfaces modes. When using the Classic UI, only one document can be open in a workspace, and other features may not be available.

**Related Topics**

- “Manage Ribbon Dialog Box” on page 83
- “Keyboard Mapper” on page 183
- “Mouse Mapper” on page 189
Create a Session Document File

To access a host, you need to open a session on that host. In InfoConnect, you can create a session document that allows you to configure and reuse your session. Terminal sessions are pre-configured to use built-in Ribbon, theme, keyboard map, and mouse map files. If you choose, you can create custom versions of these files to modify the appearance and capabilities of each session.

CAUTION: If you specify a custom file for a session, be sure to maintain the same file name and file path (relative to the session document file) when you deploy the files. If InfoConnect cannot find the custom file when it starts a session, it prompts to use a built-in file.

To create a new terminal session

1 Open the Create New Document dialog box.
   The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ribbon or Reflection Browser</td>
<td>From the Quick Access Toolbar, click the New Document button.</td>
</tr>
<tr>
<td>TouchUx</td>
<td>Tap the Folder icon and then under File, select New.</td>
</tr>
</tbody>
</table>
2 From the Create New Document dialog box, select a session template.

3 In the Compatibility drop-down box, select the set of default settings you want to use for this session, if any.
   The compatibility settings include keyboard maps and themes similar to those of other emulation products. The default InfoConnect compatibility setting is optimized for this product.

4 Click Create.

5 For Host Name/IP Address, enter the fully qualified host name.

   **NOTE:** Both IPv4 addresses (in the form 127.0.0.1) and IPv6 addresses (in the form 2001:0db8:3c4d:0015:0000:0000:abcd:ef12) are accepted.

6 Change other settings if necessary.

7 If you want to add custom files (for example, custom theme, keyboard map, or Ribbon files), select Configure additional settings and click OK. Then, on the Settings dialog box, click the link for the file you want to customize (for example, Manage Themes, Manage Ribbon, or Manage Keyboard Maps) and follow the online instructions to select a custom file.

8 From the Quick Access Toolbar, click the Save button to save the session document.

Related Topics

- “Configuring InfoConnect” on page 70
- “Secure Connections” on page 327
- “Create a 3270 Printer Session” on page 526
- “Create a 5250 Printer Session” on page 535
- “Create New Document Dialog Box” on page 122

Open a Terminal Session

To access a host, you need to open a session on that host. Once you’ve created and saved a session document, you can connect to the host simply by opening the session document.
To open an existing terminal session

1. Go to the Open dialog box.

   The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ribbon or Reflection Browser</td>
<td>From the Quick Access Toolbar, click the Open button.</td>
</tr>
<tr>
<td>TouchUx</td>
<td>Tap the Folder icon and then select Open.</td>
</tr>
</tbody>
</table>

2. Select the session you want, and then click Open.

Related Topics

- “Open a Layout” on page 51
- “Session Documents and Related Files” on page 146

Share Sessions as Templates

Session documents contain references to the following settings (all of which can be customized):
host, ribbon, theme, keyboard map, and mouse map.

After you configure a session document, you can share and reuse your settings by saving the document as a template. Templates provide an unntitiled copy of the original, giving you a quick and easy way to create pre-configured documents, while ensuring that your original file remains unchanged.
InfoConnect includes several templates in the **Create New Document** dialog box. When you create a template, as long as you save it to the Templates folder (the default location), it is added to this dialog box under **User Defined**.

**To share a session document**

1. Open the session document that you've configured.

2. **Save the session as a template.**
   
   2a. Do one of the following:
   
   The steps depend on your user interface mode (page 120).

   **User Interface Mode** | **Steps**
   --- | ---
   Ribbon (Office 2007) | On the **InfoConnect** button , choose **Save As** and then **Save Template**.
   Ribbon (Office 2010) | On the **File** menu, choose **Save As** and then **Save Template**.
   InfoConnect Browser | In the search box, enter **S** and then, under **Actions**, select **Save Template**.

   2b. Name the template file with an .rsft extension, and then save the template to the Templates folder.

3. Move the template file from the Templates folder on your computer to either a shared location or to the Templates folder on a computer that has **InfoConnect** installed.

**NOTE:** If you copy the template file to a location other that the Templates folder, make sure it's a trusted location or **InfoConnect** won't open it.

The Templates folder is in the following location:

- **Windows XP:**
  
  Documents and Settings\user\Application Data\Attachmate\Reflection\Workspace\**data_folder**
  
  or-

- **Windows 7 or Vista:**
  
  Users\**user_name**\AppData\Roaming\Attachmate\Reflection\Workspace\**data_folder**

**NOTE:** The name of the **data_folder** is **R2014_versionName**. (For example, the **data_folder** name in **InfoConnect 2014 R1** is **R2014_R1**.)

4. To make changes to the template, you must replace the template file — save the file that contains your changes using the same filename and extension as the template.

**Related Topics**

- “Specify Trusted Locations Dialog Box” on page 329
- “Customize the Ribbon” on page 74
- “Specifying a Custom Keyboard Map” on page 177
- “Specifying a Mouse Map” on page 184
- “Create a Session Document File” on page 147
Encrypt a Session File

You can encrypt 3270, 5250, and Open Systems session documents to protect them against unauthorized changes. Encryption effectively scrambles the data in a session document, helping to prevent unauthorized users from reading and changing the file’s contents. For best results, use document encryption in conjunction with the encryption options in the Permissions Manager.

In Reflection, you can easily encrypt sessions by saving them in the Encrypted Session Document format.

Alternatively, you can encrypt documents using a command-line program installed with Reflection, FileEncrypt.exe. With this program, you can also determine whether session documents are encrypted, and if they are, you can decrypt them.

To encrypt a session in Reflection

1. Open a session document.

2. Open the Save As dialog box.
   
   The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ribbon (Office 2007)</td>
<td>On the Reflection button , choose Save As.</td>
</tr>
<tr>
<td>Ribbon (Office 2010)</td>
<td>On the File menu, choose Save As.</td>
</tr>
<tr>
<td>InfoConnect Browser</td>
<td>On the InfoConnect menu, choose Save As.</td>
</tr>
<tr>
<td>TouchUx</td>
<td>On the InfoConnect menu, tap the Folder icon and then under File, select Save As.</td>
</tr>
</tbody>
</table>

3. From the Save as Type menu, choose the available encryption format, and then click Save.
To encrypt, decrypt, or test sessions using FileEncrypt.exe

- From a command line, enter any of the following commands:

<table>
<thead>
<tr>
<th>To</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encrypt a document</td>
<td><code>fileencrypt /e [file_in] [file_out]</code></td>
</tr>
<tr>
<td>Decrypt a document</td>
<td><code>fileencrypt /d [file_in] [file_out]</code></td>
</tr>
<tr>
<td>Test a document for encryption</td>
<td><code>fileencrypt /t [file_in]</code></td>
</tr>
</tbody>
</table>

where:

- `[file_in]` = The filename, including the extension and relative path.
- `[file_out]` = (Optional) A new name for the output file.

For example:

```
fileencrypt /e Session.rd3x SessionEncrypted.rd3x
```

**NOTE:** FileEncrypt.exe searches only the current directory for session files, and requires administrative credentials to encrypt or decrypt a file.

Connecting to the Host

Index Term
Primary: host connection
Secondary: overview

Index Term
Primary: connecting to the host
Secondary: overview

By default, terminal session documents are configured to connect to the host automatically when you create or open a terminal session. However, with a session document open in InfoConnect, you can manually disconnect or connect. You can also set up a session so that it doesn't automatically connect to the host.
To manually disconnect or connect to a session

- Do one of the following:
  
  The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ribbon</td>
<td>On the Session tab, in the Host group, click ![disconnect_icon] to disconnect or ![connect_icon] to connect.</td>
</tr>
<tr>
<td>InfoConnect Browser</td>
<td>On the InfoConnect menu, choose Host and then Disconnect or Connect.</td>
</tr>
<tr>
<td>TouchUX</td>
<td>On the InfoConnect menu, tap the folder icon and then under Host, select Connect.</td>
</tr>
</tbody>
</table>

To stop a session from automatically connecting to the host

1. Open a terminal session.

2. Open the Document Settings dialog box.
   The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ribbon or Reflection Browser</td>
<td>With a session open in Reflection, from the Quick Access Toolbar, click ![folder_icon].</td>
</tr>
<tr>
<td>TouchUX</td>
<td>Tap the Gear icon and then select ![folder_icon] Document Settings.</td>
</tr>
</tbody>
</table>

3. Under Host Connection, click Configure Connection Settings.

4. Under Host Connection Options, clear the Automatically connect to the host option.

Related Topics

- “Create a Session Document File” on page 147
- “Open a Terminal Session” on page 148
- “Configure Connection Settings Dialog Box” on page 215
- “Select Host Code Page Dialog Box (3270)” on page 228
- “Configure Connection Settings Dialog Box” on page 247
- “Select Host Code Page Dialog Box (5250)” on page 258
- “Configure Connection Settings Dialog Box (VT)” on page 265

Context Menu Editor Dialog Box

Index Term
Primary: right-click menu

Index Term
Primary: Context Menu Editor
Index Term
Primary: adding
Secondary: items to right-click menu

Getting there
The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ribbon</td>
<td>Click the Appearance tab and in the <strong>Menus</strong> group, select <strong>Context Menu</strong>.</td>
</tr>
<tr>
<td>Reflection Browser</td>
<td>On the Reflection menu, choose <strong>View</strong> and then choose <strong>Context Menu</strong>.</td>
</tr>
<tr>
<td>TouchUX</td>
<td>Tap the Wrench icon and then under <strong>View</strong>, select <strong>Context Menu</strong>.</td>
</tr>
</tbody>
</table>

From this dialog box, you can modify the context menu for session documents.

**NOTE:** Context menus in Web page documents are a function of the browser application and cannot be modified.

Select, add or remove context menu:
This drop-down menu lists the program’s default context menu and any custom context menus that have been added. Use the **Add** and **Remove** buttons to create and delete custom context menus.

Edit selected context menu:

<table>
<thead>
<tr>
<th>Menu Items</th>
<th>Shows the items on the current context menu. An ampersand (&amp;) before a letter indicates that you can use the ALT key with that letter to trigger the action.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Menu Item</td>
<td>Adds a new menu item below the currently selected menu item. New menu items have no defined action. To change the label and map an action to the new item, use the <strong>Label</strong> field and <strong>Select Action</strong> button from the <strong>Menu Item Settings</strong> group box.</td>
</tr>
<tr>
<td>Add Separator</td>
<td>Adds a new separator line below the currently selected menu item.</td>
</tr>
<tr>
<td>Delete</td>
<td>Removes the selected item from the context menu.</td>
</tr>
<tr>
<td>Move Up / Move Down</td>
<td>Moves the selected item up or down in the <strong>Menu Items</strong> list.</td>
</tr>
</tbody>
</table>

**Menu Item Settings**

| Label | Provide a name for the menu item. |
| Action | The internal name for the action. To change the action, choose the **Select Action** button. |
| Select Action | Opens the **Select Action** dialog box, from which you can select a variety of actions, or build an action sequence. |
Terminal Settings

Terminal settings consist of a variety of emulation specific options that affect the keyboard, display, and other behaviors.

- Configure Terminal Settings for 3270 (page 229)
- Configure Terminal Settings for 5250 (page 258)
- Configure Terminal Settings for VT (page 282)

Configuring Input and Text Handling

When you create a new session document, it is automatically configured to use the default input settings for that host. You can configure your session to use different settings, or you can customize those settings and create your own keyboard map, mouse map, and clipboard settings.

Productivity features such as Auto Complete and Auto Expand provide additional ways to customize input and text handling.

In this Section

- “Clear the Clipboard on Close” on page 155
- “Quick Keys” on page 156
- “Select Action Dialog Box” on page 161
- “Configure Clipboard Settings Dialog Box (3270 and 5250)” on page 165
- “Configure Clipboard Settings Dialog Box (VT)” on page 167
- “Manage Hotspots Dialog Box” on page 169
- “Select a Hotspots File Dialog Box” on page 169
- “Modify Hotspots Dialog Box” on page 170
- “Hotspot Options Dialog Box” on page 171
- “Set Up Hotspot Display Settings Dialog Box” on page 173
- “Create a New Hotspots File Dialog Box” on page 175
- “Specify which Dialog Box to Open when InfoConnect Starts” on page 175
- “Set Up a Workspace Startup Action Sequence” on page 176

Clear the Clipboard on Close

Index Term
Primary: Clipboard
Secondary: clear on close

For security reasons, you may want to ensure that any data copied to the clipboard is cleared when you close the workspace.

To clear the clipboard automatically

1. Open InfoConnect Workspace Settings dialog box.
   The steps depend on your user interface mode (page 120).
2 Click **Configure Workspace Defaults**.

3 Under **Workspace**, select **Clear clipboard when closing workspace**.

**Related Topics**

- “Configure Clipboard Settings Dialog Box (3270 and 5250)” on page 165
- “Copy and Paste Host Data” on page 39

**Quick Keys**

**Index Term**

Primary: sending keys
Secondary: using Quick Keys

**Index Term**
Primary: page up or down

**Index Term**
Primary: newline key

**Index Term**
Primary: keys, sending
Secondary: using Quick Keys

**Index Term**
Primary: erase EOF

**Index Term**
Primary: enter key

Use the Quick Keys gallery on the Ribbon for quick access to terminal keys for host sessions.

**In this Section**

- “3270 Quick Keys” on page 156
- “5250 Quick Keys” on page 157
- “VT Quick Keys” on page 158

**3270 Quick Keys**

**Index Term**
Primary: reset
Secondary: 3270
In 3270 terminal sessions, the following Quick Keys are available from the Ribbon.

**Program Attention Keys**

- **PA1 - PA3** Select to send a program attention key to the host.

**Program Function Keys**

- **PF1 - PF24** Select to send a program function key to the host.

**Other**

- **Attention** Select to send an Attention key to the host.
- **Enter** Select to send an Enter key to the host.
- **Newline** Select to move the cursor to the beginning of a new line.
- **Erase EOF** Select to erase all characters, from the cursor to the end of the entry.
- **Reset** Clear the Input Inhibited indicator and reset the Insert mode.
- **Clear** Set buffer locations for the active partition to nulls and the Reply mode to the default, transmit the Clear Aid key to the host, and move the cursor position to the top left corner.

**5250 Quick Keys**

- **Index Term** Primary: roll up or down
- **Index Term** Primary: reset
- **Index Term** Primary: Quick Keys
- **Index Term** Primary: program function keys
In 5250 terminal sessions, the following Quick Keys are available from the Ribbon.

**Program Attention Keys**

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PA1 - PA3</td>
<td>Select to send a program attention key to the host.</td>
</tr>
</tbody>
</table>

**Program Function Keys**

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PF1 - PF24</td>
<td>Select to send a program function key to the host.</td>
</tr>
</tbody>
</table>

**Other**

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attention</td>
<td>Select to send an Attention key to the host.</td>
</tr>
<tr>
<td>Enter</td>
<td>Select to send an Enter key to the host.</td>
</tr>
<tr>
<td>Newline</td>
<td>Select to move the cursor to the beginning of a new line.</td>
</tr>
<tr>
<td>Erase EOF</td>
<td>Select to erase all characters, from the cursor to the end of the entry.</td>
</tr>
<tr>
<td>Reset</td>
<td>Exit insert mode, diacritical mode, or hex mode; end help and system request functions; clear operator errors; and remove the Input Inhibited indicator and reset the Insert mode. Select Reset twice (consecutively) to exit Plus CR mode.</td>
</tr>
<tr>
<td>Clear</td>
<td>Signal the host to erase all user-entered text from the current screen.</td>
</tr>
<tr>
<td>Roll Up</td>
<td>Select to scroll down one page in the current host screen. This option is equivalent to Page Down.</td>
</tr>
<tr>
<td>Roll Down</td>
<td>Select to scroll up one page in the current host screen. This option is equivalent to Page Up.</td>
</tr>
</tbody>
</table>

**VT Quick Keys**

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Soft reset (VT)</td>
<td></td>
</tr>
<tr>
<td>Reset</td>
<td>Exit insert mode, diacritical mode, or hex mode; end help and system request functions; clear operator errors; and remove the Input Inhibited indicator and reset the Insert mode. Select Reset twice (consecutively) to exit Plus CR mode.</td>
</tr>
<tr>
<td>Clear</td>
<td>Signal the host to erase all user-entered text from the current screen.</td>
</tr>
<tr>
<td>Recall last setup (VT)</td>
<td></td>
</tr>
</tbody>
</table>
In VT terminal sessions, you can access a gallery of Quick Keys from the Ribbon. The specific set of keys available from the gallery depends on the terminal type your session is emulating. The standard keys for VT terminals are shown below.

**Program Function Keys**

- **PF1 - PF4**: Select to send a program function key to the host.

**VT Function Keys**

- **F1 - F20**: Select to send a VT function key to the host.

**Edit Keys**

The VT keyboard has a block of six editing keys that InfoConnect simulates. These keys send the following escape sequences:

- **Find**: `<ESC>[1~`
- **Insert**: `<ESC>[2~`
- **Remove**: `<ESC>[3~`
- **Select**: `<ESC>[4~`
- **Previous**: `<ESC>[5~`
- **Next**: `<ESC>[6~`
Reset

Clear Communications

This command:
- Cancels printing operations
- Cancels escape sequences, control sequences, and device control strings
- Turns logging off
- Clears receive and transmit buffers
- Resets XOFF (DC3) signals

For all types of connections, an XON (DC1) signal is sent to the host.

This command can often remedy communications problems when the host connection appears to be "stuck." Clear Communications does not disconnect you from the host computer.

Terminal

Also called a "soft reset," this command:
- Emits a beep
- Sets the main display as the active display
- Cancels any pending autowrap
- Sets character sets to their default values
- Sets Insert/Replace mode to Replace
- Unlocks the keyboard (if it was locked)
- Sets the cursor keys to Normal, and the numeric keypad to Numeric
- Sets the origin to Absolute
- Homes the cursor
- Sets Graphic Rendition and Selective Erase to Normal
- Enables Text Cursor mode
- Sets the top margin to 1, and the bottom to 24
- Sets the UPSS to the last saved value
- Initializes the communications port for serial connections to the last activated values, and clears the receive buffer

Recall Last Setup

Also called a "hard reset," this command restores the terminal settings for the active connection to their last saved settings. Settings specific to InfoConnect, such as file transfer settings, preferences, and printer settings, are not reset.

In addition, this command:
- Cancels a pending Wait method
- Clears the display and places the cursor in the upper-left corner
- Sets the select graphic rendition (SGR) function to Normal
- Sets the selective erase attribute (DECSCA) to Erasable
- Clears the user-defined keys (DECUDK)
- Selects the default character sets: ASCII in GL and User-preferred Supplemental Set in GR

Enter

Select to send an Enter key to the host.
Select Action Dialog Box

Because you can specify an action to complete almost any task in InfoConnect, there are several ways to access the Select Action dialog box:
Mouse Mapper

1. Open a session document.
2. Open the Mouse Mapper dialog box as follows:
3. Position your mouse on the image to the left and click a mouse button or mouse and key combination.
   The steps depend on your user interface mode (page 120).

   **User Interface Mode** | **Steps**
   --- | ---
   Ribbon | On the Tools tab, click Mouse Mapper.
   InfoConnect Browser | On the InfoConnect menu, choose Tools, and then Mouse Mapper.
   TouchUx | Tap the Gear icon and then select Document Settings. Under Input Devices, click Manage Mouse Map. Then choose whether to modify the current mouse map or create a new map.

4. Click Select Action.

Keyboard Mapper

1. Open a session in InfoConnect.
2. Open the InfoConnect Keyboard Mapper dialog box as follows:
   The steps depend on your user interface mode (page 120).

   **User Interface Mode** | **Steps**
   --- | ---
   Ribbon | On the Tools ribbon, click Keyboard Mapper.
   InfoConnect Browser | On the InfoConnect menu, choose Tools, and then Keyboard Mapper.
   TouchUx | Tap the Wrench icon and then under Tools, select Keyboard Mapper.

3. Press a key or keyboard combination and then click Select Action.

UI Designer

1. Open a session document.
2. On the Ribbon, click the Appearance tab.
3. From the Menus group, click UI Designer.
4. From the Insert Controls pane, click the Button control, and then click the Select Action button in the Settings pane.

Context Menu Editor

1. Open a session document.
2. Open the Context Menu Editor as follows:
   The steps depend on your user interface mode (page 120).
3 Click **Select Action**.

### Hotspots

1. Open a session document. The steps depend on your user interface mode (page 120).

2. **Under Terminal Appearance**, click **Manage Hotspots**.

3. Click **Modify the currently selected hotspots file**.

4. Enter or select hotspot text, and then click **Select Action**.

From this dialog box, you can assign an action or a function to a mouse button, keyboard key, hotspot, or menu item. An action can be any action you can perform within InfoConnect, such as sending keystrokes, running a macro, executing a menu command, navigating to a recorded host screen page, transferring a file, or printing.

Actions are divided into categories listed in the task pane on the left, and the actions or functions available for assignment to an item depends on the selected category. Some functions also require additional information, such as the keystrokes to send for a Send Key command.

The settings for **Other Action** appear by default. A description for each task-pane item follows.

#### Other Action

- **Action category** Select from the list of feature sets that include programmable actions.
- **Action** Select the desired programmable action.
- **Action parameters** Specify any additional settings required to program the action. For example, if you select the action **Launch Application**, you must specify the application name and a working directory under **Action parameters**.

#### Send Key

- **Key** Select an Action Identifier (AID) key from the list.
Send Text

Text to send to host  Enter the text you want to send when the action runs. You can do this in two ways:

Select a special character  Select the special character to send.

**NOTE:** Before you create an action that opens a file or starts an application, place the file or application in a trusted location (page 892).

Launch Application

**NOTE:** Before you create an action that opens a file or starts an application, place the file or application in a trusted location (page 892).

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application name</td>
<td>Type the name of the executable file (EXE) or click Browse to select it.</td>
</tr>
<tr>
<td>Parameters</td>
<td>Type any command line parameters you want to use to start the application.</td>
</tr>
<tr>
<td>Working directory</td>
<td>Type the path to the folder where the application automatically searches for files.</td>
</tr>
</tbody>
</table>

Open URL

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use matched hotspot text for the URL</td>
<td>Select this check box to create a link from any text string that matches the hotspot. The link opens the specified URL. This option is only available when mapping a hotspot to an action.</td>
</tr>
<tr>
<td>URL</td>
<td>Type the desired URL.</td>
</tr>
<tr>
<td>Open in new tab</td>
<td>Select to open the specified URL in a new Web document in the workspace.</td>
</tr>
<tr>
<td>Open in default browser</td>
<td>Select to start the default Web browser at the specified URL.</td>
</tr>
<tr>
<td>Open in existing tab</td>
<td>Select to specify an existing Web page document.</td>
</tr>
</tbody>
</table>

**NOTE:** The document is not available from the drop-down list unless it is already open in the workspace.

Run Reflection Workspace Macro

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select macro when action occurs</td>
<td>Select to choose the macro each time you run the action.</td>
</tr>
<tr>
<td>Select macro</td>
<td>Select to specify a VBA project that contains the macro from the menu.</td>
</tr>
</tbody>
</table>
Action Sequence

**Sequence of actions**
Create and list, in order, a series of actions to be performed sequentially. Click **Add** to specify an action, **Delete** to remove an action, and **Move up** or **Move down** to change the order of the list.

**Action category**
Select from the list of feature sets that include programmable actions.

**Action parameters**
Specify any additional settings required to program the action. For example, if you select the action **Launch Application**, you must specify the application name and a working directory under **Action parameters**.

Related Topics

- “Specify Trusted Locations Dialog Box” on page 329
- “Add a Keyboard Shortcut” on page 179
- “Add a Mouse Action” on page 185

Configure Clipboard Settings Dialog Box (3270 and 5250)

Index Term
Primary: paste settings
Secondary: IBM sessions

Index Term
Primary: fill cut areas

Index Term
Primary: editing options

Index Term
Primary: delimiters
Secondary: field

Index Term
Primary: cut/copy/paste settings

Index Term
Primary: copying
Secondary: text

Index Term
Primary: Clipboard
Secondary: settings

Getting there

1. Open a terminal session.
   
   The steps depend on your user interface mode (page 120).
Under **Input Devices**, select **Configure Clipboard Settings**.

### Basic Editing Actions

#### Cut Options

Select the way you want cut or cleared characters to be filled using the following options:

- **Fill cut area with spaces**: Replaces the characters with an equal number of spaces.
- **Fill cut area with nulls**: Replaces the characters with an equal number of nulls.

#### Copy Options

Specify the behavior of text and fields that you copy using the following options:

- **Automatically copy selected text**: Copies selected text to the clipboard automatically.
- **Deselect after copy**: Clears selection after it has been copied to the clipboard.
- **Retain selection**: Maintains a selected area. When you select an area of the screen, and then navigate to a new screen, the area remains selected. This allows you to copy from the same area on different screens without having to select the area again.
- **Copy trailing spaces**: Copies the selected field, including any trailing spaces.
- **Copy input fields only**: Copies only from areas on the screen where input is allowed. Characters in protected fields are replaced with spaces.
- **Copy format options**: Specifies which file formats to copy from Reflection to the clipboard. If you choose more than one format, the application to which the data is pasted automatically uses the format that best suits its needs. (For example, some versions of Microsoft Word would use the .rtf format.)
- **Use table format**: Converts two or more spaces to tabs when data is copied. If there are two or more spaces between words in a selection, the spaces are replaced with a single tab character when you copy the data. (Most spreadsheet and word processing applications interpret tab characters as cell separators.) If there is only one space between words, it remains a space when you copy the data, unless it is followed by a numerical character (0-9, +, or .).

Use **Blanks between fields** to specify the number of spaces between words that should be converted to a single tab character when **Use table format** is selected.
Data delimiters

Specifies whether the data copied from Reflection should be separated by delimiters at field boundaries or at word boundaries. This option controls formatting for spreadsheet or other cell-based information and affects only the text and BIFF formats.

Paste Options

Specify the behavior of cut or copied text using the following options:

- **Data delimiters**: Specifies whether the data copied from Reflection should be separated by delimiters at field boundaries or at word boundaries. This option controls formatting for spreadsheet or other cell-based information and affects only the text and BIFF formats.

- **Paste Options**

  Specify the behavior of cut or copied text using the following options:

  - **Mask protected fields**: Specifies how pasted text is mapped onto the screen:
    - If unselected (the default), the text is interpreted as a linear stream that can contain new lines and delimiters, and is pasted accordingly.
    - If selected, the text is interpreted as a host screen image and overlaid onto the current screen starting at the current cursor position. Where the current screen contains an unprotected field, the source image text is pasted; where the current screen contains a protected field, the source image text is skipped.

  - **Wrap text to next input field**: Causes text that would have been truncated at the end of a field (or the selected paste area) to be pasted to the next unprotected field instead of being truncated. (This option is available only if **Mask protected fields** is not selected).

    - **Wrap to field below**: Wraps text to the next field below instead of the next field to the right.

    - **Align text to input fields**: Aligns space separated data with fields on the screen. This allows you to copy a block of data from a Word form (or other document) into a host screen that has the same field layout as the form.

    - **Use field delimiters**: Maintains formatting for spreadsheet or other cell-based information. In most cases, if you enable Wrap text to next input field, you should also enable this option.

  - **Replace tabs with**: Replaces any tab characters in the pasted data with the specified character or combination of characters.

  - **Clear to end of field after paste**: Clears all of the previous data remaining in a field after pasting new data into it.

  - **Move cursor after paste**: Causes the cursor to move to the end of the pasted text. When unselected, the cursor is restored to the position it was in before the text was pasted.

**Configure Clipboard Settings Dialog Box (VT)**

Index Term

Primary: paste settings
Secondary: VT sessions

Index Term

Primary: Clipboard
Secondary: settings (VT)

Getting there

1. Open a terminal session.

The steps depend on your user interface mode (page 120).
2 Under **Input Devices**, select **Configure Clipboard Settings**.

### Basic Editing Actions

#### Copy Options

Specify the behavior of copied text using the following options:

<table>
<thead>
<tr>
<th>Copy Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Line by line</strong></td>
<td>Copies text on a line by line basis. Carriage returns and line feeds are also copied.</td>
</tr>
<tr>
<td><strong>Unformatted data</strong></td>
<td>Copies text as data with no formatting. Carriage returns and line feeds are not copied.</td>
</tr>
<tr>
<td><strong>Paragraph for word processing</strong></td>
<td>Copies text formatted for word processing. (Insert a space at the end of each line if required to prevent words from running together.) The selected text is treated as one or more paragraphs. A carriage return and a linefeed are inserted only before a blank line.</td>
</tr>
</tbody>
</table>

#### Copy Table Method

Copies text in a tabular format that can be opened in spreadsheets. There are two options for setting table columns:

- **Detect columns (using vertical spaces)**: Detects columns by analyzing the data and finding spaces that line up vertically on the page.
- **Replace multiple spaces or tabs**: Sets columns by replacing multiple spaces or tabs with a single tab. If there is more than one space between words, the space is changed to a single tab character. Most spreadsheets and word processor tables interpret tab characters as cell separators. A single space remains a space when you copy the data, unless it is immediately followed by a numeric character (0-9, +, -, or.).

#### Paste Options

Specify the behavior of pasted text using the following options:

- **Paste buffer size**: This setting specifies the size of a paste block, which is the number of characters pasted from the clipboard to the terminal window before a pause occurs. Set the length of the pause with **Paste delay**.

- **Paste delay**: This setting specifies how many tenths of a second InfoConnect waits between paste blocks when pasting data from the clipboard into display memory. Set the size of the paste block with **Paste buffer size**.
Manage Hotspots Dialog Box

Index Term
Primary: hotspots
Secondary: managing files

Getting there

1 Open a terminal session.
   The steps depend on your user interface mode (page 120).

   User Interface Mode | Steps
   --- | ---
   Ribbon or [InfoConnect] Browser | With a session open in [InfoConnect], from the Quick Access Toolbar, click 📂.
   TouchUx | Tap the Gear icon and then select 📂 Document Settings.

2 Under Terminal Appearance, click Manage Hotspots.

Hotspots files allow you to use your mouse to interact with your terminal session. When you create a terminal session document, it includes a pointer to a default, built-in hotspots file. You can choose a different hotspots file for each session, and you can create custom hotspots files with the settings you prefer.

NOTE: A mouse map provides additional ways to control the way your mouse works in a terminal session.

Select another hotspots file
Click to choose a different hotspots file from a list of existing hotspots files. The file must be in a trusted location.

Modify the currently selected hotspots file
Select to modify the hotspots file used by this session. Because built-in files are read-only, if the currently selected file is a built-in file, it will be saved as a custom file when you change it.

Create a new hotspots file from an existing hotspots file
Click to create a custom hotspots file based on an existing hotspots file. To reopen the file later, it must be saved in a trusted location.

Related Topics

- “Manage Mouse Map Dialog Box” on page 187

Select a Hotspots File Dialog Box

Getting there

1 Open the Settings dialog box.
   The steps depend on your user interface mode (page 120).
Under Terminal Appearance, click Manage Hotspots.

3 Click Select another hotspots file.

From this dialog box, select a hotspots file to use with this session.

Built-In

- Select this option to show the hotspots files distributed with InfoConnect.

Custom

- Select this option to show the hotspots files that you've previously modified and saved. If the file you want doesn't appear in the list, click Browse to select it.

**NOTE:** The file must be in a trusted location.

**Related Topics**

- “Manage Hotspots Dialog Box” on page 169

**Modify Hotspots Dialog Box**

**Index Term**

Primary: mapping
Secondary: hotspots

**Index Term**

Primary: hotspots
Secondary: modifying

**Getting there**

1 Open a terminal session.

The steps depend on your user interface mode (page 120).

**User Interface Mode**

**Steps**

Ribbon or InfoConnect Browser

With a session open in InfoConnect, from the Quick Access Toolbar, click .

TouchUx

- Tap the Gear icon and then select Document Settings.

2 Under Terminal Appearance, click Manage Hotspots.

3 Click Modify the currently selected hotspots file.

From this dialog box, you can change the way the mouse works in InfoConnect. The session document uses the configured hotspots file until you reconfigure it.
NOTE

- Additional hotspots options are available in the Set Up Hotspot Display Settings dialog box.
- A mouse map provides additional ways to control the way your mouse works in a terminal session.

Map Hotspot

Define and add hotspots to the hotspots file using the following options:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hotspot text</td>
<td>Type a text string, up to 80 characters, to identify the hotspot. InfoConnect creates a hotspot wherever this text string is encountered in your host application.</td>
</tr>
<tr>
<td>Select Action</td>
<td>Select an action to associate with the specified hotspot text.</td>
</tr>
</tbody>
</table>

Hotspot Mapper

The hotspot mapper shows all defined hotspot text and their associated actions, which you can modify or delete.

The list shows the order in which hotspots are evaluated. If the same hotspot appears multiple times with different definitions, InfoConnect uses the definition that's evaluated first. Use the Move Up and Move Down buttons to change the order.

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modify</td>
<td>Opens the Hotspot Options dialog box, from which you can modify the characteristics of the hotspot, including the action associated with the hotspot text.</td>
</tr>
<tr>
<td>Delete</td>
<td>Removes the selected hotspot from the hotspot map.</td>
</tr>
</tbody>
</table>

Related Topics

- “Set Up Hotspot Display Settings Dialog Box” on page 173
- “Hotspot Options Dialog Box” on page 171

Hotspot Options Dialog Box

getting there

1 Open a terminal session.
   The steps depend on your user interface mode (page 120).
Under **Terminal Appearance**, click **Manage Hotspots**.

3. Click **Modify the currently selected hotspots file**.

4. Under **Hotspot Mapper**, click **Modify**.

From this dialog box, you can change the action or other characteristics associated with a hotspot.

**Hotspot Options**

Modify the selected hotspot using the following options:

**Hotspot text**
Type a text string, up to 80 characters, to identify the hotspot. *InfoConnect* creates a hotspot wherever this text string is encountered in your host application.

**Select Action**
Select an action to associate with the specified hotspot text.

**Tooltip**
Type the text to display when the mouse cursor is over the hotspot.

**Match case**
Select to make the hotspot case sensitive.

**Only valid at row**
If selected, the hotspot will appear only if the text is in the specified row.

**Only valid at column**
If selected, the hotspot will appear only if the text is in the specified column.

**Auto invoke when text appears on display**
Select to cause the hotspot to be invoked as soon as it appears on the screen.

**Text is preceded by a delimiter**
Select to match the text only if the text is preceded by a delimiter specified under **Hotspot Delimiter**. For example, if you define the hotspot "host" and select this option, the word "unixhost" wouldn't be a hotspot.

**Text is followed by a delimiter**
Select to match the text only if the text is followed by a delimiter specified under **Hotspot Delimiter**. For example, if you define the hotspot "host" and select this option, the word "hostfile" wouldn't be a hotspot.

**Match until a delimiter**
Select to define the end of the hotspot as the delimiter(s) specified under **Hotspot Delimiter**.

**Hotspot Delimiter**

**Space**
Select to use the white space created by pressing the SPACEBAR as a hotspot delimiter.

**Any of these characters**
Select to use any of the listed characters as hotspot delimiters. When this option is selected, you can edit the list of delimiters.
Set Up Hotspot Display Settings Dialog Box

Getting there

1. Open a terminal session.
   The steps depend on your user interface mode (page 120).

   **User Interface Mode** | **Steps**
   --- | ---
   Ribbon or InfoConnect Browser | With a session open in InfoConnect, from the Quick Access Toolbar, click .
   TouchUx | Tap the Gear icon and then select Document Settings.

2. Under Terminal Appearance, click Set Up Hotspot Display Settings.

Hotspots are virtual buttons that appear in terminal sessions. By using hotspots, you can control your terminal session with the mouse instead of the keyboard. Typically, clicking a hotspot transmits a terminal key or command to the host, but you can also configure hotspots to open a Web page, launch a macro, or perform a variety of other actions.

From this dialog box, you can enable hotspots in your terminal session documents, or change the way you activate them.
NOTE: Additional hotspots options are available on the Modify Hotspots dialog box.

Hotspot Display

- **Enable all defined hotspots**
  - Select to enable hotspots in the current session document.
  - When this check box is cleared, you can still define and maintain your hotspot configuration, but hotspots won't work or display on your screen.

- **Hotspot style**
  - Select the way you want hotspots to appear on the screen.
  - If you select Not visible, you can still use hotspots. The pointer changes to an arrow when it's over a hotspot, allowing you to invoke it by clicking the mouse, just as you would if it was visible.

Hotspot Activation

By default, a double-click with the left mouse button activates a hotspot in documents that you create from the InfoConnect 2014 and legacy EXTRA! templates. A single click with the left mouse button activates a hotspot in documents that you create using legacy Reflection templates.

To change the activation method, use the following settings:

- **Choose the mouse button to activate Hotspots**
  - Choose the mouse button (Left, Middle, or Right) that activates a hotspot.
  - Select Double-click to require two clicks of the specified mouse button to activate a hotspot.

- **Choose key(s) to press in combination with mouse click**
  - Select one or more keys to require a key press in combination with the specified mouse click settings to activate a hotspot.

NOTE: You can specify the same mouse action, or mouse chord, to activate a hotspot and to trigger another action. When the pointer is over the hotspot, the mouse action will activate the hotspot; in all other areas of the document, the mouse action will trigger the action you defined in the Mouse Mapper.

Default Hotspot Options

- **Match criteria**
  - Select Match case to make the hotspot case sensitive.

- **Hotspot Delimiters**
  - Select Space to use the white space created by pressing the SPACEBAR as a hotspot delimiter.
  - Select Any of these characters to use any of the listed characters as hotspot delimiters. When this option is selected, you can edit the list of delimiters.

Related Topics

- "Modify Hotspots Dialog Box" on page 170
- "Hotspot Options Dialog Box" on page 171
- "Mouse Mapper" on page 189
Create a New Hotspots File Dialog Box

Getting there

1. Open a terminal session.
   The steps depend on your user interface mode (page 120).

   **User Interface Mode**
   - **Ribbon or InfoConnect Browser**
     - With a session open in InfoConnect, from the **Quick Access Toolbar**, click **Manage Hotspots**.
   - **TouchUx**
     - Tap the Gear icon and then select **Document Settings**.

2. Under **Terminal Appearance**, click **Manage Hotspots**.
3. Click **Create a new hotspots file from an existing hotspots file**.

From this dialog box, select the hotspots file to use as a template for creating a new hotspots file.

**Built-In**
Select this option to show the hotspots files distributed with InfoConnect.

**Custom**
Select this option to show the hotspots files that you've previously modified and saved. If the file you want doesn't appear in the list, click **Browse** to select it.

**NOTE:** The file must be in a trusted location.

**Use the new file in the current session document**
Select this option to use the file you are about to create with the current session.

**Related Topics**
- “Manage Hotspots Dialog Box” on page 169

Specify which Dialog Box to Open when **InfoConnect Starts**

By default, the **Create New Document** dialog box is displayed when you open the **InfoConnect** workspace.

**To specify which dialog box to display when **InfoConnect** opens**

1. Open Workspace Settings.
   The steps depend on your user interface mode (page 120).
Under **Workspace Settings**, click **Configure Workspace Defaults**.

3 In the **When starting workspace** box, select one of the following options.

<table>
<thead>
<tr>
<th>Select this</th>
<th>To do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show New dialog</td>
<td>Display the New dialog box used to choose which type of session to configure.</td>
</tr>
<tr>
<td>Show Open dialog</td>
<td>Display the Open dialog box used to choose a session document file.</td>
</tr>
<tr>
<td>Show nothing</td>
<td>Open the workspace without displaying a dialog box.</td>
</tr>
<tr>
<td>Run Startup Action</td>
<td>Specify an action or sequence of actions to perform when the workspace opens.</td>
</tr>
</tbody>
</table>

### Set Up a Workspace Startup Action Sequence

You can set up **InfoConnect** to perform a series of actions when a workspace starts, rather than when a session opens and connects to the host.

This allows you to automate actions that are independent of a session. For example, if you are creating Visual Basic for Application (VBA) macros, you can set up an action sequence that opens the VB Project Editor, the VBA Help, and the VBA Guide when you open a workspace.

**To set up a workspace startup action sequence**

1 **Open the InfoConnect Workspace Settings dialog box.**

   The steps depend on your [user interface mode](page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ribbon (Office 2007)</td>
<td>On the Reflection button, choose <strong>Reflection Workspace Settings</strong>.</td>
</tr>
<tr>
<td>Ribbon (Office 2010)</td>
<td>On the <strong>File</strong> menu, choose <strong>Reflection Workspace Settings</strong>.</td>
</tr>
<tr>
<td>Reflection Browser</td>
<td>On the Reflection menu, choose <strong>Settings</strong> and then <strong>Reflection Workspace Settings</strong>.</td>
</tr>
<tr>
<td>TouchUx</td>
<td>Tap the Gear icon and then select <strong>Reflection Workspace Settings</strong>.</td>
</tr>
</tbody>
</table>

2 Under **Workspace Settings**, click **Configure Workspace Defaults**.

3 Under **Workspace and Documents**, in the **When starting workspace** list, select **Run Startup action**.
4 Click Select Action.
5 On the left pane of the Select Action dialog box, under Map To, select Action Sequence.
6 Under Run Startup Action, click Add and, in the Action list, choose an action.
7 Repeat Step 6 to add additional actions and complete the action sequence.

Related Topics
• “Run a Startup Macro” on page 875

Specifying a Custom Keyboard Map

Index Term
Primary: mapping
Secondary: keyboard

Index Term
Primary: keyboard
Secondary: overview

A keyboard map lists host terminal keys and their definitions, as well as all defined keystrokes (shortcuts).

Related Topics
• “Select the Keyboard Map for a Session” on page 177
• “Create a Custom Keyboard Map” on page 178
• “Add a Keyboard Shortcut” on page 179
• “Delete a Keyboard Shortcut” on page 180
• “Restore the Default Keyboard Map” on page 181

Select the Keyboard Map for a Session

InfoConnect pre-configures all session documents to use a built-in keyboard map file. You can choose to use a different built-in map, or a custom map that you’ve created.

To select a keyboard map
1 Open the Document Settings dialog box.
   The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ribbon or Reflection Browser</td>
<td>With a session open in Reflection, from the Quick Access Toolbar, click .</td>
</tr>
<tr>
<td>TouchUx</td>
<td>Tap the Gear icon and then select Document Settings.</td>
</tr>
</tbody>
</table>

2 Under Input Devices, click Manage Keyboard Map.
3 Click Select another keyboard map file.
4 Do one of the following:

<table>
<thead>
<tr>
<th>To</th>
<th>Do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select a built-in keyboard map</td>
<td>Click <strong>Built-in</strong>, and then select a map from the list; for example, Default 5250 en.xkb.</td>
</tr>
<tr>
<td>Select a custom keyboard map</td>
<td>Click <strong>Custom</strong>, and then browse to a custom keyboard map file.</td>
</tr>
<tr>
<td><strong>NOTE</strong>: The file must be in a trusted location.</td>
<td></td>
</tr>
</tbody>
</table>

Related Topics

- “Create a Custom Keyboard Map” on page 178
- “Select the Mouse Map for a Session” on page 185
- “Select a Keyboard Map File Dialog Box” on page 182
- “Specify Trusted Locations Dialog Box” on page 329

Create a Custom Keyboard Map

Index Term  
Primary: keyboard  
Secondary: custom

Index Term  
Primary: custom  
Secondary: keyboard map

Host terminal and PC keyboards have different sets of keys; for example, many terminal keyboards have a Transmit key, but PC keyboards do not. InfoConnect pre-configures each session document with a built-in "keyboard map," substituting a PC key (or combination of keys) for the terminal function, so that a PC can communicate with a host in the same way as a terminal. You can create a custom “keyboard map” on page 892 by adding, removing, or redefining keystroke combinations from an existing keyboard map.

To create a custom keyboard map

1. Open the Document Settings dialog box.
   
   The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ribbon or Reflection Browser</td>
<td>With a session open in Reflection, from the Quick Access Toolbar, click</td>
</tr>
<tr>
<td>TouchUx</td>
<td>Tap the Gear icon and then select  Document Settings</td>
</tr>
</tbody>
</table>

2. In the Settings dialog box, under Input Devices, click Manage Keyboard Map.

3. In the Manage Keyboard Map dialog box, click Create a new keyboard map from an existing keyboard map file.

4. In the Create a New Keyboard Map file dialog box, select a keyboard map file to use as a template for your new file (for example, Default 3270.xkb).
5 If you want to use the new keyboard map file in your current session, choose **Use the new file in the current session document**.

6 Click **OK**.

7 Do one of the following:

<table>
<thead>
<tr>
<th>To Do this</th>
<th>To Do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a keystroke definition</td>
<td>Under <strong>Map Keys</strong>, enter a key combination (keystroke) in the box, click the <strong>Select Action</strong> menu, and then choose <strong>Send Key</strong>. From the <strong>Key</strong> drop-down box, choose the host terminal key to which you want to map, and then click <strong>OK</strong>.</td>
</tr>
<tr>
<td>Change the definition of a keystroke</td>
<td>Select the key combination you want to change and click <strong>Modify</strong>. Specify an action for the keystroke, and then click <strong>OK</strong>.</td>
</tr>
<tr>
<td>Remove a keystroke definition</td>
<td>Select the key combination you want to remove, and then click <strong>Delete</strong>.</td>
</tr>
</tbody>
</table>

8 When you are done making changes, click **OK**.

9 When prompted, save the new keyboard map in the **Keyboard Maps** folder.

10 If you are prompted that this is not a secure location, click **Yes**. The file is saved in your **Documents\Attachmate\Reflection\Keyboard Maps** folder.

**Related Topics**

- “Select the Keyboard Map for a Session” on page 177
- “Create a New Keyboard Map File Dialog Box” on page 183

**Add a Keyboard Shortcut**

You can create keyboard shortcuts that perform any assignable action during a **InfoConnect** session. For example, using the **Keyboard Mapper**, you can select a standard action, such as **Send Text** or **Launch Application**, or you can create a macro or complex sequence of actions that you assign to a keystroke.
To add a keyboard shortcut

1 Open the Keyboard Mapper Dialog Box.
   1a Open a session in Reflection.
   1b Open the Reflection Keyboard Mapper dialog box as follows:
      The steps depend on your user interface mode (page 120).

   User Interface Mode          Steps
   Ribbon                       On the Tools ribbon, click Keyboard Mapper.
   Reflection Browser           On the Reflection menu, choose Tools, and then
                                  Keyboard Mapper.
   touchUx                      Tap the Wrench icon and then under Tools, select
                                  Keyboard Mapper.

2 Under Map Keys, enter a keystroke (for example, CTRL+K).

   NOTE: Avoid using keystrokes already defined in the keyboard map.

3 Assign an action by doing one of the following:
   - From the Select Action menu, choose a task (for example, Launch Application).
   -or-
   - Click the Select Action button, and from the Select Action dialog box, specify an action or
     action sequence.

4 Enter parameters for the action, if required, and then click OK.

5 Save your changes to a custom keyboard map file.
   The new keyboard shortcut appears in the table under Keyboard Mapper.

Related Topics
   - “Select Action Dialog Box” on page 161
   - “Create a Custom Keyboard Map” on page 178

Delete a Keyboard Shortcut

1 Open the Keyboard Mapper Dialog Box.
   1a Open a session in Reflection.
   1b Open the Reflection Keyboard Mapper dialog box as follows:
      The steps depend on your user interface mode (page 120).

   User Interface Mode          Steps
   Ribbon                       On the Tools ribbon, click Keyboard Mapper.
   Reflection Browser           On the Reflection menu, choose Tools, and then
                                  Keyboard Mapper.
   touchUx                      Tap the Wrench icon and then under Tools, select
                                  Keyboard Mapper.
2 From the **Keyboard Mapper** table, select the key combination you want to remove.
3 Click **Delete**, and then click **OK**.
4 Save your changes, as needed.

**Restore the Default Keyboard Map**

*Index Term*
- Primary: restore default
- Secondary: keyboard map

*Index Term*
- Primary: keyboard
- Secondary: default

If you have problems using a customized “keyboard map” on page 892 in a session document, you can restore the default keyboard map.

**To restore a default keyboard map**

1 **Open the Document Settings dialog box.**
   - The steps depend on your **user interface mode** (page 120).
   - **User Interface Mode**
     - **Ribbon or Reflection Browser**
       - With a session open in Reflection, from the **Quick Access Toolbar**, click .
     - **TouchUx**
       - Tap the Gear icon and then select .
   - **Steps**
     - **Ribbon or Reflection Browser**
       - With a session open in Reflection, from the **Quick Access Toolbar**, click .
     - **TouchUx**
       - Tap the Gear icon and then select .

2 **Under Input Devices, click Manage Keyboard Map.**
3 Click **Select another keyboard map file**.
4 Click **Built-in**, and select a map from the list that matches your host session; for example, for a 5250 host session, choose Default 5250 en.xkb.
5 Click **OK**.

**Manage Keyboard Map Dialog Box**

**Getting there**

1 **Open a terminal session.**
   - The steps depend on your **user interface mode** (page 120).
   - **User Interface Mode**
     - **Ribbon or InfoConnect Browser**
       - With a session open in **InfoConnect**, from the **Quick Access Toolbar**, click .
     - **TouchUx**
       - Tap the Gear icon and then select .
   - **Steps**
     - **Ribbon or InfoConnect Browser**
       - With a session open in **InfoConnect**, from the **Quick Access Toolbar**, click .
     - **TouchUx**
       - Tap the Gear icon and then select .

2 **Under Input Devices, click Manage Keyboard Map.**
Keyboard map files control the action of keys on your PC keyboard, so that they correspond to specific host keys or provide keyboard shortcuts. When you create a terminal session document, it includes a pointer to a default, built-in keyboard map file. You can choose a different keyboard map file for each session, and you can create custom keyboard map files with the settings you prefer.

**Select another keyboard map file**  
Click to choose a different keyboard map file from a list of existing keyboard map files. The file must be in a trusted location.

**Modify the currently selected keyboard map file**  
Select to modify the keyboard map file used by this session. Because built-in files are read-only, if the currently selected file is a built-in file, it will be saved as a custom file when you change it.

**Create a new keyboard map from an existing file**  
Click to create a custom keyboard map file based on an existing keyboard map file. To reopen the file later, it must be saved in a trusted location.

**Related Topics**
- “Specify Trusted Locations Dialog Box” on page 329

### Select a Keyboard Map File Dialog Box

**Getting there**

1. Open the Document Settings dialog box.
   The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ribbon or Reflection Browser</td>
<td>With a session open in Reflection, from the Quick Access Toolbar, click</td>
</tr>
<tr>
<td>TouchUx</td>
<td>Tap the Gear icon and then select Document Settings.</td>
</tr>
</tbody>
</table>

2. Under Input Devices, click Manage Keyboard Map.
3. Click Select another keyboard map file.

From this dialog box, select a keyboard map file to use with this session.

**Built-In**  
Select this option to show the keyboard map files distributed with InfoConnect.

**Custom**  
Select this option to show the keyboard map files that you’ve previously modified and saved. If the file you want doesn't appear in the list, click Browse to select it.

**NOTE:** The file must be in a trusted location.

**Related Topics**
- “Select the Keyboard Map for a Session” on page 177
- “Specify Trusted Locations Dialog Box” on page 329
Keyboard Mapper

Index Term
Primary: keyboard
Secondary: mapper dialog box

Getting there

1. Open a session in InfoConnect.
2. Open the InfoConnect Keyboard Mapper dialog box as follows:

   The steps depend on your user interface mode (page 120).

User Interface Mode       Steps
Ribbon                     On the Tools ribbon, click Keyboard Mapper.
InfoConnect Browser        On the InfoConnect menu, choose Tools, and then Keyboard Mapper.
TouchUX                    Tap the Wrench icon and then under Tools, select Keyboard Mapper.

With the Keyboard Mapper, you can view and edit terminal keyboard maps, or create keyboard shortcuts.

Map Keys

  Redefine keystrokes using the following options:

| Press the key or key combination that you want to map | Define the combination of keys for the keystroke. |
| Reset                                                  | Resets the selected key combination to None.     |
| Select Action                                          | Select an action to associate with the specified keystroke. |

Keyboard Mapper

  This table shows you all of the defined keystrokes for the map, which you can modify.

| Modify | Opens the Select Action dialog box, from which you can change the action associated with the keystroke. |
| Delete | Removes the selected keystroke from the keyboard map. |

Create a New Keyboard Map File Dialog Box

Getting there

1. Open a terminal session.

   The steps depend on your user interface mode (page 120).
Under Input Devices, click Manage Keyboard Map.

3 Click Create a new keyboard map from an existing keyboard map file.

From this dialog box, select the keyboard map file to use as a template for creating a new keyboard map file.

**Built-In**

Select this option to show the keyboard map files distributed with InfoConnect.

**Custom**

Select this option to show the keyboard map files that you’ve previously modified and saved. If the file you want doesn’t appear in the list, click Browse to select it.

**NOTE:** The file must be in a trusted location.

**Use the new file in the current session document**

Select this option to use the file you are about to create with the current session.

Related Topics

- “Create a Custom Keyboard Map” on page 178
- “Specify Trusted Locations Dialog Box” on page 329

**Specifying a Mouse Map**

A mouse map is a configuration file that shows all of the defined mouse clicks and mouse/key combinations for your mouse. Even though session documents are pre-configured to use the built-in mouse map, you can configure the mouse to help you perform a variety of functions in InfoConnect. For example, you can add mouse actions that connect to hosts, start applications, and perform commands on the InfoConnect graphical interface.

After you add mouse actions in the Mouse Mapper, you can save the modified mouse map as a new, custom mouse map file, which you can use with other session documents.

**Related Topics**

- “Select the Mouse Map for a Session” on page 185
Select the Mouse Map for a Session

A mouse map is a configuration file that shows all of the defined mouse clicks and mouse/key combinations for your mouse. InfoConnect pre-configures all session documents to use a built-in mouse map file. You can choose to use a different built-in map, or a custom map that you’ve created.

To select a mouse map

1 Open the Document Settings dialog box.
   The steps depend on your user interface mode (page 120).

   User Interface Mode   Steps
   Ribbon or Reflection Browser   With a session open in Reflection, from the Quick Access Toolbar, click

   TouchUx   Tap the Gear icon and then select Document Settings.

2 Under Input Devices, click Manage Mouse Map.
3 Click Select another mouse map file.
4 From the Select a Mouse Map File dialog box, do one of the following:

   To    Do this
   Select a built-in mouse map    Click Built-in, and then select a map from the list; for example, mouse.xmm.
   Select a custom mouse map    Click Custom, and then browse to a custom mouse map file.

   NOTE: The file must be in a trusted location.

Related Topics

- “Add a Mouse Action” on page 185
- “Select a Mouse Map File Dialog Box” on page 188
- “Select the Keyboard Map for a Session” on page 177
- “Specify Trusted Locations Dialog Box” on page 329

Add a Mouse Action

Index Term
Primary: mouse
Secondary: action

Index Term
Primary: adding
Secondary: mouse action
Using the **Mouse Mapper**, you can assign an action to a mouse click, or to a mouse click and keystroke combination. Each time you perform that mouse click in **InfoConnect**, the specified action occurs.

### To add a mouse action

1. **Open a session in** **InfoConnect**.
2. **Open the Mouse Mapper Dialog box.**
   
   The steps depend on your **user interface mode** ([page 120](#)).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ribbon</td>
<td>On the <strong>Tools</strong> tab, click <strong>Mouse Mapper</strong>.</td>
</tr>
<tr>
<td>Reflection Browser</td>
<td>On the <strong>Reflection</strong> menu, choose <strong>Tools</strong>, and then <strong>Mouse Mapper</strong>.</td>
</tr>
<tr>
<td>TouchUx</td>
<td>Tap the Gear icon and then select <strong>Document Settings</strong>. Under <strong>Input Devices</strong>, click <strong>Manage Mouse Map</strong>. Then choose whether to modify the current mouse map or create a new map.</td>
</tr>
</tbody>
</table>

3. **Under Map Mouse Click**, place your pointer over the image, and then do either of the following:
   - Click a mouse button.
   - or-
   - Click a mouse button while pressing a modifier key (for example, CTRL).

4. **Assign an action by doing one of the following:**
   - From the **Select Action** menu, choose a task (for example, **Launch Application**).
   - or-
   - Click the **Select Action** button, and from the **Select Action** dialog box, specify an action or action sequence.

5. **Enter parameters for the action**, if required, and then click **OK**.

6. **Save your changes to a custom mouse map file**, if necessary.

   The new mouse action appears in the **Mouse Map** table.

### Delete a Mouse Action

1. **Open a session in** **InfoConnect**.
2. **Open the Mouse Mapper Dialog box.**
   
   The steps depend on your **user interface mode** ([page 120](#)).
3 From the Mouse Mapper dialog box, select the key combination you want to remove.
4 Click Delete, and then click OK.
5 Save your changes, as needed.

**Restore the Default Mouse Map**

Index Term
Primary: restore default
Secondary: mouse map

Index Term
Primary: mouse
Secondary: default map

If you have problems using a customized mouse map in a session document, you can restore the default mouse map.

**To restore a default mouse map**

1 Open the Document Settings dialog box.
   The steps depend on your user interface mode (page 120).

   **User Interface Mode** | **Steps**
   --- | ---
   Ribbon or Reflection Browser | With a session open in Reflection, from the Quick Access Toolbar, click.
   TouchUx | Tap the Gear icon and then select Document Settings.

2 Under Input Devices, click Manage Mouse Map.
3 Click Select another mouse map file.
4 Click Built-in, and select Mouse.xmm from the list.
5 Click OK.

**Manage Mouse Map Dialog Box**

**Getting there**

1 Open a terminal session.
   The steps depend on your user interface mode (page 120).
2 Under **Input Devices**, click **Manage Mouse Map**.

Mouse map files control the way your mouse works in a terminal session. When you create a terminal session document, it includes a pointer to a default, built-in mouse map file. You can choose a different mouse map file for each session, and you can create custom mouse map files with the settings you prefer.

**NOTE:** Hotspots provide additional ways for you to use your mouse to interact with a terminal session.

### Select another mouse map file
- **Steps:** Click to choose a different mouse map file from a list of existing mouse map files. The file must be in a trusted location.

### Modify the currently selected mouse map file
- **Steps:** Select to modify the mouse map file used by this session. Because built-in files are read-only, if the currently selected file is a built-in file, it will be saved as a custom file when you change it.

### Create a new mouse map from an existing file
- **Steps:** Click to create a custom mouse map file based on an existing mouse map file. To reopen the file later, it must be saved in a trusted location.

#### Related Topics
- “Specify Trusted Locations Dialog Box” on page 329
- “Manage Hotspots Dialog Box” on page 169

### Select a Mouse Map File Dialog Box

#### Getting there

1. **Steps:** Open the Document Settings dialog box.
   - **Ribbon or InfoConnect Browser**
     - With a session open in InfoConnect, from the Quick Access Toolbar, click .
   - **TouchUx**
     - Tap the Gear icon and then select Document Settings.

2. **Steps:** Under **Input Devices**, click **Manage Mouse Map**.

3. **Steps:** Click **Select another mouse map file**.

   From this dialog box, select a mouse map file to use with this session.
### Related Topics

- “Select the Mouse Map for a Session” on page 185
- “Specify Trusted Locations Dialog Box” on page 329

### Mouse Mapper

#### Index Term

Primary: mouse  
Secondary: mapper dialog box

#### Getting there

The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ribbon</strong></td>
<td>On the Tools tab, click Mouse Mapper.</td>
</tr>
<tr>
<td><strong>InfoConnect Browser</strong></td>
<td>On the InfoConnect menu, choose Tools, and then Mouse Mapper.</td>
</tr>
<tr>
<td><strong>TouchUx</strong></td>
<td>Tap the Gear icon and then select Document Settings. Under Input Devices, click Manage Mouse Map. Then choose whether to modify the current mouse map or create a new map.</td>
</tr>
</tbody>
</table>

From this dialog box, you can change the way the mouse works in InfoConnect. The session document uses the configured mouse map until you reconfigure it.

#### Map Mouse Click

Define and add mouse clicks (or mouse/key combinations) to the mouse map using the following options:

- **Position your mouse pointer on the image to the left, then click the mouse and key combination you want to map**  
  - Describes the mouse click or mouse/key combination after you perform it on the image to the left; for example, Ctrl+Left.

- **Select Action**  
  - Select an action to associate with the specified mouse/key combination.

- **Reset**  
  - Clears the mouse click or mouse/key combination.
Mouse Mapper

The mouse map shows all defined mouse clicks and mouse/key combinations, which you can modify or delete.

Modify

Opens the Select Action dialog box, from which you can change the action associated with the mouse click.

Delete

Removes the selected key combination from the mouse map.

Related Topics

- “Set Up Hotspot Display Settings Dialog Box” on page 173

Create a New Mouse Map File Dialog Box

Getting there

1. Open a terminal session.
   The steps depend on your user interface mode (page 120).
   
   User Interface Mode
   
   Steps
   
   Ribbon or InfoConnect Browser
   With a session open in InfoConnect, from the Quick Access Toolbar, click .
   
   TouchUx
   Tap the Gear icon and then select Document Settings.

2. Under Input Devices, click Manage Mouse Map.
3. Click Create a new mouse map from an existing mouse map file.

From this dialog box, select the mouse map file to use as a template for creating a new mouse map file.

Built-In

Select this option to show the mouse map files distributed with InfoConnect.

Custom

Select this option to show the mouse map files that you've previously modified and saved. If the file you want doesn't appear in the list, click Browse to select it.

NOTE: The file must be in a trusted location.

Use the new file in the current session document

Select this option to use the file you are about to create with the current session.

Related Topics

- “Specify Trusted Locations Dialog Box” on page 329

Productivity Tools

Index Term
Primary: productivity tools
Productivity features accelerate data entry and host navigation, maximizing user productivity, while reducing errors. Features such as Auto Complete, Auto Expand, Spell Check, Scratch Pad, Recent Typing, and Screen History enable users to save thousands of keystrokes throughout the day, freeing up time to serve customers more efficiently, and for more productive, revenue-producing activities.

Office Tools, Screen History, Recent Typing, and the Scratch Pad open task panes in the document window. To reopen the task panes when you open the workspace, save the workspace as a layout.

**NOTE:** VT sessions support only Office Tools integration, Scratch Pad, and the manual capture function of Screen History. Other productivity features are not available with VT sessions.

### Office Tools Integration

The Office Tools feature allows you to integrate host data with Microsoft Office applications, if those applications are installed on your computer. You can create Word documents and PowerPoint presentations, send e-mail, schedule appointments, add notes and tasks, and create new contacts.

### Screen History

Screen History creates recordings of IBM 3270 and 5250 host screens as you navigate to them. VT screens can be recorded using manual capture. You can view and/or verify the information from those screens, and send multiple host screens to Microsoft Word, PowerPoint, and Outlook (Email Message and Note only), if they are installed on your computer.

### Recent Typing

Using the Recent Typing gallery or task pane, you can quickly view and select from a list of recently typed items, and send the selected string to the active document. This eliminates the need to manually re-enter information, saving time, and reducing errors when entering commonly-typed commands or field data.

### Scratch Pad

Use the Scratch Pad to keep notes associated with a session. From the task pane you can print or save the Scratch Pad notes as .RTF or .TXT files.

### Spelling

Set criteria for the spelling checker. With Spelling options, you can correct spelling automatically, or specify several ways to check spelling as you type.

**NOTE:** Spell check is not supported for Japanese.

### Auto Complete

The Auto Complete feature recalls what you type, and automatically makes suggestions to help populate fields as it learns common commands that are repeated. By default, typing is saved with the screen location, and suggested when you type at that screen location again.

### Auto Expand

Use the Auto Expand feature to add acronyms or shortcuts for long words, phrases, or complex repeat commands. The shortcut, when typed and followed by the Spacebar, automatically expands to the full word or phrase.
In this Section

- “Integrate Host Data with Office Tools” on page 192
- “Enter Data with Recent Typing” on page 195
- “Take Notes with Scratch Pad” on page 196
- “Enter Data with Auto Complete” on page 197
- “Enter Data with Auto Expand” on page 198
- “Find and Fix Spelling Errors” on page 199
- “Create a Custom Spell Check Dictionary” on page 201
- “Configure Office Tools Dialog Box” on page 202
- “Office Tools Dialog Box” on page 203
- “Configure Recent Typing Dialog Box” on page 204
- “Configure Auto Complete Dialog Box” on page 205
- “Configure Auto Expand Dialog Box” on page 207
- “Configure Spell Checking Dialog Box” on page 208
- “Configure Productivity Defaults Dialog Box” on page 210

Integrate Host Data with Office Tools

Index Term
Primary: word processing

Index Term
Primary: sticky notes

Index Term
Primary: sending data
Secondary: to Office applications

Index Term
Primary: screen history
Secondary: send to Office tools

Index Term
Primary: presentation

Index Term
Primary: PowerPoint

Index Term
Primary: Outlook

Index Term
Primary: Office tools
Secondary: word processing

Index Term
Primary: Office tools
Secondary: send data to

Index Term
Primary: Office tools
Secondary: presentation
You can send entire host screens or selected data directly to Microsoft Office products installed on your computer.

To copy and paste host screens or data, see “Copy and Paste Host Data” on page 39.

To send data from the current screen to an Office component

1. Navigate to the host data you want to send.
2. Select specific data to send.
   -or-
   To send the entire screen, don’t select anything.
3. Do one of the following:
   The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ribbon</td>
<td>Click the Office Tools split button to open the Office Tools docking pane.</td>
</tr>
<tr>
<td>InfoConnect Browser</td>
<td>On the InfoConnect menu, choose Send to.</td>
</tr>
<tr>
<td>TouchUx</td>
<td>On the toolbar, tap the Office Tools icon.</td>
</tr>
</tbody>
</table>
Choose the Office component to receive the host data.

To send host screens from screen history to an Office component

1. Open the Screen History task pane.
   The steps depend on your user interface mode (page 120).

   **User Interface Mode**                     **Steps**
   Ribbon                                       On the **Session** ribbon, click the **Screen History** button.
   InfoConnect Browser                         On the InfoConnect menu, choose **View** and then **Screen History**.
   TouchUx                                      Tap the Wrench icon and then under **View**, choose **Screen History**.

2. From the toolbar in the **Screen History** task pane, click the **Office Tools** button.
3. Select the screens that you want to send.
4. From the **Document Type** list box, select the type of Office document that you want to create:

   **Choose**                        **To do this**
   **Word processing document**   Create a Word document that includes the selected screens as text or images — specify which in the **Insert screens** list box.
   **Presentation**                 Create a PowerPoint presentation that includes the selected screens as bitmap images.
   **Email message**                Create an Outlook e-mail message that includes the selected screens as text.
   **Note**                        Create an Outlook "sticky" note that includes the selected screens as text.

5. Click **OK**.

**Related Topics**

- “Copy and Paste Host Data” on page 39
Enter Data with Recent Typing

Using the Recent Typing gallery or task pane, you can quickly view and select from a list of recently typed items, and send the selected string to the active document. This eliminates the need to manually re-enter information, saving time, and reducing errors when entering commonly-typed commands or field data.

NOTE

- This feature is not available with VT sessions.
- Typing is not captured in hidden-text fields such as passwords.

To enter data with Recent Typing

1. Navigate to the host field where you want to input the data.
2. Open the Recent Typing gallery or task pane.
3. Double-click the string you want to input.

The following commands are also available from the toolbar in the Recent Typing task pane:

Click | To do this
-----|------------------------
 ![File] | Open a previously saved Recent Typing file.
 ![Save] | Save the contents of the Recent Typing task pane as a file (.RRTL). When you close your session, your recent typing items are not maintained unless you save them to a separate file.
 ![Delete] | Delete the selected item.
 ![Clear] | Clear all of the contents at once.
 ![AutoHide] | Put the task pane into auto-hide mode. This collapses the task pane against the side of the application frame. (To re-open the task pane, mouse over the side of the frame.)

NOTE: You can use the keyboard to locate (and select) recently typed items in the list. For example, press the A key to locate the most recently typed item beginning with the letter A.
Take Notes with Scratch Pad

Use the Scratch Pad to keep notes associated with a session. From the task pane you can print or save the Scratch Pad notes as .RTF or .TXT files.

To reopen the file later, it must be saved in a trusted location.

To take notes with Scratch Pad

1. Open the Scratch Pad.
   - Open the InfoConnect Scratch Pad as follows:
     - The steps depend on your user interface mode (page 120).

2. Type your notes into the Scratch Pad.
3. Save your notes by clicking the Save As toolbar button.

The following commands are also available from the toolbar in the Scratch Pad task pane (You can also use common keyboard shortcuts like CTRL+A, CTRL+C, and so on):

   Click   To do this
   ![Save]  Save the contents of the Scratch Pad task pane as a Rich Text File (.RTF) or as plain text (.TXT). When you close your session, your Scratch Pad is not maintained unless you save it to a separate file.
   ![Open]  Open any .RTF or .TXT file.
   ![Print]  Print the contents of the Scratch Pad.
   ![Cut]  Cut the selected item and copy it to the Clipboard.

   The file must be in a trusted location.
The Auto Complete feature recalls what you type, and automatically makes suggestions to help populate fields as it learns common commands that are repeated. By default, typing is saved with the screen location, and suggested when you type at that screen location again.

**NOTE:** Auto Complete does not record typing in hidden-text fields such as passwords, nor does it offer suggestions to complete typing in such fields.

To enter data with Auto Complete, you must first have some suggestion data saved with your session. To generate suggestion data, type a string into a host field, followed by a Spacebar or a host key (Tab, field exit, AID key, and so on). The data is associated only with the field in which it was entered, unless you are configured to use field independent Auto Complete (select the Make Suggestions from All Screen Data option on the Configure Auto Complete dialog box).

This feature is not available with VT sessions.

**To enter data with Auto Complete**

1. Begin typing text into a host field.
   - A pop-up window may appear with one or more suggestions, depending on your Auto Complete configuration and previous data entry activity.
2. If the suggestion is correct, press the ENTER key to input the data.
   - or-

---

**Related Topics**

- “Specify Trusted Locations Dialog Box” on page 329

**Enter Data with Auto Complete**

Index Term

Primary: typing suggestions

Index Term

Primary: suggestions when typing

Index Term

Primary: data entry
Secondary: typing suggestions

Index Term

Primary: auto complete
Secondary: using
If there are multiple suggestions, use the Up and Down Arrow keys on your keyboard to scroll through the suggestion list.

3  (Optional) To prevent the active suggestion from being suggested again in the current field, press the ESC key.

As you continue typing, the pop-up window will remain open until the word being typed no longer matches any previous suggestion data.

Related Topics

- “Configure Auto Complete Dialog Box” on page 205
- “Configure Productivity Defaults Dialog Box” on page 210

## Enter Data with Auto Expand

Use the Auto Expand feature to add acronyms or shortcuts for long words, phrases, or complex repeat commands. The shortcut, when typed and followed by the Spacebar, automatically expands to the full word or phrase.

### NOTE

- This feature is not available with VT sessions.
- Expansion does not occur in hidden-text fields such as passwords.

### To enter data with Auto Expand

1. Build a dictionary in the Auto Expand Settings.
   1a  Open the Document Settings dialog box.

   The steps depend on your user interface mode (page 120).
1b On the Settings dialog box, under Productivity, click Configure Auto Expand
1c From the Configure Auto Expand dialog box, create the desired Auto Expand definitions.
1d Click OK.

2 To insert data using Auto Expand, in the host field where you want the expanded data, type the abbreviation for an entry, and then press the Spacebar key.

The abbreviation is replaced with the Auto Expand definition you specified.

Related Topics

- “Configure Auto Expand Dialog Box” on page 207
- “Configure Productivity Defaults Dialog Box” on page 210

Find and Fix Spelling Errors

By default, spell check works as you type, using wavy underlines to indicate possible errors. If you prefer to wait until after you’ve finished entering content to make corrections, or you find the wavy underlines distracting, you can hide them.

NOTE: This feature is not available with VT sessions.

To show or hide spelling corrections as you type

1 Open the Configure Spell Checking dialog box.

The steps depend on your user interface mode (page 120).
From the **Configure Spell Checking** page, select or clear **Check spelling as you type**.

### To correct spelling as you type

1. Open the **Configure Spell Checking** dialog box.
   - The steps depend on your user interface mode (page 120).

2. From the **Configure Spell Checking** page, select **Automatically correct spelling as you type**.
   - Commonly misspelled words are corrected without prompt or indication as you type.
   - **NOTE:** This feature is available only for English.

### To correct an error

1. Right-click a word with a wavy underline, and then select the alternate spelling or correction you want.

2. If the spelling you want is not in the suggestion list, or if no suggestions appear, enter the correct spelling manually.
   - You can also add the item to a custom spell-check dictionary to make it available in the future.
   - For more information, see “Create a Custom Spell Check Dictionary” on page 201.
   - **NOTE:** If no suggestions appear, there aren’t any available, or the suggestions available are too long to fit in the remaining space in the field.

Use the procedure below to check spelling on the entire screen, not just typed text.

### To check spelling on the whole screen

1. Select **Check Screen**.
   - Check for possible errors as follows:
Possible spelling errors are indicated with wavy underlines.

**NOTE:** Check Screen is disabled if you have cleared the Check spelling as you type check box.

2 Right-click a word with a wavy underline, and then select the alternate spelling or correction you want.

**Related Topics**
- “Configure Spell Checking Dialog Box” on page 208
- “Create a Custom Spell Check Dictionary” on page 201
- “Configure Productivity Defaults Dialog Box” on page 210

**Create a Custom Spell Check Dictionary**

To increase the usefulness of the spell check feature, it helps to create a custom spell check dictionary, and add words to it that may be specific to your business or industry that are not included in the main dictionary. When you use spell check, both the main dictionary and your custom dictionary will be used.
NOTE

- This feature is not available with VT sessions.
- Spell check is not supported for Japanese.
- The spell check dictionaries are not used to correct spelling as you type. Instead, that feature uses a separate file of commonly misspelled words.

To create a custom spell check dictionary

1. Open the Configure Spell Checking dialog box.
   The steps depend on your user interface mode (page 120).

   User Interface Mode | Steps
   -------------------|-----------------------------------------------
   Ribbon | On the Tools ribbon, from the Tools group, click Spell Check.
   Reflection Browser | In the search box, enter S and then, under Actions, choose Spell Check Settings.
   TouchUx | Tap the Gear icon and select Document Settings. Then, under Productivity, select Configure Spell Checking.

2. In the Custom Dictionary File field, type the path and filename that you want for your custom dictionary file.
   The filename must have an extension (we recommend .tlx).

3. Click OK.
   The file is created for you.

To add items to your custom spell check dictionary

1. On a host screen, right-click an item marked as misspelled that you want to add to your dictionary.

2. From the list that appears, choose Add to Dictionary.

Related Topics

- “Configure Spell Checking Dialog Box” on page 208
- “Find and Fix Spelling Errors” on page 199

Configure Office Tools Dialog Box

Index Term
Primary: Office tools
Secondary: configuring

Getting there

1. Open a terminal session.
   The steps depend on your user interface mode (page 120).
2 Under **Productivity**, click **Configure Office Tools**.

The Office Tools feature allows you to integrate host data with Microsoft Office applications, if those applications are installed on your computer. You can create Word documents and PowerPoint presentations, send e-mail, schedule appointments, add notes and tasks, and create new contacts.

### Office Tools Defaults

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Presentation template file</strong></td>
<td>Set the default presentation template file.</td>
</tr>
<tr>
<td><strong>Word-processing template file</strong></td>
<td>Set the default word-processing template file.</td>
</tr>
<tr>
<td><strong>Close Office documents when exiting the workspace</strong></td>
<td>Select to close Office documents when exiting InfoConnect. If the documents are not saved, Office will prompt you to save them before closing.</td>
</tr>
</tbody>
</table>

#### Related Topics

- “Integrate Host Data with Office Tools” on page 192
- “Office Tools Dialog Box” on page 203

### Office Tools Dialog Box

#### Getting there

1. Open the Document Settings dialog box.

   The steps depend on your **user interface mode** (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ribbon or InfoConnect Browser</strong></td>
<td>With a session open in InfoConnect, from the Quick Access Toolbar, click 📖.</td>
</tr>
<tr>
<td><strong>TouchUx</strong></td>
<td>Tap the Gear icon and then select 📖 <strong>Document Settings</strong>.</td>
</tr>
</tbody>
</table>

2. On the Settings dialog box, under **Productivity**, click **Configure Office Tools**.

   **NOTE:** You can also access the Office Tools dialog box by clicking 📖 in the Screen History task pane.
Use this dialog box, accessible from the Screen History task pane, to send multiple screens from Screen History to Microsoft Word, PowerPoint, and Outlook (Email Message and Note only). To use this feature, Microsoft Office applications must be installed on your computer.

**NOTE:** Only text areas of the host screen are included in the recorded image; host graphics images are not included.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Screens</td>
<td>Displays a thumbnail of all screens in the current screen history file.</td>
</tr>
<tr>
<td>Select All</td>
<td>Click to select all the screens in the current screen history file.</td>
</tr>
<tr>
<td>Select None</td>
<td>Click to clear selection of all the screens in the current screen history file.</td>
</tr>
<tr>
<td>Document type</td>
<td>Select the type of Microsoft Office document you want to create.</td>
</tr>
<tr>
<td>Insert screens</td>
<td>Select Text to insert the selected screens as text; or Images to insert the selected screens as a bitmap.</td>
</tr>
</tbody>
</table>

**Related Topics**
- “Integrate Host Data with Office Tools” on page 192
- “Configure Office Tools Dialog Box” on page 202

## Configure Recent Typing Dialog Box

**Index Term**
- Primary: recent typing
- Secondary: configuring

**Index Term**
- Primary: capture
- Secondary: recent typing

### Getting there

1. Open the Document Settings dialog box. The steps depend on your user interface mode (page 120).

   **User Interface Mode** | **Steps** |
   --------------- |-----------|
   Ribbon or **InfoConnect** Browser | With a session open in **InfoConnect**, from the **Quick Access Toolbar**, click **Document Settings**. |
   **TouchUx** | Tap the Gear icon and then select **Document Settings**. |

2. On the Settings dialog box, under **Productivity**, click **Configure Recent Typing**. Using the Recent Typing gallery or task pane, you can quickly view and select from a list of recently typed items, and send the selected string to the active document. This eliminates the need to manually re-enter information, saving time, and reducing errors when entering commonly-typed commands or field data.
NOTE

- This feature is not available with VT sessions.
- Typing is not captured in hidden-text fields such as passwords.

Options

Number of words to remember

InfoConnect identifies and remembers new typed words when a field is exited by Tab key, Spacebar, or other terminal-specific method.

Minimum word length (characters)

This feature defines the number of characters that InfoConnect considers a word. At the default setting of 3 characters, if you type something such as "US" into a field, it will not be remembered, and does not appear on the Recent Typing gallery and task pane.

Clear recent typing list when disconnected

When selected, the Recent Typing list is deleted when the session is disconnected for any reason. When cleared, the Recent Typing list is deleted when the session is closed.

NOTE: If the Recent Typing list has been saved to a file, the recent typing file is not affected.

Related Topics

- “Enter Data with Recent Typing” on page 195
- “Configure Productivity Defaults Dialog Box” on page 210

Configure Auto Complete Dialog Box

Index Term
Primary: auto complete
Secondary: configure

Getting there

1. Open the Document Settings dialog box.
   The steps depend on your user interface mode (page 120).

   User Interface Mode         Steps
   Ribbon or InfoConnect Browser With a session open in InfoConnect, from the Quick Access Toolbar, click ➤.
   TouchUx                      Tap the Gear icon and then select ➤ Document Settings.

2. On the Settings dialog box, under Productivity, click Configure Auto Complete.

The Auto Complete feature recalls what you type, and automatically makes suggestions to help populate fields as it learns common commands that are repeated. By default, typing is saved with the screen location, and suggested when you type at that screen location again.
NOTE

- This feature is not available with VT sessions.
- To use Auto Complete with uppercase only fields, clear the Use case sensitivity for suggestions option. Uppercase only fields are required to support alpha data on Japanese systems. They are also common on AS/400 systems for which 5250 emulation is used.

Options

Suggestions

Use case sensitivity for suggestions
Clear this check box to have Auto Complete ignore case when you are typing in a host field.

Make suggestions from all screen data
When selected, Auto Complete makes suggestions based on all user data that has been entered into any field used during the session. Field independent Auto Complete results in many more suggestions in many more screen locations.

Save suggestion data in session file
When selected, Auto Complete "remembers" the data entered during the current session, so that if the session is closed, and then reopened, suggestions will still be available.

Clear suggestions
Clears stored suggestions created from data entered by users. The next typed entry will begin creating a new set of data from which Auto Complete suggestions are made.

Characters typed before suggestions are made
After you type this number of characters, the suggestion pop-up appears.

Maximum number of suggestions
Select the maximum number of items you want Auto Complete to suggest for any word.

Maximum word length to offer suggestions on
Specify the longest word on which to apply Auto Complete. Longer words are ignored by this feature.

Overwrite and Insert

These options determine how Auto Complete behaves when entering a definition into a field with pre-existing data.

Wrap text into next field
If the Auto Complete suggestion pushes existing data past the end of the field, the additional data is added at the beginning of the next available field.

Erase to the end of the field after inserting Auto Complete suggestion
Select to have all other data in the field deleted after the Auto Complete suggestion is entered.

Insert mode
Select to maintain existing field data, with the Auto Complete suggestion inserted at the cursor location.

If the insertion pushes existing data past the end of the field, the data is truncated.

Overwrite mode
Select to overwrite only the data that exists where the Auto Complete suggestion is being placed. Other data in the field will not be affected.
NOTE: Auto Complete does not record typing in hidden-text fields such as passwords, nor does it offer suggestions to complete typing in such fields.

Related Topics

- “Enter Data with Auto Complete” on page 197
- “Configure Productivity Defaults Dialog Box” on page 210

Configure Auto Expand Dialog Box

Index Term
Primary: dictionary
Secondary: auto expand

Index Term
Primary: auto expand
Secondary: configure

Getting there

1 Open the Document Settings dialog box.
   The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ribbon or InfoConnect</td>
<td>With a session open in InfoConnect, from the Quick</td>
</tr>
<tr>
<td>Browser</td>
<td>Access Toolbar, click</td>
</tr>
<tr>
<td>TouchUx</td>
<td>Tap the Gear icon and then select Document Settings.</td>
</tr>
</tbody>
</table>

2 On the Settings dialog box, under Productivity, click Configure Auto Expand.

You can build a "dictionary" of “Auto Expand” on page 892 definitions for the current session.

NOTE

- This feature is not available with VT sessions.
- Expansion does not occur in hidden-text fields such as passwords.
- To use Auto Expand with uppercase only fields, clear the Use case sensitivity when expanding option. Uppercase only fields are required to support alpha data on Japanese systems. They are also common on AS/400 systems for which 5250 emulation is used.
Definitions
Select the row, or double-click in the fields to enable text entry.

* Click to select the entire row. With the row selected, you can begin typing into the Abbreviation field, or you can delete the row with the Delete key.

Abbreviation
Type the acronym or shortcut to enter on the host screen. The shortcut is expanded to the long word, phrase, or command entered in the Expansion field on the same row. Spaces are not permitted in the Abbreviation text box.

Expansion
Type the long word, phrase, or command to associate with the acronym or shortcut entered in the Abbreviation field on the same row.

Options
Use case sensitivity when expanding
Clear this check box to have Auto Expand ignore case when you are typing in a host field.

Auto Expand abbreviations cannot be duplicated in the dictionary, regardless of case, even if this option is selected.

To use Auto Expand with uppercase only fields, clear this option.

Wrap text into next field
Select to prevent expansions from being truncated if they don’t fit in the current field. Characters that don’t fit are entered into the next unprotected field on the host screen.

Overwrite and Insert
These options determine how Auto Expand behaves when entering a definition into a field with pre-existing data.

Erase to the end of the field after inserting Auto Expand definition
Select to have all other data in the field deleted after the Auto Expand definition is entered.

Insert mode
Select to maintain existing field data, with the Auto Expand definition inserted at the cursor location.

If the insertion pushes existing data past the end of the field, the data is truncated.

Overwrite mode
Select to overwrite only the data that exists where the Auto Expand definition is being placed. Other data in the field is not affected.

Related Topics
- “Enter Data with Auto Expand” on page 198
- “Configure Productivity Defaults Dialog Box” on page 210

Configure Spell Checking Dialog Box
Index Term
Primary: spell check
Secondary: configuring
Getting there

1. Open the Document Settings dialog box.
The steps depend on your user interface mode (page 120).

   **User Interface Mode**
   - Ribbon or **InfoConnect** Browser
   - **TouchUX**

   **Steps**
   - With a session open in **InfoConnect**, from the **Quick Access Toolbar**, click ➤.
   - Tap the Gear icon and then select ➤ **Document Settings**.

2. On the Settings dialog box, under **Productivity**, click **Configure Spell Checking**.

   From this settings page, you can customize the way Spell Check works.

---

**NOTE**

- This feature is not available with VT sessions.
- Spell check is not supported for Japanese.

**Options**

- **Check spelling as you type**
  - Spell Check marks possible errors with wavy underlines.

- **Automatically correct spelling as you type**
  - Commonly misspelled words are corrected without prompt or indication as you type.
    
    **NOTE**: This feature is available only for English.

- **Ignore words in UPPERCASE**
  - If you are typing in UPPERCASE letters, Spell Check does not attempt to correct spelling.

- **Ignore words with numbers**
  - If you are typing a word with a number in it, like Reflection2014, Spell Check does not attempt to correct the spelling.

- **Correct TWO INITIAL CAPITALS**
  - If you type two consecutive uppercase letters at the beginning of a word, Spell Check changes the second uppercase letter to a lowercase letter; for example, **ENter** changes to **Enter**.

- **Correct accidental usage of cAPS LOCK key**
  - If you accidentally type a word in Title Case with the CAPS LOCK key turned on, Spell Check corrects the capitalization; for example, **ENTER kEY** changes to **Enter Key**.

- **Custom dictionary file**
  - Specify the path to the custom dictionary for the current session. For more information see the “Create a Custom Spell Check Dictionary” on page 201 topic.

- **Minimum field size to check spelling**
  - Specify the shortest field in which to check spelling.

- **Maximum word length to check spelling**
  - Specify the longest word to check for spelling. Longer words are ignored by the spell checker.
Configure Productivity Defaults Dialog Box

Getting there

1. Open the Document Settings dialog box. The steps depend on your user interface mode (page 120).

   **User Interface Mode** | **Steps**
   --- | ---
   Ribbon or InfoConnect Browser | With a session open in InfoConnect, from the Quick Access Toolbar, click .
   TouchUx | Tap the Gear icon and then select Document Settings.

2. On the Settings dialog box, under Productivity, click Configure Productivity Defaults.

   Use this settings page to enable or disable certain Productivity features for the current session.

**NOTE:** VT sessions support only Office Tools integration, Scratch Pad, and the manual capture function of Screen History. Other productivity features are not available with VT sessions.

**Default Productivity Settings**

- **Enable Recent Typing**
  - Select to enable this feature.
  - Using the Recent Typing gallery or task pane, you can quickly view and select from a list of recently typed items, and send the selected string to the active document. This eliminates the need to manually re-enter information, saving time, and reducing errors when entering commonly-typed commands or field data.

- **Enable Auto Complete**
  - Select to enable this feature.
  - The Auto Complete feature recalls what you type, and automatically makes suggestions to help populate fields as it learns common commands that are repeated. By default, typing is saved with the screen location, and suggested when you type at that screen location again.
Enable Auto Expand

Select to enable this feature.

Use the Auto Expand feature to add acronyms or shortcuts for long words, phrases, or complex repeat commands. The shortcut, when typed and followed by the Spacebar, automatically expands to the full word or phrase.

Enable Spell Check

Select to enable this feature. Clearing this check box disables both automatic and manual spell check.

NOTE: Spell check is not supported for Japanese.

Related Topics

- “Enter Data with Recent Typing” on page 195
- “Enter Data with Auto Complete” on page 197
- “Enter Data with Auto Expand” on page 198
- “Find and Fix Spelling Errors” on page 199

IBM 3270 Sessions

Index Term
Primary: sessions
Secondary: IBM 3270

Index Term
Primary: host connection
Secondary: IBM 3270

Index Term
Primary: connecting to the host
Secondary: IBM 3270

This section includes detailed information on configuring your IBM 3270 terminal sessions.

In this Section

- “Connect 3270 Sessions using the Express Logon Feature (ELF)” on page 212
- “3270 Terminal Document Settings Dialog Box” on page 213
- “Configure Connection Settings Dialog Box” on page 215
- “Set Up Backup Connection Settings Dialog Box” on page 218
- “Configure Advanced Connection Settings Dialog Box” on page 221
- “Select Host Code Page Dialog Box (3270)” on page 228
- “Configure Terminal Settings Dialog Box” on page 229
- “Configure Terminal Attributes Dialog Box” on page 232
- “Editing a Host Code Page” on page 233
Connect 3270 Sessions using the Express Logon Feature (ELF)

Use this procedure to configure a 3270 session to connect to the host using the "Express Logon Feature (ELF)" on page 891.

This procedure includes four parts:

1. Configure the host for ELF
2. Install digital certificates on the host and client
3. Configure ELF for a 3270 session
4. Record the connect macro that logs on using the ELF token values

**NOTE:** If you connect to the host using ELF through the Reflection Security Gateway, you must configure End-to-End encryption from the Administrative WebStation. For more information, see the InfoConnect Installation and Deployment Guide.

To configure the Host for ELF

1. Configure the host to support SSL/TLS connections.
2. Configure ELF and note the applid value.

For instructions, see the documentation included with the IBM host.

To install digital certificates on the host and client

To make connections using ELF, all Reflection users must have both host and personal certificates installed. (If the certificates are from a trusted Certificate Authority, you only need to install personal certificates.) For more information, refer to Technical Note 1757 (http://support.attachmate.com/techdocs/1757.htm).

To configure ELF for a 3270 session

1. Create a new 3270 session document:
   1a. Specify the **Host name/ IP Address**. If your configuration requires the host name to match the certificate, enter the name that exactly matches the CommonName or the SubjectAltName field specified in the host certificate.
   1b. Specify the **Port** used for SSL connections by your host. This is configured by the IBM host administrator.

2. Select the **Configure additional settings** check box and click **OK**.

3. Under Host Connection, click **Configure Connection Settings**.

4. (Recommended) Under **Host Connection Options, When connection is terminated**, choose **Leave disconnected**.

   Because you are configuring automatic logon, your user name and password are no longer necessary. This means you will be logged back in immediately after every log off if the default **Reconnect automatically** is selected. If you prefer to leave Auto Reconnect on while you're working, you can create a logoff macro that turns off this setting just prior to logging off.

5. Click **Configure > Advanced Connection Settings**.

6. Scroll down to **Security** and in the **ELF application ID** box, enter the applid value from the host.
7 Click Security Settings, and in the Security Properties dialog box, do the following:
   7a Select Use SSL/TLS security.
   7b (Optional) Change the values for Encryption strength and SSL/TLS version.
   7c Specify a value for ELF application ID. For example, the application ID (applid) for TSO is TSO+smfid (located in the SMFPRMxx member of SYS1.PARMLIB). For additional information, refer to the IBM system documentation.

8 Save your settings.

To record a connect macro that logs on using the ELF token values

1 Open the 3270 session file you just created. (You should be connected but not yet logged on.)
2 Start the macro recorder.
3 Log on using a valid user name and password. (Editing your macro will be easiest if you don’t include your user name when you enter the logon command. Type the logon, press Enter, then type your user name.) You will edit the macro to remove specific user information and replace it with ELF token values that support logon by any authenticated user.
4 Stop the macro recorder.
5 In the Stop Recording dialog box, name the macro (for example "ELF logon"), select Make this the connect macro, and Click OK.
6 Open the Visual Basic Editor.
7 Edit the TransmitANSI statement that sends your user name. Remove your user name and replace it with the ELF token )USR.ID(. The edited line will look like this:

   .TransmitANSI " )USR.ID("

8 Comment out or delete the line that uses the GetPassword method to set the password. Replace it with a new line that sets the password variable equal to the ELF password token )PSS.WD(. The modified code should look like this:

   Dim hostpassword As String
   'hostpassword = .GetPassword(" Password ===>", ", ", ", ")
   hostpassword = " )PSS.WD("
   .TransmitANSI hostpassword

9 Save the session file.
10 Connect using the modified Reflection session. You should connect and be logged in without having to enter a user name and password.

3270 Terminal Document Settings Dialog Box

Getting there

1 Open the Create New Document dialog box.
   The steps depend on your user interface mode (page 120).
2 From the Create New Document dialog box, select a 3270 terminal session template, and then click **Create**.

**Connection**

**Enter Host (or System) Name or IP Address**

Identify the host to which you will connect. Type the host name, alias, or numeric IP address.

**NOTE:** Both IPv4 addresses (in the form 127.0.0.1) and IPv6 addresses (in the form 2001:0db8:3c4d:0015:0000:0000:abcd:ef12) are accepted.

**Port**

Type the host port or socket number that the session should use. This field accepts any number between 0 and 66,535 (default = 23).

**Device name**

Specify a particular LU or pool of LUs (up to 32 characters) on the host. If no device name is entered, the server connects to any available LU at the specified port.

**Use Telnet Extended**

If selected, enables TN3270E protocols when supported.

**Terminal**

**Terminal/Device type**

Specify the model of the terminal or device type emulated by this session.

You can select a value from the drop-down box, or type a value that is not listed. This allows you to specify a terminal model that is not implicitly supported but might work, such as Fujitsu.

In most cases you should leave this setting at the default value. If you choose any other value, be sure to use a string that is acceptable to the host; otherwise, you may experience problems connecting to the host, and emulation problems after connecting to the host. Typically, these types of problems occur if the host is not configured to recognize the terminal specified.
### Configure Connection Settings Dialog Box

**Model ID**
Specify the model of the terminal or device type emulated by this session.

If the string specified in Terminal/Device type includes &M, the &M is replaced with the model number from this list when the string is sent to the host. For example, if IBM-3279-&M is specified and Model 3 is selected here, the string sent to the host is IBM-3279-3.

Selecting an Extended model allows the host to specify a greater number of colors (seven instead of four) and a wider variety of display attributes. Any Model allows the gateway or mainframe to determine which model ID to use.

Each model is associated with a terminal window display of a specific size (e.g., 24 rows by 80 columns). To specify a different number of rows or columns, select <Custom Model Extended>. When Model ID is set to <Custom Model Extended>, Terminal/Device type changes to IBM-DYNAMIC.

The default value is Model 2 24x80 Extended.

**Rows**
The number of rows to use in the terminal window display. The valid range is 24 - 255.

If the host application specifies a particular screen size, this value may be ignored.

**Columns**
The number of columns to use in the terminal window display. The valid range is 80 - 255.

If the host application specifies a particular screen size, this value may be ignored.

**Enable graphics**
When selected, enables this session to emulate a graphics terminal.

This allows you to run any host application that uses the IBM Graphics Data Display Manager (GDDM) library, such as SAS or ImageView.

**Host code page**
Select the language and associated host code page to be used by your session. If you are not sure which language and code page to use, check with your system administrator. The default is US English, code page 037.

**Keyboard map**
Specify the keyboard map to use with this session.

**Configure additional settings**
Select to open a page from which you can customize host connection, terminal configuration, and other settings for this session.

When selected, the session does not auto-connect. This allows you to modify settings before connecting to the session.

### Related Topics
- “Create a Session Document File” on page 147
- “Configure Connection Settings Dialog Box” on page 215
- “Editing a Host Code Page” on page 233
1 Open a 3270 terminal session.
   The steps depend on your user interface mode (page 120).

   **User Interface Mode**
   - **Ribbon or InfoConnect Browser**
     With a session open in InfoConnect, from the Quick Access Toolbar, click 📧.
   - **TouchUx**
     Tap the Gear icon and then select 📁 Document Settings.

2 Under **Host Connection**, click **Configure Connection Settings**.
From this dialog box, you can specify the settings for a TN3270 connection.

**Connection**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Host name/IP address</strong></td>
<td>Identify the host to which you will connect. Type the host name, alias, or numeric IP address.</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>Type the host port or socket number that the session should use. This field accepts any number between 0 and 66,535 (default = 23).</td>
</tr>
<tr>
<td><strong>Device name</strong></td>
<td>Specify a particular LU or pool of LUs (up to 32 characters) on the host. If no device name is entered, the server connects to any available LU at the specified port.</td>
</tr>
</tbody>
</table>
Host Connection Options

Use Telnet Extended
If selected, enables TN3270E protocols when supported.

Automatically connect to the host
Select to establish a host connection as soon as the associated session document is opened.

When connection is terminated
Specify options for reconnecting after any disconnection that is not initiated from InfoConnect.

Choose
To have InfoConnect...

Reconnect automatically
Attempt to reestablish the connection.

Prompt for reconnection
Prompt whether to attempt to reestablish the connection. (When No is selected, the session is left open and disconnected.)

Leave disconnected
Leave the session disconnected with the session open.

Close session automatically
Close the session.

Text Display

Terminal/Device type
Specify the model of the terminal or device type emulated by this session.

You can select a value from the drop-down box, or type a value that is not listed. This allows you to specify a terminal model that is not implicitly supported but might work, such as Fujitsu.

In most cases you should leave this setting at the default value. If you choose any other value, be sure to use a string that is acceptable to the host; otherwise, you may experience problems connecting to the host, and emulation problems after connecting to the host. Typically, these types of problems occur if the host is not configured to recognize the terminal specified.

Model ID
Specify the model of the terminal or device type emulated by this session.

If the string specified in Terminal/Device type includes &M, the &M is replaced with the model number from this list when the string is sent to the host. For example, if IBM-3279-&M is specified and Model 3 is selected here, the string sent to the host is IBM-3279-3.

Selecting an Extended model allows the host to specify a greater number of colors (seven instead of four) and a wider variety of display attributes. Any Model allows the gateway or mainframe to determine which model ID to use.

Each model is associated with a terminal window display of a specific size (e.g., 24 rows by 80 columns). To specify a different number of rows or columns, select <Custom Model Extended>. When Model ID is set to <Custom Model Extended>, Terminal/Device type changes to IBM-DYNAMIC.

The default value is Model 2 24x80 Extended.
**Rows**
The number of rows to use in the terminal window display. The valid range is 24 - 255.
If the host application specifies a particular screen size, this value may be ignored.

**Columns**
The number of columns to use in the terminal window display. The valid range is 80 - 255.
If the host application specifies a particular screen size, this value may be ignored.

**Graphics Display**

**Enable graphics**
When selected, enables this session to emulate a graphics terminal.
This allows you to run any host application that uses the IBM Graphics Data Display Manager (GDDM) library, such as SAS or ImageView.

**Model ID**
When **Enable graphics** is selected, specifies the type of graphics terminal emulated by this session.

**Related Topics**
- “Configure Advanced Connection Settings Dialog Box” on page 221
- “Set Up Backup Connection Settings Dialog Box” on page 218
- “Configure Terminal Settings Dialog Box” on page 229
- “Configure Terminal Attributes Dialog Box” on page 232

**Set Up Backup Connection Settings Dialog Box**

**Index Term**
Primary: IP
Secondary: rollover for TN3270

**Index Term**
Primary: failover
Secondary: for 3270 connections

**Index Term**
Primary: backup hosts
Secondary: for 3270 connections

**Getting there**
1. Open a 3270 terminal session.
   The steps depend on your user interface mode (page 120).
2 Under **Host Connection**, click **Set Up Backup Connection Settings**.

From this dialog box, you can specify the settings for one or more backup TN3270 connections. If your primary connection fails, these connections will be tried next, in the order they are listed.

**Backup Hosts**

Add a host to the Backup Host list by clicking the **Add** button. Use the **Move Up** and **Move Down** buttons to change the order in which the hosts are tried.

**Enter Host (or System) Name or IP Address**

Identify the host to which you will connect. Type the host name, alias, or numeric IP address.

**NOTE:** Both IPv4 addresses (in the form 127.0.0.1) and IPv6 addresses (in the form 2001:0db8:3c4d:0015:0000:0000:abcd:ef12) are accepted.

**Port**

Type the host port or socket number that the session should use. This field accepts any number between 0 and 66,535 (default = 23).

**Device name**

Specify a particular LU or pool of LUs (up to 32 characters) on the host. If no device name is entered, the server connects to any available LU at the specified port.

**Host Connection Options**

When you enter more than one backup host, the connection options for each host are listed on a separate tab.

**Use Telnet Extended**

If selected, enables TN3270E protocols when supported.
Terminal/Device type

Specify the model of the terminal or device type emulated by this session.

You can select a value from the drop-down box, or type a value that is not listed. This allows you to specify a terminal model that is not implicitly supported but might work, such as Fujitsu.

In most cases you should leave this setting at the default value. If you choose any other value, be sure to use a string that is acceptable to the host; otherwise, you may experience problems connecting to the host, and emulation problems after connecting to the host. Typically, these types of problems occur if the host is not configured to recognize the terminal specified.

Model ID

Specify the model of the terminal or device type emulated by this session.

If the string specified in Terminal/Device type includes &M, the &M is replaced with the model number from this list when the string is sent to the host. For example, if IBM-3279-&M is specified and Model 3 is selected here, the string sent to the host is IBM-3279-3.

Selecting an Extended model allows the host to specify a greater number of colors (seven instead of four) and a wider variety of display attributes. Any Model allows the gateway or mainframe to determine which model ID to use.

Each model is associated with a terminal window display of a specific size (e.g., 24 rows by 80 columns). To specify a different number of rows or columns, select <Custom Model Extended>. When Model ID is set to <Custom Model Extended>, Terminal/Device type changes to IBM-DYNAMIC.

The default value is Model 2 24x80 Extended.

Rows

The number of rows to use in the terminal window display. The valid range is 24 - 255.

If the host application specifies a particular screen size, this value may be ignored.

Columns

The number of columns to use in the terminal window display. The valid range is 80 - 255.

If the host application specifies a particular screen size, this value may be ignored.

Enable graphics

When selected, enables this session to emulate a graphics terminal.

This allows you to run any host application that uses the IBM Graphics Data Display Manager (GDDM) library, such as SAS or ImageView.

Model ID

When Enable graphics is selected, specifies the type of graphics terminal emulated by this session.
Security

Security Settings

Secure data communications with SOCKS or SSL/TLS.

Related Topics

- “Configure Connection Settings Dialog Box” on page 215
- “Configure Advanced Connection Settings Dialog Box” on page 221
- “Configure Terminal Settings Dialog Box” on page 229
- “Configure Terminal Attributes Dialog Box” on page 232

Configure Advanced Connection Settings Dialog Box

Index Term
Primary: timeout
Secondary: keep alive (3270)

Index Term
Primary: telnet location
Secondary: 3270 sessions

Index Term
Primary: telnet
Secondary: advanced TN3270

Index Term
Primary: SYSREQ key

Index Term
Primary: NOP or NOOP, See keep alive

Index Term
Primary: keep alive
Secondary: 3270 sessions

Index Term
Primary: HLLAPI
Secondary: 3270 options

Index Term
Primary: Express Logon Feature (ELF)

Index Term
Primary: ELF

Index Term
Primary: connecting to the host
Secondary: preserving, See keep alive

Index Term
Primary: ATTN key

Getting there

1. Open a 3270 terminal session.
   The steps depend on your user interface mode (page 120).
2 Under **Host Connection**, click **Configure Advanced Connection Settings**.

From this dialog box, you can define advanced TN3270 features.

### Advanced TN3270

#### TN3270 Specific

- **Treat SYSREQ key as** Select the action that should be taken when you press the SYSREQ key. The definition of this key and its values vary by host application.

- **Treat ATTN key as** Select the action that should be taken when you press the ATTN key. The definition of this key and its values vary by host application.

- **Same model for primary and alternate screens** Select to use the same model type for both primary and alternate screen sizes. When selected, you can use a model type other than model 2 for primary screens.

#### TN3270 Enhanced Protocol

- **Enable associated printer** Select this option to associate a 3270 terminal session with a specific 3270 printer session, so that all print jobs from the selected terminal session are sent to the print device associated with the specified printer session.

- **Associated 3270 printer session** Select this option to specify the associated printer session by document name.

  When you use this option, the printer session starts automatically when the terminal session connects to the host.

- **Association string** Select this option to specify the associated printer session using an association string. The string must use only uppercase characters, and is limited to a maximum of 300 characters.

  The association string identifies the selected 3270 terminal session. Once you’ve entered the string here, you can select it from the TN Association list box when configuring the associated 3270 printer session.

  When you use this option, you must start the printer session before you can use it.
Connection Action
You can configure a session to run a macro, start an application, open a Web page, send an e-mail message, or perform a variety of other actions before or after it connects to the host.

Run a macro or other action before the initial connection
Select to run the connection action after the session file is opened but before the session initially connects to a host. (This action is performed even if the session is not configured to connect automatically.)

Select Action
Click to select an action to perform or a macro to run before you connect to the host. By default, the Select Action window opens at the screen for selecting a macro. If you prefer to perform a different action when your session connects, you can select other actions from the task pane.

Run a macro or other action after the initial connection
Select to run the connection action when the session initially connects to a host.

Select Action
Click to select an action to perform or a macro to run when you connect to the host.

Run when reconnecting
Select to run the connection action when the session initially connects to a host, and every time it reconnects to the host.

Security

ELF application ID
Specify the application ID to use the IBM Express Logon Feature (ELF). This feature allows you to connect and logon without entering a user ID and password.

To enable this feature, click Security Settings, then select Use SSL/TLS Security. This feature also requires that you configure the host, install certificates (if necessary) on user computers, and create a connect macro. See "Connect 3270 Sessions using the Express Logon Feature (ELF)" on page 212.

Security Settings
Secure data communications with SOCKS or SSL/TLS.
Miscellaneous

Keep Alive

Send Keep Alive packets
Select to provide a constant check between your session and the host so that you become aware of connection problems as they occur.

Choose one of the three types of keep-alive packets:

<table>
<thead>
<tr>
<th>Choose</th>
<th>To cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>The TCP/IP stack to keep track of the host connection. This method requires less system resources than Send NOP Packets or Send Timing Mark Packets. However, most TCP/IP stacks send Keep Alive packets infrequently.</td>
</tr>
<tr>
<td>SendNOP Packets</td>
<td>InfoConnect to periodically send a No Operation (NOP) command to the host. The host is not required to respond to these commands, but the TCP/IP stack can detect if there was a problem delivering the packet.</td>
</tr>
<tr>
<td>Send Timing Mark Packets</td>
<td>InfoConnect to periodically send a Timing Mark Command to the host to determine if the connection is still active. The host should respond to these commands. If InfoConnect does not receive a response or there is an error sending the packet, it shuts down the connection.</td>
</tr>
</tbody>
</table>

Keep Alive timeout in seconds
Select the interval between the keep-alive requests. The range of values is 1 to 9999 seconds; the default value is 600 seconds.

Telnet Location

Telnet location
(Optional) Type up to 41 characters of descriptive text to provide information about your session. For example, you might include your PC's location, computer name, or IP address.

This features uses the SEND-LOCATION option supported under Telnet connections (RFC779).

InfoConnect does not initiate a WILL SEND command unless you activate the Telnet location option by typing information in this box.
HLLAPI

Options

Short name
Select a HLLAPI short name to associate with this session. This value is used by a HLLAPI application to identify a host session. Any single capital letter (A-Z) can be used as a short name.

By default, InfoConnect assigns the first available letter (A if no other sessions are running) and saves that short name value when you save your session document. If you open multiple sessions that have the same HLLAPI short name value, InfoConnect automatically reassigns the HLLAPI short name of each newly opened session using the next available letter.

If your HLLAPI application requires a specific short name value, specify this value, then save your session document. If you run multiple sessions, you must ensure that sessions running at the same time do not require the same HLLAPI short name.

If you want InfoConnect to generate new, arbitrary short name values for each new session, save all session documents with the HLLAPI short name set to A. InfoConnect will always set the HLLAPI short name to A for the first session, and will reset the short name to the next available letter for each subsequent session.

Long name
Enter a HLLAPI long name to associate with this session. A HLLAPI long name identifies the host session for the convenience of the user. It is not used by the HLLAPI application. The long name can be up to eight characters long and can include letters, numbers, and other characters.

Compatibility
If you are migrating from a legacy EXTRA! or Reflection product, and your application uses the default HLLAPI compatibility settings, simply select Reflection or EXTRA! from the Compatibility drop-down list. This configures the HLLAPI support in InfoConnect to match the default settings found in those applications.

If your application requires custom HLLAPI compatibility settings, select Custom from the Compatibility drop-down list. Once Custom is selected, you can enter a custom compatibility mask.

NOTE: Because of variations in the implementation of HLLAPI in previous products, when HLLAPI applications from EXTRA! and from previous versions of Reflection are run against InfoConnect, they may not behave exactly as they did when run against the product for which they were originally written. Even when you have selected the correct compatibility setting, minor differences may be seen in the status or return code reported by a handful of functions.

Custom compatibility mask
The possible numeric values for the custom compatibility mask styles are "bit masks" that contain separate bits of information about Reflection's HLLAPI configuration. Each style is equated to a decimal and hexadecimal value. A list of the styles and values is shown in the table below.

To create a compatibility mask, add the decimal or hexadecimal values of each style and enter the sum into the Custom Compatibility Mask field. Values can be entered in either decimal or hexadecimal format; however, when using hexadecimal values, replace the Ox at the front of the value with &H. For example, to use hexadecimal value 0x5380, enter &H5380 in the Custom Compatibility Mask field.

For example, to turn on the Propagate EAB (decimal value = 1), Input Inhibited Position (decimal value = 8), and Don't Wrap at PS End (decimal value = 512), add these three numbers (1 + 8 + 512 = 521) and enter the total into the Compatibility Mask field.
<table>
<thead>
<tr>
<th>Style</th>
<th>Decima Value</th>
<th>Hex Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Propagate EAB</td>
<td>1</td>
<td>0x0001</td>
</tr>
<tr>
<td>Query Host Update Protocol</td>
<td>2</td>
<td>0x0002</td>
</tr>
<tr>
<td>Input Inhibited Position</td>
<td>4</td>
<td>0x0004</td>
</tr>
<tr>
<td>Copy PS to String Beyond End</td>
<td>8</td>
<td>0x0008</td>
</tr>
<tr>
<td>Wait a Second</td>
<td>16</td>
<td>0x0010</td>
</tr>
<tr>
<td>Modify Protected Field</td>
<td>32</td>
<td>0x0020</td>
</tr>
<tr>
<td>Translate 5250 Attributes to 3270</td>
<td>64</td>
<td>0x0040</td>
</tr>
</tbody>
</table>

- **Propagate EAB**: When this bit is on, executing a Copy Presentation Space or Copy Presentation Space to String function, with the EAB and NOXLATE session parameters, causes each extended attribute specified at the start of a field to be copied to all characters in the field that do not have the corresponding extended attribute explicitly on. When this bit is off, the attribute is not copied to such characters. This bit applies only to 3270 sessions.

- **Query Host Update Protocol**: When this bit is on, Query Host Update functions report changes to the presentation space only if they are initiated by the host. When this bit is off, functions report changes initiated from the host or from the keyboard.

- **Input Inhibited Position**: This bit determines the position of the "input inhibited" indicator in the string returned from Copy OIA. When it is on, the indicator appears at position 9. When it is off, the indicator appears at position 5.

- **Copy PS to String Beyond End**: This bit determines what happens when the Copy Presentation Space to String function specifies a string that goes beyond the end of the presentation space. When it is on, no error is reported, the data from the position specified to the end of the presentation space is copied, and the remainder of the result string is set to binary zeros. When it is off, Reflection returns an error (APIPARAMETERERROR, value 2).

- **Wait a Second**: When this bit is on, HLLAPI waits one second beyond the last host-initiated presentation space modification before attempting to return a result. When it is off, HLLAPI does not wait. This affects functions Copy OIA, Query Host Update, Copy Presentation Space to String, and Copy Presentation Space.

- **Modify Protected Field**: When this bit is on, the Copy Presentation Space to String function can be used to copy to protected fields. When it is off, such copies are disallowed.

- **Translate 5250 Attributes to 3270**: When this bit is on, attributes copied by the HLLAPI application from the 5250 presentation space are translated to 3270 attributes. When it is off, Reflection returns 5250 attribute values (with the high order 2 bits on).
Always Blank

When this bit is on, data characters found in the presentation space (by Copy Presentation Space to String or Copy Presentation Space) that can not be translated to ASCII are always translated to spaces. When it is off, the ATTRB setting is used to specify what should be done with such characters (if ATTRB is on, they are passed as their original value; if it is off, they are translated to spaces).

Transmit Modified Protected Fields

This bit is relevant when HLLAPI modification of protected fields is allowed (see Modify Protected Field). When it is on, the modified protected field is not sent to the host in response to a read modified command. When it is off, the modified protected field is sent.

Don't Wrap at PS End

This bit determines what happens if, on a copy from a string to the presentation space, the end of the presentation space is reached before the string is completely copied. If this bit is on, the operation terminates and returns an APITRUNCATED error. If it is off, copying continues at the beginning of the presentation space.

Error on Bad Escape

When this bit is on, undefined escape sequences passed to Send Key are reported by returning APIPARAMETERERROR. When it is off, such errors are ignored.

Terminate Send Key at AID

The default behavior for Send Key is to divide strings to be sent into segments terminated by an AID key, and then to send these segments sequentially, reporting an error only if the emulator objects (through input inhibited or busy status). When this bit is on, HLLAPI terminates the send after the first such segment, reporting an error if Error on Send Key Past AID is on. When this bit is off, HLLAPI does not report an error under such circumstances.

Error on Send Key Past AID

When this bit is on, the HLLAPI application reports an error if Send Key continues to send characters after a transmitted AID key. When it's off, the application does not report an error under such circumstances.

Return Zero Length Fields

If this bit is set, Find Field Position (31) returns APIOK and position of next field (in the position parameter) for a zero length field. Otherwise, it returns APIZEROLENFIELD and a 0 in the position parameter.
Caching Off

When set on, this bit disables the caching mechanism that increases performance. If you are having problems with your application synching with the Reflection screen, try turning on this bit. After enabling this bit, you may notice some degradation in HLLAPI performance.

Old Flashpoint

Flashpoint versions 3.1 and earlier expect consecutive CopyPS calls to include or not include attributes regardless of how attributes are set. Turning on this bit makes HLLAPI accept this behavior.

DOS ASCII Converter

This bit converts a HLLAPI character to DOS ASCII format.

EXTRA! OIA Values

When this bit is on, the Copy OIA returns OIA buffer values that match the EXTRAI values instead of the default Reflection values.

Rumba Style

The InfoConnect HLLAPI configuration matches the default settings found in RUMBA.

EXTRA! Style

The InfoConnect HLLAPI configuration matches the default settings found in EXTRA!.

Related Topics

- “Configure Connection Settings Dialog Box” on page 215
- “Set Up Backup Connection Settings Dialog Box” on page 218
- “Configure Terminal Settings Dialog Box” on page 229
- “Configure Terminal Attributes Dialog Box” on page 232

Select Host Code Page Dialog Box (3270)

Index Term

Primary: host code pages
Secondary: for 3270 sessions

Index Term

Primary: host code pages
Secondary: Country Extended Code Page (CECP)

Index Term

Primary: Country Extended Code Page (CECP)

Index Term

Primary: code pages
Secondary: for 3270 sessions
Getting there

1. Open a 3270 terminal session.
   The steps depend on your user interface mode (page 120).

   **User Interface Mode**
   **Steps**
   Ribbon or InfoConnect Browser
   With a session open in InfoConnect, from the Quick Access Toolbar, click 🔄.
   TouchUx
   Tap the Gear icon and then select 🔄 Document Settings.

2. Under **Terminal Configuration**, click **Select Host Code Page**.

**Host Code Page**

- **Language/Code page**
  Select the language and associated host code page to be used by your session. If you are not sure which language and code page to use, check with your system administrator. The default is US English, code page 037.

- **Enable Country Extended Code Page (CECP)**
  Select to make additional characters available in the configured National character set. See your host documentation for details.

**Related Topics**

- “Change the UI Language” on page 123
- “Editing a Host Code Page” on page 233

**Configure Terminal Settings Dialog Box**
Getting there

1. Open a 3270 terminal session.
   The steps depend on your user interface mode (page 120).

   **User Interface Mode**
   **Steps**

   **Ribbon or InfoConnect Browser**
   With a session open in InfoConnect, from the Quick Access Toolbar, click 📚.

   **TouchUx**
   Tap the Gear icon and then select 📚 Document Settings.

2. Under Terminal Configuration, click Configure Terminal Settings.

   From this dialog box, you can set input and other options for your 3270 terminal.

Input

**Keyboard**

**Keyboard type**

Specify which keys can be used in numeric fields.

<table>
<thead>
<tr>
<th>Select</th>
<th>To use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal</td>
<td>Only number keys and certain symbol keys (such as + and =).</td>
</tr>
<tr>
<td>Data Entry</td>
<td>All keys.</td>
</tr>
<tr>
<td>Typewriter</td>
<td>Number keys, shifted number keys (producing symbols such as @ and #), and uppercase letters (A-Z).</td>
</tr>
</tbody>
</table>

**Enable word wrap**

When selected, text is wrapped to the next available field when entered text is too long to fit into the text entry field.
Enable type ahead

When selected, the characters that you type in the terminal window are buffered, allowing you to keep typing after you send data to the host.

The following 3270 functions are processed immediately and are not buffered, even when Enable Type Ahead is selected:
- Alt Cursor
- Cursor Select
- Next Window
- Pan Left
- Pan Right
- Reset
- Scroll up

Keyboard Error
Select the way you want keyboard errors to be handled.

<table>
<thead>
<tr>
<th>No auto reset when a keyboard error occurs</th>
<th>Auto reset when a keyboard error occurs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Before you can resume data entry, you must press Reset to clear the error message.</td>
<td>The next key you press clears the error and attempts to execute the keystroke as follows:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>If</th>
<th>This occurs</th>
</tr>
</thead>
<tbody>
<tr>
<td>The cursor is in a valid input field and the key is a data key</td>
<td>The data is entered there if it is valid data for that field (for example, a numeric character in an input field that only accepts numbers). Otherwise, the cursor is moved to the next valid input field, and if the data is valid for that field, it is entered there.</td>
</tr>
<tr>
<td>The cursor is in a valid input field and the key is a function key</td>
<td>The key operation is executed. Otherwise, the cursor is moved to the next valid input field, and the key is ignored.</td>
</tr>
<tr>
<td>The current screen contains no valid input fields</td>
<td>An error message appears with each keystroke you press, and no keystrokes are executed.</td>
</tr>
</tbody>
</table>

Auto reset without error message

You don't need to press Reset to clear a keyboard error. No error is reported and the next key you press attempts to execute the keystroke as follows:

<table>
<thead>
<tr>
<th>If the cursor</th>
<th>This occurs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is in a valid input field</td>
<td>The key is ignored. This is true for both data keys and function keys.</td>
</tr>
</tbody>
</table>
Configure Terminal Attributes Dialog Box

Support double-byte character set
Select to use Asian languages such as Japanese, Chinese, and Korean in your terminal session.

Rectangular Selection (Mouse)
Dragging the mouse across an area selects only the text within that area. When this option is cleared (unchecked), the selection wraps to line ends.

Related Topics
- “Configure Connection Settings Dialog Box” on page 215
- “Configure Advanced Connection Settings Dialog Box” on page 221
- “Set Up Backup Connection Settings Dialog Box” on page 218
- “Configure Terminal Attributes Dialog Box” on page 232

Getting there
1. Open a 3270 terminal session.
   The steps depend on your user interface mode (page 120).

   **User Interface Mode**
   - **Ribbon or InfoConnect Browser**
   - **TouchUx**

   **Steps**
   - With a session open in InfoConnect, from the Quick Access Toolbar, click .
   - Tap the Gear icon and then select Document Settings.

2. Under **Terminal Configuration**, click **Configure Terminal Attributes**.
Terminal Attributes

Enable host beep  When selected, beeps sent by the host are sounded.

Disable text blinking  When selected, text set to blink by the host does not blink.

Blink rate  Specifies the speed at which text set to blink by the host blinks.

Input field underlining  Specifies whether to underline fields that allow input. You can set options to never underline, allow the host to control underlining, or always underline.

Related Topics

- “Configure Terminal Settings Dialog Box” on page 229
- “Configure Connection Settings Dialog Box” on page 215
- “Set Up Backup Connection Settings Dialog Box” on page 218
- “Configure Advanced Connection Settings Dialog Box” on page 221

Editing a Host Code Page

Index Term
Primary: EBCDIC
Secondary: translate to ANSI

Index Term
Primary: ANSI
Secondary: translate to EBCDIC

Index Term
Primary: host code pages
Secondary: editing

Index Term
Primary: code pages
Secondary: editing

Using the InfoConnect Translation Table editors, you can edit the host code pages InfoConnect uses to translate ANSI to EBCDIC, and EBCDIC to ANSI. This makes it possible to use currently unsupported character sets, and to customize InfoConnect for unique host system environments.

NOTE

- Only users with administrator privileges can use this feature.
- This feature is not available with VT sessions.
- Host code page data is saved in the file R8ncs.dll, located in the InfoConnect installation folder (page 889). It is recommended that you make a backup copy of this file before making changes.

The translation table editors are located in the InfoConnect folder.
Separate tables are provided for display, file transfer, printer, and other uses. When you change an EBCDIC to ANSI translation table, you should make the corresponding change to the ANSI to EBCDIC translation table, so that the data interaction between InfoConnect and the host is consistent for both PC-to-host and host-to-PC transactions.

The character search window in the bottom right corner of the **Character Translation Table** tab provides a way to search for any character in a table. To search for a character, enter the character in the search window and press Enter. The table editor moves you to the location in the table that contains the character.

## IBM 5250 Sessions

**Index Term**  
**Primary:** sessions  
**Secondary:** IBM 5250

**Index Term**  
**Primary:** host connection  
**Secondary:** IBM 5250

**Index Term**  
**Primary:** connecting to the host  
**Secondary:** IBM 5250

This section includes detailed information on configuring your IBM 5250 terminal sessions.

**In this Section**

- “Input Modes and Special Characters” on page 235
- “Enter Diacritical Characters” on page 238
- “Status Lines” on page 238
- “Configure a Device Name” on page 243
- “5250 Terminal Document Settings Dialog Box” on page 244
- “Configure Connection Settings Dialog Box” on page 247
- “Set Up Backup Connection Settings Dialog Box” on page 249
- “Configure Advanced Connection Settings Dialog Box” on page 251
- “Select Host Code Page Dialog Box (5250)” on page 258
- “Configure Terminal Settings Dialog Box” on page 258

<table>
<thead>
<tr>
<th>To edit this type of host code page</th>
<th>Use this editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard 3270</td>
<td>Edit3270.exe</td>
</tr>
<tr>
<td>Standard 5250</td>
<td>Edit5250.exe</td>
</tr>
<tr>
<td>Double-byte 3270</td>
<td>ed3270db.exe</td>
</tr>
<tr>
<td>Double-byte 5250</td>
<td>ed5250db.exe</td>
</tr>
</tbody>
</table>
Input Modes and Special Characters

Special input modes available on a 5250 terminal include extended graphics mode, hex mode, insert mode, Plus CR mode, and text assist (word-processing) mode. Diacritical characters can be entered when the terminal is in extended graphics mode.

Extended Graphics Mode

The following special characters are available in extended graphics mode:

Blue indicates the character that is inserted if you press SHIFT with this key; purple indicates the character that is inserted if you press this key without SHIFT.

The default mapping for extended graphics mode is ALT+LEFT SHIFT. When the session is in extended graphics mode, a + appears near the center of the 3488 status line.

If the Preserve Entry Mode check box in the Configure Terminal Settings dialog box is selected, ALT+LEFT SHIFT functions as a toggle to take the session into and out of extended graphics mode. Reset (LEFT CTRL) also takes the session out of extended graphics mode.

If the Preserve Entry Mode check box is cleared, the session automatically exits extended graphics mode after you enter a graphics character or a diacritical character.

Hex Mode

On a 5250 terminal, hex mode is entered by pressing a terminal key. The default mapping for hex mode is ALT+F7. When the session is in hex mode, the letter h or H appears on the 3488 status line.
Enter hex mode before entering a hexadecimal value for a character. To enter a hexadecimal value, type two characters. These characters can be 0-9 or a-f. No other input is allowed in hex mode.

When you enter the first character of your hex value, the h in the status line becomes a capital H. If **Preserve Entry Mode** is selected in the Configure Terminal Settings dialog box, pressing LEFT CTRL takes the character out of the buffer but doesn’t exit hex mode. (You can use this method to retract the character you typed. To show this, the capital H becomes a small h once again.) Press LEFT CTRL again to back completely out of hex mode.

If **Preserve Entry Mode** is not selected, a single Reset (LEFT CTRL) takes you out of hex mode.

**Insert Mode**

The default mapping for insert mode is INSERT.

When the session is in insert mode, the insert symbol (\(\wedge\)) appears in the 3488 status line. In the 5250 status line, the letters IM are displayed in inverse video.

Characters you type when the terminal is in insert mode are inserted at the cursor position. As you type, existing characters at and to the right of the cursor position shift one position to the right for each character you type. There must be a null character at the right end of the insert field for each character you type in insert mode. If you attempt to insert more characters than there are nulls, \(\wedge\) appears in the status line and input is inhibited. Press Reset (LEFT CTRL) to remove the symbol and enable input.

**Plus CR Mode**

In this mode, a two-character hexadecimal value is displayed in front of each field in the terminal window. The meaning of the hexadecimal value is indicated by the code that appears in the status line.

<table>
<thead>
<tr>
<th>Code</th>
<th>Hex Value Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>d</td>
<td>The field and display attributes for each field.</td>
</tr>
<tr>
<td>c</td>
<td>The extended character buffer values for each field.</td>
</tr>
<tr>
<td>a</td>
<td>The character attributes for each character in the terminal window.</td>
</tr>
</tbody>
</table>

The default mapping for Plus CR is ALT+F12. Each time you press ALT+F12, the code and hex values change to the next one in sequence. Press Reset (Left CTRL) twice to exit Plus CR mode.

**Text Assist (Word-Processing) Mode**

When using Text Assist mode, you can select the level of assistance (Basic or Intermediate) that you want displayed on your screen by pressing PF21 in any of these three screens in OfficeVision:

- Send Note
- Work with Mail
- Work with Documents in Folders

The following word processing functions can be used in Text Assist mode on the AS/400. If you use one of these functions when the session is not in word-processing mode results, the message "0027 = Key not supported by this emulation" is sent to your screen. (See your host documentation for more information on word-processing mode.)
<table>
<thead>
<tr>
<th>Function</th>
<th>Keystroke</th>
<th>Description/Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Begin bold</td>
<td>CTRL+B</td>
<td></td>
</tr>
<tr>
<td>Begin underline</td>
<td>CTRL+U</td>
<td></td>
</tr>
<tr>
<td>Beginning of line</td>
<td>CTRL+LEFT ARROW</td>
<td></td>
</tr>
<tr>
<td>Bottom of page</td>
<td>CTRL+DOWN ARROW</td>
<td></td>
</tr>
<tr>
<td>Carriage return</td>
<td>RIGHT CTRL</td>
<td>CTRL+PLUS SIGN (+) and CTRL+MINUS SIGN (-) can also be used to enter a carriage return</td>
</tr>
<tr>
<td>Center text</td>
<td>CTRL+C</td>
<td>By default, CTRL+C copies text to the clipboard. To use it to center text in Text Assist mode, you must remap the key combination.</td>
</tr>
<tr>
<td>Delete at the cursor</td>
<td>CTRL+DELETE</td>
<td>If you are currently viewing an attribute plane, deletes the current value at the cursor position. If you are in the data plane, deletes all values in all planes at the cursor position.</td>
</tr>
<tr>
<td>position</td>
<td></td>
<td></td>
</tr>
<tr>
<td>End attribute</td>
<td>CTRL+J</td>
<td></td>
</tr>
<tr>
<td>End of line</td>
<td>CTRL+RIGHT ARROW</td>
<td></td>
</tr>
<tr>
<td>Find next stop code</td>
<td>CTRL+N</td>
<td>By default, CTRL+N opens a new window. To use it to find the next stop code in Text Assist mode, you must remap the key combination.</td>
</tr>
<tr>
<td>Half index down</td>
<td>CTRL+H</td>
<td></td>
</tr>
<tr>
<td>Half index up</td>
<td>CTRL+Y</td>
<td></td>
</tr>
<tr>
<td>Insert symbols</td>
<td>CTRL+A</td>
<td>By default, CTRL+A is ”Select All.” To use it in Text Assist mode, you must remap the key combination.</td>
</tr>
<tr>
<td>Page end</td>
<td>CTRL+P</td>
<td></td>
</tr>
<tr>
<td>Required carriage return</td>
<td>RIGHT CTRL</td>
<td></td>
</tr>
<tr>
<td>Required space</td>
<td>CTRL+SPACEBAR</td>
<td></td>
</tr>
<tr>
<td>Required tab</td>
<td>CTRL+TAB</td>
<td>To use this key combination in Text Assist mode, you must remap the key combination.</td>
</tr>
<tr>
<td>Stop</td>
<td>CTRL+S</td>
<td>To use this key combination in Text Assist mode, you must remap the key combination.</td>
</tr>
<tr>
<td>Tab</td>
<td>TAB</td>
<td></td>
</tr>
<tr>
<td>Text tab advance</td>
<td>CTRL+T</td>
<td>Moves the cursor from the current position to the next defined tab stop. If there are no tab stops in the current field, tab advance moves the cursor to the first tab stop in the next field on the screen.</td>
</tr>
<tr>
<td>Top of page</td>
<td>CTRL+UP ARROW</td>
<td></td>
</tr>
<tr>
<td>Word underline</td>
<td>CTRL+W</td>
<td></td>
</tr>
</tbody>
</table>
Enter Diacritical Characters

Diacritical characters are characters printed with special symbols above or below them.

To enter a diacritical character in a 5250 session

1. Put Reflection in extended graphics mode.
   The default keystroke for entering extended graphics mode is ALT+LEFT SHIFT.
2. Press a key to indicate the diacritical mark you want to insert:

<table>
<thead>
<tr>
<th>Key</th>
<th>Mark</th>
</tr>
</thead>
<tbody>
<tr>
<td>g</td>
<td>#193 Grave accent ( ` )</td>
</tr>
<tr>
<td>;</td>
<td>#194 Acute accent ( ’ )</td>
</tr>
<tr>
<td>t</td>
<td>#196 Tilde ( ~ )</td>
</tr>
<tr>
<td>f</td>
<td>#195 Circumflex ( ^ )</td>
</tr>
<tr>
<td>“</td>
<td>#200 Diaerisis ( ¨ )</td>
</tr>
<tr>
<td>’</td>
<td>#203 Cedilla ( , )</td>
</tr>
<tr>
<td>d</td>
<td>#202 Ring ( ° )</td>
</tr>
</tbody>
</table>

3. Press the letter key for the letter to combine with the diacritical mark. If you press SPACEBAR, the diacritical mark is inserted by itself. Only certain character choices can be combined with the diacritical character.

<table>
<thead>
<tr>
<th>Mark</th>
<th>Characters</th>
</tr>
</thead>
<tbody>
<tr>
<td>#193 Grave accent ( ` )</td>
<td>a, e, i, o, u, or SPACEBAR</td>
</tr>
<tr>
<td>#194 Acute accent ( ’ )</td>
<td>a, e, i, o, u, or SPACEBAR</td>
</tr>
<tr>
<td>#196 Tilde ( ~ )</td>
<td>a, n, o, or SPACEBAR</td>
</tr>
<tr>
<td>#195 Circumflex ( ^ )</td>
<td>a, e, i, o, u, or SPACEBAR</td>
</tr>
<tr>
<td>#200 Diaerisis ( ¨ )</td>
<td>a, e, i, o, u, lowercase y, or SPACEBAR</td>
</tr>
<tr>
<td>#203 Cedilla ( , )</td>
<td>c or SPACEBAR</td>
</tr>
<tr>
<td>#202 Ring ( ° )</td>
<td>a</td>
</tr>
</tbody>
</table>

Status Lines

In this Section

- “3488 Status Line” on page 239
The 3488 status line looks like this:

```
■ n [R X ] ▶ nnn nnn d nnnn + ☞ 混在 Ha A ‾ A ＜S ＜C nn/nn
```

These codes and symbols in the 3488 status line are as follows:

<table>
<thead>
<tr>
<th>Code</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>■</td>
<td>System available. The session is connected to the host.</td>
</tr>
<tr>
<td>n</td>
<td>The 5250 session number (as low as 1, or as high as 16). As you connect 5250 terminal sessions, each new session is assigned the lowest available number. A session retains its number for as long as it is connected.</td>
</tr>
<tr>
<td>☞</td>
<td>Message waiting. If this icon appears, the host has one or more messages for this session.</td>
</tr>
<tr>
<td>R</td>
<td>Keyboard reserved. When this symbol is present, a HLLAPI application is reserving the keyboard. The keyboard is locked until the HLLAPI application releases it.</td>
</tr>
<tr>
<td>X</td>
<td>Input inhibited. The system cannot process keyboard input. This symbol can appear because the system is processing input or because it has detected an error. If an error has occurred you may need to press the Help key (SCROLL LOCK) and the Reset key (LEFT CTRL) before you can start working with the host again.</td>
</tr>
<tr>
<td>▶</td>
<td>Typeahead. An underline beneath this symbol indicates that data is in the buffer. The session can buffer up to 256 characters when the keyboard is locked (for example, while the host program is processing).</td>
</tr>
<tr>
<td>nnn</td>
<td>Keyboard errors. Specifies the number of keyboard errors that have occurred since the host connection was established. This information only appears when InfoConnect is displaying field attributes.</td>
</tr>
<tr>
<td>nnn</td>
<td>Link errors. Specifies the number of link parity errors that have occurred since the host connection was established. This information appears when InfoConnect is displaying field attributes.</td>
</tr>
<tr>
<td>d, c, or a</td>
<td>Plus CR mode.</td>
</tr>
<tr>
<td>nnnn</td>
<td>Error code. This four-digit code defines the terminal error that has occurred.</td>
</tr>
<tr>
<td>+</td>
<td>Extended graphics mode.</td>
</tr>
<tr>
<td>混在</td>
<td>Both single- and double-byte characters are accepted in the current field.</td>
</tr>
</tbody>
</table>
The 5250 status line looks like this:

```
混在 <S <C nnn 06/53 SA MW KS IM II KR <name> <device>
```

The codes in the 5250 status line are as follows:

<table>
<thead>
<tr>
<th>Code</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>全角</td>
<td>Only double-byte characters are accepted in the current field.</td>
</tr>
<tr>
<td>英数</td>
<td>Only single-byte characters are accepted in the current field.</td>
</tr>
<tr>
<td>△</td>
<td>Diacritic mode. Indicates that 1) the session has been placed in extended graphics mode, and 2) one of the characters that puts InfoConnect in diacritic mode has been entered.</td>
</tr>
<tr>
<td>H or h</td>
<td>Hexadecimal mode.</td>
</tr>
<tr>
<td>a</td>
<td>Indicates that the ALT key has been pressed.</td>
</tr>
<tr>
<td>A</td>
<td>Indicates that Caps Lock is on.</td>
</tr>
<tr>
<td>^</td>
<td>Indicates that InfoConnect is in Insert mode.</td>
</tr>
<tr>
<td>&lt;S</td>
<td>Screen direction indicator (Arabic only). When this symbol appears, the host screen is displayed in right to left, top to bottom orientation.</td>
</tr>
<tr>
<td>&lt;C</td>
<td>Cursor direction indicator (Arabic only). When this symbol displays, typing direction switches to right to left.</td>
</tr>
<tr>
<td>nn/nn</td>
<td>Cursor position. Specifies the location of the cursor in the terminal window in row/column format.</td>
</tr>
</tbody>
</table>

Related Topics
- “Configure Terminal Settings Dialog Box” on page 258
- “Status Lines” on page 238

**5250 Status Line**

Index Term
Primary: symbols
Secondary: 5250 status line

Index Term
Primary: status line (5250)

Index Term
Primary: status line
Secondary: codes, 5250
The debug status line looks like this:

```
52 01 01.00.00.20.0099.5000 00 20.00.04.02 c0.c0.00.21 14/07 05f6 20/7
```

Most fields on the debug status line contain two-character hexadecimal numbers.

Related fields are separated by periods. For example, the string 01.00.00.20.0099.5000 near the beginning of the example status line shows six fields that contain information relating to host field attributes. Unrelated fields are separated by spaces.
If InfoConnect is in Plus CR mode and an error occurs, characters in positions 9-31 on the debug status line are replaced by magenta characters that provide information about the error condition. These characters are important to Attachmate Technical Support.

<table>
<thead>
<tr>
<th>Code</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>Input inhibit. If the &quot;X&quot; is present, the system cannot process keyboard input.</td>
</tr>
<tr>
<td>&lt;char&gt;</td>
<td>If this character is displayed The session is in this mode</td>
</tr>
<tr>
<td>d, c, or a</td>
<td>Plus CR</td>
</tr>
<tr>
<td>D</td>
<td>Data processing</td>
</tr>
<tr>
<td>W</td>
<td>Word processing (text assist)</td>
</tr>
<tr>
<td>U</td>
<td>Undefined</td>
</tr>
<tr>
<td>hex number</td>
<td>Pending read command. Identifies the datastream read command sent by the host.</td>
</tr>
<tr>
<td>hex number</td>
<td>Field count. The total number of fields on the current screen.</td>
</tr>
<tr>
<td>hex number</td>
<td>Field number. The number of the field under the cursor (if consecutive fields in a continued entry field are counted as multiple fields).</td>
</tr>
<tr>
<td>hex number</td>
<td>Base field memory. The number of the field under the cursor (if consecutive fields in a continued entry field are counted as a single field).</td>
</tr>
<tr>
<td>hex number</td>
<td>Field modification. The number of times the field under the cursor has been modified.</td>
</tr>
<tr>
<td>hex number</td>
<td>Field display attribute. The host-defined display attribute for the field under the cursor.</td>
</tr>
<tr>
<td>hex number</td>
<td>Field length. The number of characters in the field under the cursor.</td>
</tr>
<tr>
<td>hex number</td>
<td>Field format word. The field attribute for the field under the cursor.</td>
</tr>
<tr>
<td>&lt;character&gt;</td>
<td>The character sent by the host, enclosed in quotes.</td>
</tr>
<tr>
<td>hex number</td>
<td>Host data. The EBCDIC value for the character under the cursor.</td>
</tr>
<tr>
<td>hex number</td>
<td>Display data. The ANSI value of the character under the cursor.</td>
</tr>
<tr>
<td>hex number</td>
<td>Display format. The line type and font value for the character under the cursor.</td>
</tr>
<tr>
<td>hex number</td>
<td>Display attribute. The display attribute for the character as shown.</td>
</tr>
<tr>
<td>hex number</td>
<td>Display color. The color attribute for the character as shown.</td>
</tr>
<tr>
<td>hex number</td>
<td>ECB attribute. The extended character buffer attribute for the character under the cursor.</td>
</tr>
<tr>
<td>hex number</td>
<td>ECB color. The color specified by the extended character buffer for the character under the cursor.</td>
</tr>
<tr>
<td>hex number</td>
<td>ECB video. The video graphic value specified by the extended character buffer for the character under the cursor (not currently used).</td>
</tr>
<tr>
<td>hex number</td>
<td>Input field memory. Indicates the order in which fields were created. The first field created is field 00.</td>
</tr>
<tr>
<td>hex number</td>
<td>Field type memory. The first part of this value indicates the position of the character under the cursor within the field; the second part indicates whether the character under the cursor is detectable as a hotspot.</td>
</tr>
<tr>
<td>hex number</td>
<td>Cursor row. The row under the cursor.</td>
</tr>
</tbody>
</table>
### Configure a Device Name

In 5250 terminal sessions, the device name (also called the display name or workstation ID) is visible in the sign-on screen when you connect to your host.

You can configure the session to generate unique customized device names. Special characters can be included in the device name value to specify how the device name is displayed and incremented.

If you choose not to configure the device name, the AS/400 automatically assigns a device name for the session in the format QPADEV<####>.

### To configure the device name

1. Open a 5250 terminal session.
2. **Open the Document Settings dialog box.**
   - **User Interface Mode**
     - **Ribbon or Reflection Browser**
       - With a session open in Reflection, from the Quick Access Toolbar, click.
     - **TouchUX**
       - Tap the Gear icon and then select Document Settings.
3. Under **Host Connection**, click **Configure Connection Settings**.
4. Verify that the **Generate a device name** check box is selected.
5. In the **Device name** field, enter a device name, then click OK and save your session.

### Related Topics

- “Configure Terminal Settings Dialog Box” on page 258
- “Status Lines” on page 238

<table>
<thead>
<tr>
<th>Code</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>hex number</td>
<td>Cursor column. The column under the cursor.</td>
</tr>
<tr>
<td>hex number</td>
<td>Cursor index. Indicates the cursor location in a single hex value. Numbering starts at the left end of the first row, moves right to the end of the first row, continues at the left of the second row, and so on.</td>
</tr>
<tr>
<td>decimal number</td>
<td>Cursor row/column. The row, column location of the cursor, represented in decimal.</td>
</tr>
</tbody>
</table>
This character | Specifies
---|---
* | An alphabetic counter used to create a unique device name. It is replaced by A, B, C and so on. If the entire alphabet is used, the generated device names continue with AA, AB, AC, and so on.
% | The session type. It is replaced by P for printer sessions; S for display sessions.
= | A numeric counter used to create a unique device name. It is replaced by 1, 2, 3, and so on.
&COMPN | The local workstation name, left-trimmed, if the generated name exceeds 10 characters.
&USERN | The local user name, left-trimmed, if the generated name exceeds 10 characters.
+ | The use of right-trim instead of left-trim with &COMPN or &USERN. This character can be placed anywhere within the string.

NOTE

- You can use only one string in combination with these characters. If you use separated strings, the second string is dropped. For example, %MyDevice= is valid. However, %My=Device is not valid, and will be treated by the system as if it were &My=.
- You cannot use both &COMPN and &USERN in the same string.
- If you leave this box blank, the AS/400 creates a device to use for your session.

Examples:

- Setting Device name to %ABC= generates the device name SABC1 for a display session. If this is rejected, Reflection will try SABC2, SABC3, and so on.
- Setting Device name to %123* generates the device name S123A for the first display session, S123B for the second session, and so on.
- Setting Device name to &COMPN* generates puternameA, puternameB, puternameC for the first three sessions when the computer name is Computername.
- Setting Device name to %My=Device generates SMy. Because only one string literal can be used at a time, the second string literal (=Device) is ignored.
- Setting Device name to +&USERN* generates karlschmiA, karlschmiB, karlschmiC for the first three sessions when the computer user name is karlschmidt.

5250 Terminal Document Settings Dialog Box

Index Term
Primary: device
Secondary: generate name

Getting there

1. Open the Create New Document dialog box
   The steps depend on your user interface mode (page 120).
From the Create New Document dialog box, select a 5250 terminal session template, and then click "Create."

**Connection**

**Enter Host (or System) Name or IP Address**
Identify the host to which you will connect. Type the host name, alias, or numeric IP address.

**NOTE:** Both IPv4 addresses (in the form 127.0.0.1) and IPv6 addresses (in the form 2001:0db8:3c4d:0015:0000:0000:abcd:ef12) are accepted.

**Port**
Type the host port or socket number that the session should use. This field accepts any number between 0 and 66,535 (default = 23).

**NOTE:** For SSL sessions, the port defaults to 992.

**Device name**
Specify the terminal device name (also called the display name or the workstation ID) that the AS/400 should use for your session. If you leave this box blank, the AS/400 creates a device to use for your session.

The device name can be up to ten characters long. You can include any of the following characters as part of the value in the "Device name" box.

<table>
<thead>
<tr>
<th>Character</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Replaced by A, B, C, and so on to create a unique device name. If the entire alphabet is used, the generated device names continue with AA, AB, AC, and so on.</td>
</tr>
<tr>
<td>%</td>
<td>Replaced by P for printer sessions and S for display sessions.</td>
</tr>
<tr>
<td>=</td>
<td>Replaced by 1, 2, 3, and so on to create a unique device name.</td>
</tr>
<tr>
<td>&amp;COMPN</td>
<td>Replaced by the local workstation name, left-trimmed, if the generated name exceeds 10 characters.</td>
</tr>
<tr>
<td>&amp;USERN</td>
<td>Replaced by the local user name, left-trimmed, if the generated name exceeds 10 characters.</td>
</tr>
<tr>
<td>+</td>
<td>Specifies right-trimming instead of left-trimming. Use with &amp;COMPN or &amp;USERN. This character can be placed anywhere in the string.</td>
</tr>
</tbody>
</table>
NOTE

- You can use only one string in combination with these characters. If you use separated strings, the second string is dropped. For example, %MyDevice= is valid. However, %My=Device is not valid, and will be treated by the system as if it were &My=.
- You cannot use both &COMPN and &USERN in the same string.
- To have InfoConnect generate unique device names automatically based on the special characters described above, the **Generate Device Names** setting must be enabled. In printer sessions, this setting is off by default. To enable it, see the “Generate Device Names” on page 588 topic.

**Generate device names**

When selected, InfoConnect automatically generates device names based on the value specified in the **Device name** field.

For example, if the specified device name is %ABC=, InfoConnect generates the device name SABC1 for a display session. If SABC1 is already in use, InfoConnect tries SABC2, SABC3, and so on.

Setting the device name to %123* generates the device name S123A for the first display session, S123B for the second session, and so on.

When cleared, if the specified device name is in use, the session does not connect.

**Terminal**

**Model ID**

Specify the terminal (also known as a display station) you want to emulate.

**Host code page**

Select the language and associated host code page to be used by your session. If you are not sure which language and code page to use, check with your system administrator. The default is US English, code page 037.

**Keyboard map**

Specify the keyboard map to use with this session.

**Configure additional settings**

Select to open a page from which you can customize host connection, terminal configuration, and other settings for this session.

When selected, the session does not auto-connect. This allows you to modify settings before connecting to the session.

**Related Topics**

- “Create a Session Document File” on page 147
- “Configure Connection Settings Dialog Box” on page 247
- “Generate Device Names” on page 588
- “Editing a Host Code Page” on page 233
Configure Connection Settings Dialog Box

Index Term
Primary: telnet
Secondary: TN5250

Index Term
Primary: name collisions

Index Term
Primary: device
Secondary: name collisions

Index Term
Primary: device
Secondary: device in use failures

Index Term
Primary: allow device in use failures

Getting there

1 Open a 5250 terminal session.
   The steps depend on your user interface mode (page 120).

   User Interface Mode          Steps
   Ribbon or InfoConnect Browser With a session open in InfoConnect, from the Quick Access Toolbar, click .
   TouchUx                      Tap the Gear icon and then select Document Settings.

2 Under Host Connection, click Configure Connection Settings.

From this dialog box, you can specify the settings for a TN5250 connection.

Connection

Enter Host (or System) Name or IP Address
Identify the host to which you will connect. Type the host name, alias, or numeric IP address.

NOTE: Both IPv4 addresses (in the form 127.0.0.1) and IPv6 addresses (in the form 2001:0db8:3c4d:0015:0000:0000:abcd:ef12) are accepted.

Port
Type the host port or socket number that the session should use. This field accepts any number between 0 and 66,535 (default = 23).

Device name
Specify the terminal device name (also called the display name or the workstation ID) that the AS/400 should use for your session. If you leave this box blank, the AS/400 creates a device to use for your session.

The device name can be up to ten characters long. You can include any of the following characters as part of the value in the Device name box.

<table>
<thead>
<tr>
<th>Character</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
* Replaced by A, B, C, and so on to create a unique device name. If the entire alphabet is used, the generated device names continue with AA, AB, AC, and so on.

% Replaced by P for printer sessions and S for display sessions.

= Replaced by 1, 2, 3, and so on to create a unique device name.

&COMPN Replaced by the local workstation name, left-trimmed, if the generated name exceeds 10 characters.

&USERN Replaced by the local user name, left-trimmed, if the generated name exceeds 10 characters.

+ Specifies right-trimming instead of left-trimming. Use with &COMPN or &USERN. This character can be placed anywhere in the string.

NOTE

- You can use only one string in combination with these characters. If you use separated strings, the second string is dropped. For example, %MyDevice= is valid. However, %My=Device is not valid, and will be treated by the system as if it were &My=.

- You cannot use both &COMPN and &USERN in the same string.

- To have InfoConnect generate unique device names automatically based on the special characters described above, the Generate Device Names setting must be enabled. In printer sessions, this setting is off by default. To enable it, see the “Generate Device Names” on page 588 topic.

Options

**Automatically connect to the host**
Select to establish a host connection as soon as the associated session document is opened.

**When connection is terminated**
Specify options for reconnecting after any disconnection that is not initiated from InfoConnect.

<table>
<thead>
<tr>
<th>Choose</th>
<th>To have InfoConnect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reconnect automatically</td>
<td>Attempt to reestablish the connection.</td>
</tr>
<tr>
<td>Prompt for reconnection</td>
<td>Prompt whether to attempt to reestablish the connection. (When No is selected, the session is left open and disconnected.)</td>
</tr>
<tr>
<td>Leave disconnected</td>
<td>Leave the session disconnected with the session open.</td>
</tr>
<tr>
<td>Close session automatically</td>
<td>Close the session.</td>
</tr>
</tbody>
</table>

**Model**

**Model ID**
Specify the model of the terminal or device type emulated by this session.
Related Topics

- “Configure Advanced Connection Settings Dialog Box” on page 251
- “Set Up Backup Connection Settings Dialog Box” on page 249
- “Configure Terminal Settings Dialog Box” on page 258

Set Up Backup Connection Settings Dialog Box

Index Term
Primary: IP
Secondary: rollover for TN5250

Index Term
Primary: failover
Secondary: for 5250 connections

Index Term
Primary: backup hosts
Secondary: for 5250 connections

Getting there

1. Open a 5250 terminal session.
   The steps depend on your user interface mode (page 120).

   **User Interface Mode**
   **Steps**
   Ribbon or InfoConnect Browser
   With a session open in InfoConnect, from the Quick Access Toolbar, click .
   TouchUx
   Tap the Gear icon and then select Document Settings.

2. Under Host Connection, click Set up Backup Connection Settings.

   From this dialog box, you can specify the settings for one or more backup TN5250 connections. If your primary connection fails, these connections will be tried next, in the order they are listed.

Backup Hosts

Add a host to the Backup Host list by clicking the Add button. Use the Move Up and Move Down buttons to change the order in which the hosts are tried.

**Enter Host (or System) Name or IP Address**
Identify the host to which you will connect. Type the host name, alias, or numeric IP address.

**NOTE:** Both IPv4 addresses (in the form 127.0.0.1) and IPv6 addresses (in the form 2001:0db8:3c4d:0015:0000:0000:abcd:ef12) are accepted.

**Port**
Type the host port or socket number that the session should use. This field accepts any number between 0 and 66,535 (default = 23).
Device name

Specify the terminal device name (also called the display name or the workstation ID) that the AS/400 should use for your session. If you leave this box blank, the AS/400 creates a device to use for your session.

The device name can be up to ten characters long. You can include any of the following characters as part of the value in the Device name box.

<table>
<thead>
<tr>
<th>Character</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Replaced by A, B, C, and so on to create a unique device name. If the entire alphabet is used, the generated device names continue with AA, AB, AC, and so on.</td>
</tr>
<tr>
<td>%</td>
<td>Replaced by P for printer sessions and S for display sessions.</td>
</tr>
<tr>
<td>=</td>
<td>Replaced by 1, 2, 3, and so on to create a unique device name.</td>
</tr>
<tr>
<td>&amp;COMPN</td>
<td>Replaced by the local workstation name, left-trimmed, if the generated name exceeds 10 characters.</td>
</tr>
<tr>
<td>&amp;USERN</td>
<td>Replaced by the local user name, left-trimmed, if the generated name exceeds 10 characters.</td>
</tr>
<tr>
<td>+</td>
<td>Specifies right-trimming instead of left-trimming. Use with &amp;COMPN or &amp;USERN. This character can be placed anywhere in the string.</td>
</tr>
</tbody>
</table>

NOTE

- You can use only one string in combination with these characters. If you use separated strings, the second string is dropped. For example, %MyDevice= is valid. However, %My=Device is not valid, and will be treated by the system as if it were &My=.
- You cannot use both &COMPN and &USERN in the same string.
- To have InfoConnect generate unique device names automatically based on the special characters described above, the Generate Device Names setting must be enabled. In printer sessions, this setting is off by default. To enable it, see the “Generate Device Names” on page 588 topic.

Host Connection Settings

When you enter more than one backup host, the connection options for each host are listed on a separate tab.
Options

Generate device names
When selected, InfoConnect automatically generates device names based on the value specified in the Device name field.

For example, if the specified device name is %ABC=, InfoConnect generates the device name SABC1 for a display session. If SABC1 is already in use, InfoConnect tries SABC2, SABC3, and so on.

Setting the device name to %123* generates the device name S123A for the first display session, S123B for the second session, and so on.

When cleared, if the specified device name is in use, the session does not connect.

Model

Model ID
Specify the terminal (also known as a display station) you want to emulate.

Security

Security Settings
Secure data communications with SOCKS or SSL/TLS.

Related Topics

- “Configure Connection Settings Dialog Box” on page 247
- “Configure Advanced Connection Settings Dialog Box” on page 251
- “Configure Terminal Settings Dialog Box” on page 258
- “Generate Device Names” on page 588

Configure Advanced Connection Settings Dialog Box

Index Term
Primary: timeout
Secondary: keep alive (5250)

Index Term
Primary: telnet location
Secondary: 5250 sessions (adv)

Index Term
Primary: telnet
Secondary: advanced TN5250

Index Term
Primary: sign-on options

Index Term
Primary: keep alive
Secondary: 5250 sessions (adv)

Index Term
Primary: IBM Enterprise Identity Mapping (EIM)
Getting there

1. Open a 5250 terminal session. The steps depend on your user interface mode (page 120).

   **User Interface Mode**
   - Ribbon or InfoConnect Browser
   - TouchUx

   **Steps**
   - With a session open in InfoConnect, from the Quick Access Toolbar, click **Document Settings**.

2. Under **Host Connection**, click **Configure Advanced Connection Settings**.

   From this dialog box, you can define advanced TN5250 features.

**Advanced 5250 Sign-on Options**

- **Do Not Sign On Automatically**
  Select if you do not want to log on to the host as soon as you establish a connection. This is the default.

- **Automatically Sign On Using Windows Credentials**
  Select to log on to the host using your Windows username and password. This option works in conjunction with IBM Enterprise Identity Mapping (EIM), which must be configured on your host computer.

- **Automatically Sign On Using Specified User ID and Password**
  Select to log on to the host using the specified user ID and password.
Connection Action
You can configure a session to run a macro, start an application, open a Web page, send an e-mail message, or perform a variety of other actions before or after it connects to the host.

Run a macro or other action before the initial connection
Select to run the connection action after the session file is opened but before the session initially connects to a host. (This action is performed even if the session is not configured to connect automatically.)

Select Action
Click to select an action to perform or a macro to run before you connect to the host. By default, the Select Action window opens at the screen for selecting a macro. If you prefer to perform a different action when your session connects, you can select other actions from the task pane.

Run a macro or other action after the initial connection
Select to run the connection action when the session initially connects to a host.

Select Action
Click to select an action to perform or a macro to run when you connect to the host.

Run when reconnecting
Select to run the connection action when the session initially connects to a host, and every time it reconnects to the host.

Security

Security Settings
Secure data communications with SOCKS or SSL/TLS.

Miscellaneous

Keep Alive

Send Keep Alive packets
Select to provide a constant check between your session and the host so that you become aware of connection problems as they occur.

Choose To cause
System The TCP/IP stack to keep track of the host connection. This method requires less system resources than Send NOP Packets or Send Timing Mark Packets. However, most TCP/IP stacks send Keep Alive packets infrequently.

Send NOP Packets InfoConnect to periodically send a No Operation (NOP) command to the host. The host is not required to respond to these commands, but the TCP/IP stack can detect if there was a problem delivering the packet.

Send Timing Mark Packets InfoConnect to periodically send a Timing Mark Command to the host to determine if the connection is still active. The host should respond to these commands. If InfoConnect does not receive a response or there is an error sending the packet, it shuts down the connection.

Keep Alive timeout in seconds
Select the interval between the keep-alive requests. The range of values is 1 to 9999 seconds; the default value is 600 seconds.
Telnet Location

Telnet location
(Optional) Type up to 41 characters of descriptive text to provide information about your session. For example, you might include your PC's location, computer name, or IP address.

This feature uses the SEND-LOCATION option supported under Telnet connections (RFC779).

InfoConnect does not initiate a WILL SEND command unless you activate the Telnet location option by typing information in this box.

HLLAPI
Options

Short name
Select a HLLAPI short name to associate with this session. This value is used by a HLLAPI application to identify a host session. Any single capital letter (A-Z) can be used as a short name.

By default, InfoConnect assigns the first available letter (A if no other sessions are running) and saves that short name value when you save your session document. If you open multiple sessions that have the same HLLAPI short name value, InfoConnect automatically reassigned the HLLAPI short name of each newly opened session using the next available letter.

If your HLLAPI application requires a specific short name value, specify this value, then save your session document. If you run multiple sessions, you must ensure that sessions running at the same time do not require the same HLLAPI short name.

If you want InfoConnect to generate new, arbitrary short name values for each new session, save all session documents with the HLLAPI short name set to A. InfoConnect will always set the HLLAPI short name to A for the first session, and will reset the short name to the next available letter for each subsequent session.

Long name
Enter a HLLAPI long name to associate with this session. A HLLAPI long name identifies the host session for the convenience of the user. It is not used by the HLLAPI application. The long name can be up to eight characters long and can include letters, numbers, and other characters.

Compatibility
If you are migrating from a legacy EXTRA! or Reflection product, and your application uses the default HLLAPI compatibility settings, simply select Reflection or EXTRA! from the Compatibility drop-down list. This configures the HLLAPI support in InfoConnect to match the default settings found in those applications.

If your application requires custom HLLAPI compatibility settings, select Custom from the Compatibility drop-down list. Once Custom is selected, you can enter a custom compatibility mask.

NOTE: Because of variations in the implementation of HLLAPI in previous products, when HLLAPI applications from EXTRA! and from previous versions of Reflection are run against InfoConnect, they may not behave exactly as they did when run against the product for which they were originally written. Even when you have selected the correct compatibility setting, minor differences may be seen in the status or return code reported by a handful of functions.
The possible numeric values for the custom compatibility mask styles are "bit masks" that contain separate bits of information about Reflection's HLLAPI configuration. Each style is equated to a decimal and hexadecimal value. A list of the styles and values is shown in the table below.

To create a compatibility mask, add the decimal or hexadecimal values of each style and enter the sum into the Custom Compatibility Mask field. Values can be entered in either decimal or hexadecimal format; however, when using hexadecimal values, replace the 0x at the front of the value with &H. For example, to use hexadecimal value 0x5380, enter &H5380 in the Custom Compatibility Mask field.

For example, to turn on the Propagate EAB (decimal value = 1), Input Inhibited Position (decimal value = 8), and Don't Wrap at PS End (decimal value = 512), add these three numbers (1 + 8 + 512 = 521) and enter the total into the Compatibility Mask field.

<table>
<thead>
<tr>
<th>Style</th>
<th>Decimal Value</th>
<th>Hex Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Propagate EAB</td>
<td>1</td>
<td>0x0001</td>
</tr>
<tr>
<td>Query Host Update Protocol</td>
<td>2</td>
<td>0x0002</td>
</tr>
<tr>
<td>Input Inhibited Position</td>
<td>4</td>
<td>0x0004</td>
</tr>
<tr>
<td>Copy PS to String Beyond End</td>
<td>8</td>
<td>0x0008</td>
</tr>
</tbody>
</table>

When this bit is on, executing a Copy Presentation Space or Copy Presentation Space to String function, with the EAB and NOXLATE session parameters, causes each extended attribute specified at the start of a field to be copied to all characters in the field that do not have the corresponding extended attribute explicitly on. When this bit is off, the attribute is not copied to such characters. This bit applies only to 3270 sessions.

When this bit is on, Query Host Update functions report changes to the presentation space only if they are initiated by the host. When this bit is off, functions report changes initiated from the host or from the keyboard.

This bit determines the position of the "input inhibited" indicator in the string returned from Copy OIA. When it is on, the indicator appears at position 9. When it is off, the indicator appears at position 5.

This bit determines what happens when the Copy Presentation Space to String function specifies a string that goes beyond the end of the presentation space. When it is on, no error is reported, the data from the position specified to the end of the presentation space is copied, and the remainder of the result string is set to binary zeros. When it is off, Reflection returns an error (APIPARAMETERERROR, value 2).
Wait a Second

When this bit is on, HLLAPI waits one second beyond the last host-initiated presentation space modification before attempting to return a result. When it is off, HLLAPI does not wait. This affects functions Copy OIA, Query Host Update, Copy Presentation Space to String, and Copy Presentation Space.

Modify Protected Field

When this bit is on, the Copy Presentation Space to String function can be used to copy to protected fields. When it is off, such copies are disallowed.

Translate 5250 Attributes to 3270

When this bit is on, attributes copied by the HLLAPI application from the 5250 presentation space are translated to 3270 attributes. When it is off, Reflection returns 5250 attribute values (with the high order 2 bits on).

Always Blank

When this bit is on, data characters found in the presentation space (by Copy Presentation Space to String or Copy Presentation Space) that can not be translated to ASCII are always translated to spaces. When it is off, the ATTRB setting is used to specify what should be done with such characters (if ATTRB is on, they are passed as their original value; if it is off, they are translated to spaces).

Transmit Modified Protected Fields

This bit is relevant when HLLAPI modification of protected fields is allowed (see Modify Protected Field). When it is on, the modified protected field is not sent to the host in response to a read modified command. When it is off, the modified protected field is sent.

Don't Wrap at PS End

This bit determines what happens if, on a copy from a string to the presentation space, the end of the presentation space is reached before the string is completely copied. If this bit is on, the operation terminates and returns an APITRUNCATED error. If it is off, copying continues at the beginning of the presentation space.

Error on Bad Escape

When this bit is on, undefined escape sequences passed to Send Key are reported by returning APIPARAMETERERROR. When it is off, such errors are ignored.
**Terminate Send Key at AID**

The default behavior for Send Key is to divide strings to be sent into segments terminated by an AID key, and then to send these segments sequentially, reporting an error only if the emulator objects (through input inhibited or busy status). When this bit is on, HLLAPI terminates the send after the first such segment, reporting an error if Error on Send Key Past AID is on. When this bit is off, HLLAPI does not report an error under such circumstances.

**Error on Send Key Past AID**

When this bit is on, the HLLAPI application reports an error if Send Key continues to send characters after a transmitted AID key. When it's off, the application does not report an error under such circumstances.

**Return Zero Length Fields**

If this bit is set, Find Field Position (31) returns APIOK and position of next field (in the position parameter) for a zero length field. Otherwise, it returns APIZEROLENFIELD and a 0 in the position parameter.

**Caching Off**

When set on, this bit disables the caching mechanism that increases performance. If you are having problems with your application synching with the Reflection screen, try turning on this bit. After enabling this bit, you may notice some degradation in HLLAPI performance.

**Old Flashpoint**

Flashpoint versions 3.1 and earlier expect consecutive CopyPS calls to include or not include attributes regardless of how attributes are set. Turning on this bit makes HLLAPI accept this behavior.

**DOS ASCII Converter**

This bit converts a HLLAPI character to DOS ASCII format.

**EXTRA! OIA Values**

When this bit is on, the Copy OIA returns OIA buffer values that match the EXTRA! values instead of the default Reflection values.

**Rumba Style**

The InfoConnect HLLAPI configuration matches the default settings found in RUMBA.
Related Topics

- “Configure Connection Settings Dialog Box” on page 247
- “Set Up Backup Connection Settings Dialog Box” on page 249
- “Configure Terminal Settings Dialog Box” on page 258

Select Host Code Page Dialog Box (5250)

**Index Term**
Primary: host code pages
Secondary: for 5250 sessions

**Index Term**
Primary: code pages
Secondary: for 5250 sessions

**Getting there**

1. Open a 5250 terminal session.
   The steps depend on your user interface mode (page 120).

   **User Interface Mode**
   - Ribbon or InfoConnect Browser
   - TouchUX
   
   **Steps**
   - With a session open in InfoConnect, from the Quick Access Toolbar, click 
   - Tap the Gear icon and then select Document Settings.

2. Under **Terminal Configuration**, click **Select Host Code Page**.

**Host Code Page**

**Language/Code page**
Select the language and associated host code page to be used by your session. If you are not sure which language and code page to use, check with your system administrator. The default is US English, code page 037.

**Related Topics**

- “Change the UI Language” on page 123
- “Editing a Host Code Page” on page 233

**Configure Terminal Settings Dialog Box**

**Index Term**
Primary: word wrap
Secondary: 5250
Index Term
Primary: type ahead
Secondary: 5250

Index Term
Primary: status line
Secondary: selecting for 5250 session

Index Term
Primary: preserve entry mode
Secondary: setting

Index Term
Primary: keyboard
Secondary: 5250 keyboard error handling

Index Term
Primary: Japanese language, See double-byte characters

Index Term
Primary: double-byte support (5250)

Index Term
Primary: double-byte characters (DBCS)
Secondary: support (5250 sessions)

Index Term
Primary: blink rate
Secondary: 5250 text

Index Term
Primary: beep
Secondary: keyboard error (5250)

Index Term
Primary: beep
Secondary: host (5250)

Index Term
Primary: DBCS
Secondary: support (5250 sessions)

Getting there

1  Open a 5250 terminal session.
   The steps depend on your user interface mode (page 120).

   **User Interface Mode**          **Steps**
   Ribbon or InfoConnect Browser    With a session open in InfoConnect, from the Quick Access Toolbar, click .

   TouchUx                        Tap the Gear icon and then select Document Settings.

2  Under Terminal Configuration, click Configure Terminal Settings.

   From this dialog box, you can set input and other options for your 5250 terminal.
Display

Use dots to separate columns
Select to use periods as column separators. This is the default unless you are running a Japanese operating system.

Use vertical lines to separate columns
Select to use vertical lines as column separators. This is the default if you are running a Japanese version of the product.

Disable text blinking
When selected, text set to blink by the host does not blink.

Blink rate
Specifies the speed at which text set to blink by the host blinks.

Status line
Select the type of status line to display at the bottom of the terminal window when your session is connected.

This option | Uses
---|---
3488 Status Line | Symbols to represent various conditions and is based on the status line you see on newer 5250 terminals from IBM.
5250 Status Line | Character pairs to represent various conditions. The characters are always shown but appear in inverse video when the condition is true. For example, when the system is not available, the letters SA appear in regular video. However, when the system is available, the letters appear in inverse video.
Debug Status Line | The 5250 datastream for troubleshooting. If you contact Attachmate Technical Support, you may be asked to use the Debug Status Line to help diagnose the problem. This option is for users with an intimate knowledge of the 5250 datastream.

Input field underlining
Specifies whether to underline fields that allow input. You can set options to never underline, allow the host to control underlining, or always underline.

Input

Word Wrap
Select the way you want word wrap to be handled. If word wrap is enabled, text is wrapped from one entry field to the next on a word boundary if possible; if word wrap is disabled, text continues from one entry field to the next without regard to word boundaries.

Host controls word wrap
The host is allowed to enable or disable word wrap on a per-field basis.

Enable word wrap
Word wrap is enabled for all entry fields regardless of host settings.

Disable word wrap
Word wrap is disabled for all entry fields regardless of host settings.

Type Ahead
Select the way you want type-ahead to be handled. If type-ahead is enabled, typed characters are buffered while the host is not ready for data; if type-ahead is disabled, typed characters are ignored until the host is ready for data.
Host controls type-ahead

The host is allowed to enable or disable type-ahead.

Enable type-ahead

Type-ahead is enabled regardless of host settings.

Disable type-ahead

Type-ahead is disabled regardless of host settings.

Keyboard Error

Select the way you want keyboard errors to be handled.

No auto reset when a keyboard error occurs

Before you can resume data entry, you must press Reset to clear the error message.

Auto reset when a keyboard error occurs

The next key you press clears the error and attempts to execute the keystroke as follows:

If

The cursor is in a valid input field and the key is a data key

This occurs

The data is entered there if it is valid data for that field (for example, a numeric character in an input field that only accepts numbers).

Otherwise, the cursor is moved to the next valid input field, and if the data is valid for that field, it is entered there.

The cursor is in a valid input field and the key is a function key

The key operation is executed. Otherwise, the cursor is moved to the next valid input field, and the key is ignored.

The current screen contains no valid input fields

An error message appears with each keystroke you press, and no keystrokes are executed.

Auto reset without error message

You don't need to press Reset to clear a keyboard error. No error is reported and the next key you press attempts to execute the keystroke as follows:

If the cursor

Is in a valid input field

This occurs

The key is ignored. This is true for both data keys and function keys.

Is not in a valid input field and the key is a data key

The cursor is moved to the next valid input field, and if the data is valid for that field, it is entered there.

Is not in a valid input field and the key is a function key

The cursor is moved to the next valid input field, and the key is ignored.
Use this value with caution, because it prevents notification of keyboard errors.

**Beep when keyboard error is detected**

You'll hear a beep when you encounter a keyboard error.

**NOTE:** If you select **Auto reset without error message**, it's recommended that you also select this option, so that you'll know when a keyboard error occurs.

### Miscellaneous

**Preserve entry mode**

When selected, the session remains in extended graphics mode or hexadecimal mode indefinitely after you enter either mode. Use the same keystroke to exit these modes as you use to enter them.

When this option is not selected, the session automatically exits extended graphics mode after you enter a graphic or diacritical character, and automatically exits hexadecimal mode after you enter a hexadecimal pair.

**Enable host beep**

When selected, beeps sent by the host are sounded.

**Enable AID field exit mode**

When selected, unrestricted sending of AID key values (F1-F24 only) to the host from restricted input fields is allowed.

**Support double-byte character set**

Select to use Asian languages such as Japanese, Chinese, and Korean in your terminal session.

**Rectangular Selection (Mouse)**

Dragging the mouse across an area selects only the text within that area. When this option is cleared (unchecked), the selection wraps to line ends.

### Related Topics
- “Configure Connection Settings Dialog Box” on page 247
- “Configure Advanced Connection Settings Dialog Box” on page 251
- “Set Up Backup Connection Settings Dialog Box” on page 249
- “3488 Status Line” on page 239
- “5250 Status Line” on page 240
- “Debug Status Line” on page 241

### VT Sessions

**Index Term**
- **Primary:** VT
- **Secondary:** emulation

**Index Term**
- **Primary:** UNIX
- **Secondary:** sessions, see also VT

**Index Term**
- **Primary:** OpenVMS
- **Secondary:** sessions, see also VT

**Index Term**
- **Primary:** HP
- **Secondary:** sessions, see also VT
This section includes detailed information on configuring your VT sessions.

In this Section

- “VT Document Settings Dialog Box” on page 263
- “ReGIS Graphics Support” on page 264
- “Configure Connection Settings Dialog Box (VT)” on page 265
- “Select Terminal Type Dialog Box” on page 281
- “Set Up Display Settings Dialog Box” on page 304
- “Set Up Safeguards Dialog Box” on page 306
- “Connect to Host Dialog Box” on page 307

Related Topics

- “Printing from VT Sessions” on page 559
- “VT File Transfer” on page 688

VT Document Settings Dialog Box

Getting there

1 Open the Create New Document dialog box.
   The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ribbon or InfoConnect Browser</td>
<td>From the Quick Access Toolbar, click the New Document button.</td>
</tr>
<tr>
<td>TouchUx</td>
<td>Tap the Folder icon and then under File, select New.</td>
</tr>
</tbody>
</table>

2 From the Create New Document dialog box, select a VT terminal session, and then click Create.

Connection

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telnet</td>
<td>Select to use your PC as a virtual terminal over a TCP/IP connection.</td>
</tr>
<tr>
<td>Secure Shell</td>
<td>Select for secure, encrypted communications between a trusted host and your PC over an insecure network. When you select Secure Shell, all connections between your PC and the remote host(s) are encrypted, protecting the data sent between these machines.</td>
</tr>
<tr>
<td>Rlogin</td>
<td>Select to use your PC as a virtual terminal over a TCP/IP connection.</td>
</tr>
<tr>
<td>Enter Host (or System) Name or IP Address</td>
<td>Identify the host to which you will connect. Type the host name, alias, or numeric IP address.</td>
</tr>
</tbody>
</table>

**NOTE:** Both IPv4 addresses (in the form 127.0.0.1) and IPv6 addresses (in the form 2001:0db8:3c4d:0015:0000:0000:abcd:ef12) are accepted.
Port

Type the host port or socket number that the session should use. This field accepts any number between 0 and 66,535 (default = 23).

User Name

Type a name that identifies you or your PC to the host.

This option is enabled only for Secure Shell or Rlogin connections.

SSH configuration

Type a descriptive name to label these connection settings, making them available for use with other sessions.

If you leave this field blank, and make changes to any secure shell configuration, InfoConnect saves the configuration scheme using the value from the Host name/IP address field. (See “SSH Configuration Schemes” on page 403.)

Terminal

Terminal Type

Select the terminal to emulate. This specifies the codes generated by the numeric keypad, the interpretation of control functions, and the response to terminal identification requests. (Values under Terminal automatically reset when you choose a terminal type.)

Support graphics

Select to support the Tektronix 401x terminal type or the Remote Graphics Instruction Set (ReGIS) by DEC. REGIS includes the following features:

- Up to 16 colors
- Shading with selected patterns and polygon fill
- Rubberband cursors
- Rotated and italicized characters
- Mouse support
- A scaled graphic showing the complete ReGIS screen (800x480 pixels) on the physical display

Keyboard map

Specify the keyboard map to use with this session.

Configure additional settings

Select to open a page from which you can customize host connection, terminal configuration, and other settings for this session.

When selected, the session does not auto-connect. This allows you to modify settings before connecting to the session.

Related Topics

- “Create a Session Document File” on page 147
- “ReGIS Graphics Support” on page 264
- “Configure Connection Settings Dialog Box (VT)” on page 265

ReGIS Graphics Support

Index Term

Primary: sixel graphics emulation
Secondary: overview
For accurate ReGIS and sixel graphics emulation using InfoConnect, on the Graphics tab from the Terminal Setup dialog box, the Terminal type should be set to one of the four graphics terminal types: VT240, VT241, VT330, or VT340.

**NOTE**

- The VT240 and VT330 are monochrome graphics terminals, providing up to four shades of gray at once.
- The VT241 and VT340 are color graphics terminals; the VT241 provides up to four different colors at once, while the VT340 provides up to 16 different colors.
- Setting your display to 256 colors is highly recommended.

All four graphics terminals support ReGIS. However, each terminal differs slightly in its implementation of ReGIS. InfoConnect should be set for the same type of terminal as that of the host graphics program.

A host program may need to determine the graphics capabilities of InfoConnect. It does so by requesting the Terminal ID (which is set on the Emulation tab from the Terminal Setup dialog box). For accurate graphics emulation, the Terminal ID should be set to the type of terminal the host expects to find: VT240, VT241, VT330, or VT340 (the default is VT320).

**NOTE:** Changing the Terminal type resets all associated settings (that is, any setting from the Terminal Setup dialog box or the Advanced Options dialog box).

**Related Topics**

- “Graphics Tab (Terminal Setup Dialog Box)” on page 299
- “Select Terminal Type Dialog Box” on page 281

**Configure Connection Settings Dialog Box (VT)**
Index Term
Primary: Rlogin
Secondary: VT connection settings

Index Term
Primary: modem
Secondary: VT connection settings

Index Term
Primary: dialing properties, modem (VT)

Index Term
Primary: Secure Shell
Secondary: SSH configuration scheme (VT)

Getting there
1. Open a VT terminal session.
   The steps depend on your user interface mode (page 120).

   **User Interface Mode**  
   **Steps**  
   Ribbon or InfoConnect Browser  
   With a session open in InfoConnect, from the Quick Access Toolbar, click .

   TouchUx  
   Tap the Gear icon and then select Document Settings.

2. Under **Host Connection**, click **Configure Connection Settings**.
   From this dialog box, you can specify the settings for a VT connection.

**Connection Method**

<table>
<thead>
<tr>
<th>Network</th>
<th>Configure a host connection through a network.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serial Port</td>
<td>Configure a host connection through a serial port on your PC.</td>
</tr>
<tr>
<td>Modem</td>
<td>Configure a host connection through a modem. The modem must first be configured in Windows.</td>
</tr>
</tbody>
</table>

**Network**

These options are available only when you have selected **Network** under **Connection Method**.

**Network Connection Type**

| Telnet               | Select to use your PC as a virtual terminal over a TCP/IP connection.  
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>When Telnet is the selected protocol, you can configure secure connections using Kerberos or SSL/TLS.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Secure Shell</th>
<th>Select for secure, encrypted communications between a trusted host and your PC over an insecure network. When you select Secure Shell, all connections between your PC and the remote host(s) are encrypted, protecting the data sent between these machines.</th>
</tr>
</thead>
</table>

| Rlogin               | Select to use your PC as a virtual terminal over a TCP/IP connection. |
## Connection Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Host name/IP address</strong></td>
<td>Identify the host to which you will connect. Type the host name, alias, or</td>
</tr>
<tr>
<td></td>
<td>numeric IP address.</td>
</tr>
<tr>
<td><strong>NOTE:</strong> Both IPv4 addresses</td>
<td>Both IPv4 addresses (in the form 127.0.0.1) and IPv6 addresses (in the</td>
</tr>
<tr>
<td>(in the form 127.0.0.1) and</td>
<td>form 2001:0db8:3c4d:0015:0000:0000:abcd:ef12) are accepted.</td>
</tr>
<tr>
<td><strong>User name</strong></td>
<td>Type a name that identifies you or your PC to the host.</td>
</tr>
<tr>
<td></td>
<td>This option is enabled only for Secure Shell or Rlogin connections.</td>
</tr>
<tr>
<td><strong>SSH configuration scheme</strong></td>
<td>Type a descriptive name to label these connection settings, making them</td>
</tr>
<tr>
<td></td>
<td>available for use with other Secure Shell sessions.</td>
</tr>
<tr>
<td></td>
<td>If you leave this field blank, and make changes to any connection settings,</td>
</tr>
<tr>
<td></td>
<td>InfoConnect saves the configuration scheme using the value from the Host</td>
</tr>
<tr>
<td></td>
<td>name/IP address field.</td>
</tr>
<tr>
<td><strong>Handle SSH User authentication</strong></td>
<td>For Secure Shell connections, display username and password prompts in the</td>
</tr>
<tr>
<td>in terminal window</td>
<td>terminal window instead of in a dialog box.</td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td>Secure data communications with Kerberos, Secure Shell, SOCKS, or SSL/TLS.</td>
</tr>
</tbody>
</table>

## Serial Port

These options are available only when you have selected **Serial Port** under **Connection Method**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Serial port to use</strong></td>
<td>InfoConnect detects available serial ports on your PC and displays them</td>
</tr>
<tr>
<td></td>
<td>here.</td>
</tr>
<tr>
<td><strong>Parity</strong></td>
<td>Set the parity for data transmission to and from the serial device on this</td>
</tr>
<tr>
<td></td>
<td>port.</td>
</tr>
<tr>
<td></td>
<td>This setting determines whether a parity bit is generated for each</td>
</tr>
<tr>
<td></td>
<td>character transmitted. Parity is used to detect errors in data</td>
</tr>
<tr>
<td></td>
<td>transmission; the number preceding the slash indicates the number of</td>
</tr>
<tr>
<td></td>
<td>data bits sent.</td>
</tr>
<tr>
<td></td>
<td>To use the multinational character set or 8-bit controls, Parity must be</td>
</tr>
<tr>
<td></td>
<td>set to one of the values that offers 8-bit controls. If your</td>
</tr>
<tr>
<td></td>
<td>communications link generates parity, and you set Parity to 8/None,</td>
</tr>
<tr>
<td></td>
<td>multinational characters appear on your screen. In this case, set Parity</td>
</tr>
<tr>
<td></td>
<td>to either 8/Even or 8/Odd.</td>
</tr>
<tr>
<td><strong>Baud</strong></td>
<td>Set the rate at which InfoConnect transmits and receives data through the</td>
</tr>
<tr>
<td></td>
<td>selected serial port.</td>
</tr>
<tr>
<td></td>
<td>The baud rate setting must match the baud rate of your direct connection.</td>
</tr>
</tbody>
</table>

## More Settings

Configure additional settings.
Modem

These options are available only when you have selected **Modem** under **Connection Method**.

**Modem to use**

InfoConnect detects modems configured on your PC and displays them here.

**Phone number**

Type the phone number you want the modem to dial when connecting. The number must adhere to the rules of your modem.

**Use country code and city code**

Select this option if you want to specify a country code and city code (or area code) for the number you are dialing.

Clear this option if you do not want to use the **Country code**, **City code**, and **Current location** options.

**Country code**

Type the country code for the country you are calling.

**City code**

Type the city code or area code for the location you are calling.

**Current location**

Select the previously defined location from which you are calling. These locations are defined from the **Dialing Properties** dialog box.

**Dialing Properties**

Add, modify, or remove a location from the **Current location** list.

**More Settings**

Configure additional settings.

**Connection Action**

You can configure a session to run a macro, start an application, open a Web page, send an e-mail message, or perform a variety of other actions before or after it connects to the host.

**Run a macro or other action before the initial connection**

Select to run the connection action after the session file is opened but before the session initially connects to a host. (This action is performed even if the session is not configured to connect automatically.)

**Select Action**

Click to select an action to perform or a macro to run before you connect to the host. By default, the **Select Action** window opens at the screen for selecting a macro. If you prefer to perform a different action when your session connects, you can select other actions from the task pane.

**Run a macro or other action after the initial connection**

Select to run the connection action when the session initially connects to a host.

**Select Action**

Click to select an action to perform or a macro to run when you connect to the host.

**Run when reconnecting**

Select to run the connection action when the session initially connects to a host, and every time it reconnects to the host.
Connection Options

- **Automatically connect to the host**
  Select to establish a host connection as soon as the associated session document is opened.

- **Allow exit while connected**
  Select to allow closing the workspace when a session is connected to a host.

- **When connection is terminated**
  Specify options for reconnecting after any disconnection that is not initiated from InfoConnect.
  
  **Choose**
  - **Reconnect automatically**
  - **Prompt for reconnection**
  - **Leave disconnected**
  - **Close session automatically**

  **To have InfoConnect**
  - Attempt to reestablish the connection.
  - Prompt whether to attempt to reestablish the connection. (When No is selected, the session is left open and disconnected.)
  - Leave the session disconnected with the session open.
  - Close the session.

Related Topics

- “General Tab (More Settings Telnet Dialog Box)” on page 269
- “Advanced Tab (More Settings Telnet Dialog Box)” on page 277
- “Options Tab (More Settings Telnet Dialog Box)” on page 271
- “More Settings Secure Shell Dialog Box” on page 273
- “More Settings RLogin Dialog Box” on page 274
- “More Settings Serial Port Dialog Box” on page 276

General Tab (More Settings Telnet Dialog Box)

Index Term

Primary: telnet
Secondary: VT connection settings, more

Getting there

1. **Open a VT terminal session:**
   The steps depend on your user interface mode (page 120).

   **User Interface Mode**
   - **Ribbon or Reflection Browser**
     With a session open in Reflection, from the Quick Access Toolbar, click .
   - **TouchUx**
     Tap the Gear icon and then select Document Settings.

2. **Under Host Connection, click Configure Connection Settings.**

3. **Under Connection Method, select Network.**
4 Under **Network Connection Type**, select **Telnet**.

5 Under **Connection Options**, click the **More Settings** button.

The options are:

**TCP port**
Most Telnet hosts wait for an incoming connection on TCP Port 23. If your host uses a different port, type that number here.

**Parity**
This setting determines whether a parity bit is generated for each character transmitted. Parity is used to detect errors in data transmission; the number preceding the slash indicates the number of data bits sent.

To use the multinational character set or 8-bit controls, **Parity** must be set to one of the values that offers 8-bit controls. If your communications link generates parity, and you set **Parity** to **8/None**, multinational characters appear on your screen. In this case, set **Parity** to either **8/Even** or **8/Odd**.

This option is not available if you are connecting to a network modem over Telnet.

**Terminal type**
To override the default terminal, select or type a value here.

In general, you control the following characteristics when you change terminal types:

- Which screen control sequences the host sends to **InfoConnect** to format the screen.
- The position of the cursor.
- Which characters to display in a host application.

If you're having trouble running a host application, the negotiation between **InfoConnect** and the host might be wrong. If you enter a terminal type that the host does not recognize, **InfoConnect** reverts to a list of default values until one is found that the host supports.

This option is not available if you are connecting to a network modem over Telnet.

**Timeout**
Specify the number of milliseconds **InfoConnect** should attempt to make a connection before timing out. The maximum value is 65535. The timeout period begins after host name resolution has taken place. This means an additional delay, usually a few seconds beyond the value specified.

When this is set to 0 (the default), **InfoConnect** timeout behavior is determined by your Windows operating system.

**Use emulation terminal ID**
Select to force **InfoConnect** to ignore the **Terminal type** setting and instead use the value from the **Terminal ID** setting on the **Emulation** tab from the **Terminal Setup** dialog box.

**Use threaded I/O**
Select to send communication calls to an independent thread that handles IO (Input/Output) processing, thus improving performance.

**Related Topics**
- “Configure Connection Settings Dialog Box (VT)” on page 265
Options Tab (More Settings Telnet Dialog Box)

Index Term
Primary: telnet
Secondary: VT connection options

Index Term
Primary: local echo (VT)
Secondary: telnet option

Index Term
Primary: echo, local (VT)
Secondary: telnet option

Getting there

1. Open a VT terminal session.
   The steps depend on your user interface mode (page 120).

   **User Interface Mode**  **Steps**
   - Ribbon or Reflection Browser  With a session open in Reflection, from the Quick Access Toolbar, click .
   - TouchUX  Tap the Gear icon and then select Document Settings.

2. Under Host Connection, click Configure Connection Settings.
4. Under Network Connection Type, select Telnet.
5. Under Connection Options, click the More Settings button.

The options are:

**Initiate option negotiation**  Specifies whether certain connection options, including whether to always request a binary mode connection, should be negotiated when the Telnet connection is established. When cleared, connections to some hosts on the Internet are expedited so that InfoConnect does not attempt to initiate negotiations for Telnet options.

**Trace negotiation**  Select to cause Telnet to write the negotiation process for the various Telnet options to the screen. This is useful for debugging.
Request binary (Option 0)

Telnet defines a 7-bit data path between the host and the terminal (or, in this case, InfoConnect). This type of data path is not compatible with certain national character sets and some file transfer protocols (for example, Xmodem and Zmodem). Fortunately, many hosts allow for 8-bit data without zeroing the 8th bit, which resolves this problem. However, in some cases, it may be necessary to force the host to use an 8-bit data path by selecting this option.

**NOTE:** This option is not available when Initiate option negotiation is cleared.

Local echo (Option 1)

Select the way you want InfoConnect to respond to remote echo from a Telnet host:

- **Specify**
  - **Automatic (default)**: Attempt to negotiate remote echo, but do as the host commands.
  - **Yes**: Negotiate local echo with the host, but always echo.
  - **No**: Negotiate remote echo with the host, but not echo.

Ctrl-Break character

Select what happens when you press Ctrl+Break. By default, InfoConnect sends the Interrupt process sequence to the host. If your host expects a Telnet break sequence, then select this option instead.

Set host window size (Option 31)

Select to send the number of rows and columns to the Telnet host whenever they change, so that the host can properly control the cursor if the window size is changed.

Dynamic terminal size (Option 31)

Select to support dynamic update of the number of rows and columns in the display when the user resizes the terminal window. Your Telnet server and application must also support NAWS (Negotiate About Window Size), otherwise display problems can occur.

Note: You can quickly determine the screen size of the terminal window whenever you hover the mouse cursor over the Row and Column indicator (located in the left corner of the status bar). Under Telnet and Secure Shell connection types, the tooltip will also feature "Auto" if Dynamic terminal size is selected.

Linemode (Option 34)

Line mode allows InfoConnect to store characters in a buffer until a carriage return is entered, at which point, the characters are sent to the host in one packet (instead of sending each single character as an individual packet).

Line mode is useful when long network delays are an issue, and allows you to reduce costs on networks that charge on a per packet basis.

- **Select**
  - **RFC Compliant**: Your host supports it, and it gets negotiated during connect.
  - **During Local Echo**: The host tells InfoConnect to do the echoing.
  - **When Not in SGA**: The host does not Suppress Go Ahead.

All options other than RFC Compliant are known as "faux" line mode.

Suppress local echo (Option 45)

Select to suppress the local echoing of characters to the display.
Renegotiate echo  Some hosts require a period of time to initialize a connection before accepting a request by the client to recognize and perform a Local Echo. Select this option to let InfoConnect attempt a second negotiation of the Local Echo option following the initialization period.

Related Topics
- “Configure Connection Settings Dialog Box (VT)” on page 265

More Settings Secure Shell Dialog Box

Index Term
Primary: Secure Shell
Secondary: VT connection settings, more

Getting there

1 Open a VT terminal session.
   The steps depend on your user interface mode (page 120).

   User Interface Mode  Steps
   Ribbon or InfoConnect Browser  With a session open in InfoConnect, from the Quick Access Toolbar, click .
   TouchUx  Tap the Gear icon and then select Document Settings.

2 Under Host Connection, click Configure Connection Settings.
3 Under Connection Method, select Network.
4 Under Network Connection Type, select Secure Shell.
5 Under Connection Options, click the More Settings button.

The options are:

Parity  This setting determines whether a parity bit is generated for each character transmitted. Parity is used to detect errors in data transmission; the number preceding the slash indicates the number of data bits sent.

To use the multinational character set or 8-bit controls, Parity must be set to one of the values that offers 8-bit controls. If your communications link generates parity, and you set Parity to 8/None, multinational characters appear on your screen. In this case, set Parity to either 8/Even or 8/Odd.

Baud  Select the rate at which InfoConnect transmits and receives data through the network connection.
### Terminal type

To override the default terminal, select or type a value here.

In general, you control the following characteristics when you change terminal types:

- Which screen control sequences the host sends to InfoConnect to format the screen.
- The position of the cursor.
- Which characters to display in a host application.

If you’re having trouble running a host application, the negotiation between InfoConnect and the host might be wrong. If you enter a terminal type that the host does not recognize, InfoConnect reverts to a list of default values until one is found that the host supports.

### Timeout

Specify the number of milliseconds InfoConnect should attempt to make a connection before timing out. The maximum value is 65535. The timeout period begins after host name resolution has taken place. This means an additional delay, usually a few seconds beyond the value specified.

When this is set to 0 (the default), InfoConnect timeout behavior is determined by your Windows operating system.

### Session limits

Select the maximum number of sessions you want to allow for a Telnet connection.

### Close on disconnect

Select to close your session document when you disconnect from the host.

### Set host window size

Select to send the number of rows and columns to the Telnet host whenever they change, so that the host can properly control the cursor if the window size is changed.

### Dynamic terminal size

Select to support dynamic update of the number of rows and columns in the display when the user resizes the terminal window. Your Telnet server and application must also support NAWS (Negotiate About Window Size), otherwise display problems can occur.

Note: You can quickly determine the screen size of the terminal window whenever you hover the mouse cursor over the Row and Column indicator (located in the left corner of the status bar). Under Telnet and Secure Shell connection types, the tooltip will also feature “Auto” if Dynamic terminal size is selected.

### Related Topics

- “Configure Connection Settings Dialog Box (VT)” on page 265

### More Settings RLogin Dialog Box

**Index Term**

- Primary: Rlogin
- Secondary: VT connection settings, more

**Getting there**

1. Open a VT terminal session.
   - The steps depend on your user interface mode (page 120).
2 Under **Host Connection**, click **Configure Connection Settings**.
3 Under **Connection Method**, select **Network**.
4 Under **Network Connection Type**, select **Rlogin**.
5 Under **Connection Options**, click the **More Settings** button.

The options are:

**TCP port**
When connecting to a host via Rlogin, most hosts wait for an incoming connection on TCP Port 513. If your host uses a different port, type that number here.

**Parity**
This setting determines whether a parity bit is generated for each character transmitted. Parity is used to detect errors in data transmission; the number preceding the slash indicates the number of data bits sent.

To use the multinational character set or 8-bit controls, **Parity** must be set to one of the values that offers 8-bit controls. If your communications link generates parity, and you set **Parity** to **8/None**, multinational characters appear on your screen. In this case, set **Parity** to either **8/Even** or **8/Odd**.

**Baud**
Select the rate at which InfoConnect transmits and receives data through the network connection.

**Terminal type**
To override the default terminal, select or type a value here.

In general, you control the following characteristics when you change terminal types:

- Which screen control sequences the host sends to InfoConnect to format the screen.
- The position of the cursor.
- Which characters to display in a host application.

If you’re having trouble running a host application, the negotiation between InfoConnect and the host might be wrong. If you enter a terminal type that the host does not recognize, InfoConnect reverts to a list of default values until one is found that the host supports.

**Timeout**
Specify the number of milliseconds InfoConnect should attempt to make a connection before timing out. The maximum value is 65535. The timeout period begins after host name resolution has taken place. This means an additional delay, usually a few seconds beyond the value specified.

When this is set to 0 (the default), InfoConnect timeout behavior is determined by your Windows operating system.

**Session limits**
Select the maximum number of sessions you want to allow for a Telnet connection.
Close on disconnect

Select to close your session document when you disconnect from the host.

Related Topics

- “Configure Connection Settings Dialog Box (VT)” on page 265

More Settings Serial Port Dialog Box

Index Term
Primary: serial port
Secondary: VT connection settings, more

Getting there

1. Open a VT terminal session.
   The steps depend on your user interface mode (page 120).

   User Interface Mode
   Steps
   Ribbon or InfoConnect Browser
   With a session open in InfoConnect, from the Quick Access Toolbar, click.
   TouchUx
   Tap the Gear icon and then select Document Settings.

2. Under Host Connection, click Configure Connection Settings.
4. Under Serial Port, click the More Settings button.

NOTE: Modem pacing is set from the More Settings - Modem dialog box.

Pacing

It is possible for InfoConnect to transmit data to a serial device faster than the device can process it, or for a serial device to transmit data to InfoConnect faster than InfoConnect can process it.

Should this continue for too long, the slower system's buffer overflows and data is lost. If the serial device recognizes the XON/XOFF handshake, you can prevent the buffer from overflowing by keeping this value set to Xon/Xoff.

Xon/Xoff transmit pacing works as follows:

- When the receive buffer has a limited amount of space left, an XOFF (DC3) character is sent as a signal to stop transmitting.
- After processing most of the backlog of characters in the receive buffer, an XON (DC1) character is sent as a signal to resume transmission.

The two systems continue in this stop-and-go fashion until all the data has been transmitted.

If Hardware is selected, the RTS and CTS pins on the RS-232 serial cable control data flow. When both the Receive and Transmit options under Pacing are set to None and you’re emulating a VT series terminal, Hold Session (VtF1) has no effect.
**Transmit**
Select a flow control method to use when *InfoConnect* transmits data to a serial device on this port.

**Receive**
Select a flow control method to use when the serial device on this port transmits data to *InfoConnect*.

**Char transmit delay**
It is possible for *InfoConnect* to send data to the host faster than the host can receive it. For example, if you paste text from the Clipboard into a host editor such as EDT, you may overrun the host's buffer.

By setting a delay between characters, you can specify how long *InfoConnect* should wait after each character when transmitting blocks of characters to the host.

This delay also affects character transmission during file transfers. Setting a value of 3 at 9600 baud lowers the effective speed of data transmission to about 2400 bits per second.

On a VMS host, setting the terminal's HOSTSYNC characteristic can also help prevent overrunning the host's buffer when pasting data. To do this, enter the following command at the DCL prompt: `SET TERMINAL/HOSTSYNC`.

For backward compatibility, you can enter a value for character delay of up to 255. However, the maximum in *InfoConnect* always reverts to 100.

**Line transmit delay**
Set the amount of time *InfoConnect* should wait after transmitting a carriage return character (the line delimiter) before transmitting the next line.

This setting also affects the delay between frames during file transfer using the WRQ/Reflection protocol. Assigning a delay may help if you are experiencing file transfer problems over an X.25 connection.

**Use threaded I/O**
Select to send communication calls to an independent thread that handles IO (Input/Output) processing, thus improving performance.

**Related Topics**
- “Configure Connection Settings Dialog Box (VT)” on page 265
- “Configure Serial Device Port Dialog Box” on page 568

**Advanced Tab (More Settings Telnet Dialog Box)**

**Getting there**

1. Open a VT terminal session.
   The steps depend on your user interface mode (page 120).
Under Host Connection, click Configure Connection Settings.

3 Under Connection Method, select Network.

4 Under Network Connection Type, select Telnet.

5 Under Connection Options, click the More Settings button.

The options are:

**Session limits**
Select the maximum number of sessions you want to allow for a Telnet connection.

**Terminal default**
Type a value to send as a backup to the Telnet server if the server requests this information, and doesn't recognize the current value set for Terminal type.

**NOTE:** During negotiations, some hosts that could successfully connect using your preferred terminal type skip over this value during negotiations and connect using the backup value specified by Terminal default. To correct this behavior, set Terminal default to an empty value ("").

**Bind to local port**
Select to choose a specific local port for InfoConnect to connect through to communicate with the host.

If this option is cleared, InfoConnect will use the next available port.

**Local port**
Specify a local port.

If this option is set to zero, InfoConnect uses the next available port.

**Send LF after CR**
A "true" Telnet host expects to see a CrNu (carriage return/null) character sequence to indicate the end of a line sent from a terminal (in this case, InfoConnect). There are some hosts on the Internet that are not true Telnet hosts, and they expect to see a Lf (line feed) character following the Cr at the end of a line. If you’re connecting to this type of Telnet host, select this option.

**Telnet location**
(Optional) Type up to 41 characters of descriptive text to provide information about your session. For example, you might include your PC’s location, computer name, or IP address.

This features uses the SEND-LOCATION option supported under Telnet connections (RFC779).

InfoConnect does not initiate a WILL SEND command unless you activate the Telnet location option by typing information in this box.

**Related Topics**
- "Configure Connection Settings Dialog Box (VT)" on page 265
More Settings Modem Dialog Box

Getting there

1. Open a VT terminal session.
   The steps depend on your user interface mode (page 120).

User Interface Mode | Steps
--- | ---
Ribbon or InfoConnect Browser | With a session open in InfoConnect, from the Quick Access Toolbar, click ![Document Settings](image). TouchUx | Tap the Gear icon and then select ![Document Settings](image).

2. Under Host Connection, click Configure Connection Settings.
4. Under Modem, click the More Settings button.

The settings in this dialog box control the modem currently selected in the Modem to use list. If you switch to another modem, these settings will then apply to that modem.

<table>
<thead>
<tr>
<th>Connection mode</th>
<th>Select</th>
<th>To do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>CALL</td>
<td>Dial the remote host specified in the Phone number box.</td>
<td></td>
</tr>
<tr>
<td>AUTO-ANSWER</td>
<td>Connect to the modem and wait for the first ring of an incoming call before answering.</td>
<td></td>
</tr>
<tr>
<td>ANSWER</td>
<td>Connect to the modem and immediately answer any incoming call.</td>
<td></td>
</tr>
<tr>
<td>DIRECT</td>
<td>Connect to the modem so you can enter modem commands in the terminal window.</td>
<td></td>
</tr>
<tr>
<td>DIALBACK</td>
<td>Dial the remote host specified in the Phone number box, disconnect, then wait for a return call. Use this setting if you are using a security dialback host.</td>
<td></td>
</tr>
</tbody>
</table>

Baud rate: Set the rate at which InfoConnect transmits and receives data through the selected modem.

The default baud rate is that specified in Windows Control Panel, from the Modem Properties dialog box, defined when you installed your modem.

When connecting to a host via modem, you may need to select a different baud rate. The maximum baud rate is a function of many factors, such as the type of modem you have and the quality and length of the communications line.
Parity

Set the parity for data transmission through this connection.

This setting determines whether a parity bit is generated for each character transmitted. Parity is used to detect errors in data transmission; the number preceding the slash indicates the number of data bits sent.

To use the multinational character set or 8-bit controls, Parity must be set to one of the values that offers 8-bit controls. If your communications link generates parity, and you set Parity to 8/None, multinational characters appear on your screen. In this case, set Parity to either 8/Even or 8/Odd.

Pacing

It is possible for InfoConnect to transmit data to a serial device faster than the device can process it, or for a serial device to transmit data to InfoConnect faster than InfoConnect can process it.

Should this continue for too long, the slower system's buffer overflows and data is lost. If the serial device recognizes the XON/XOFF handshake, you can prevent the buffer from overflowing by keeping this value set to Xon/Xoff.

Xon/Xoff transmit pacing works as follows:

- When the receive buffer has a limited amount of space left, an XOFF (DC3) character is sent as a signal to stop transmitting.
- After processing most of the backlog of characters in the receive buffer, an XON (DC1) character is sent as a signal to resume transmission.

The two systems continue in this stop-and-go fashion until all the data has been transmitted.

Transmit

Select a flow control method to use when InfoConnect transmits data to a serial device on this port.

Receive

Select a flow control method to use when the serial device on this port transmits data to InfoConnect.

Char transmit delay

It is possible for InfoConnect to send data to the host faster than the host can receive it. For example, if you paste text from the Clipboard into a host editor such as EDT, you may overrun the host's buffer.

By setting a delay between characters, you can specify how long InfoConnect should wait after each character when transmitting blocks of characters to the host.

This delay also affects character transmission during file transfers. Setting a value of 3 at 9600 baud lowers the effective speed of data transmission to about 2400 bits per second.

On a VMS host, setting the terminal's HOSTSYNC characteristic can also help prevent overrunning the host's buffer when pasting data. To do this, enter the following command at the DCL prompt: SET TERMINAL/HOSTSYNC.

For backward compatibility, you can enter a value for character delay of up to 255. However, the maximum in InfoConnect always reverts to 100.

Line transmit delay

Set the amount of time InfoConnect should wait after transmitting a carriage return character (the line delimiter) before transmitting the next line.

This setting also affects the delay between frames during file transfer using the WRQ/Reflection protocol. Assigning a delay may help if you are experiencing file transfer problems over an X.25 connection.

Related Topics

- “Configure Connection Settings Dialog Box (VT)” on page 265


**Select Terminal Type Dialog Box**

<table>
<thead>
<tr>
<th>Index Term</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary: sixel graphics emulation</td>
<td>Secondary: enable</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Index Term</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary: ReGIS Graphics support</td>
<td>Secondary: enable</td>
</tr>
</tbody>
</table>

**Getting there**

1. Open a VT terminal session.

   The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ribbon or InfoConnect Browser</td>
<td>With a session open in InfoConnect, from the Quick Access Toolbar, click .</td>
</tr>
<tr>
<td>TouchUx</td>
<td>Tap the Gear icon and then select Document Settings.</td>
</tr>
</tbody>
</table>

2. Under Terminal Configuration, click Select Terminal Type.

**Terminal Type**

Select the terminal to emulate. This specifies the codes generated by the numeric keypad, the interpretation of control functions, and the response to terminal identification requests. (Values under Terminal automatically reset when you choose a terminal type.)

**Graphics**

Support graphics

Select to support the Tektronix 401x terminal type or the Remote Graphics Instruction Set (ReGIS) by DEC. REGIS includes the following features:

- Up to 16 colors
- Shading with selected patterns and polygon fill
- Rubberband cursors
- Rotated and italicized characters
- Mouse support
- A scaled graphic showing the complete ReGIS screen (800x480 pixels) on the physical display

**Terminal Settings**

Terminal Setup

Set values specific to the type of terminal you are emulating. Changing the Terminal type resets all associated settings (that is, any setting from the Terminal Setup dialog box or the Advanced Options dialog box).
Related Topics

- “Emulation Tab for VT Terminal Types” on page 282
- “Emulation Tab for IBM 3151 Terminals” on page 284
- “Emulation Tab for Wyse Terminal Types” on page 285
- “Advanced Options Dialog Box for VT Terminal Types” on page 287
- “Advanced Options Dialog Box for IBM 3151 Terminals” on page 289
- “Advanced Options Dialog Box for Wyse Terminal Types” on page 291
- “Keyboard & Mouse Tab (Terminal Setup Dialog Box)” on page 292
- “Tabs Tab (Terminal Setup Dialog Box)” on page 299
- “Graphics Tab (Terminal Setup Dialog Box)” on page 299

Emulation Tab for VT Terminal Types

Index Term
Primary: terminal ID
Secondary: setting for VT sessions

Index Term
Primary: double-byte characters (DBCS)
Secondary: support (VT sessions)

Index Term
Primary: color
Secondary: ANSI color, using in VT

Index Term
Primary: ANSI
Secondary: enable ANSI color (VT)

Getting there

1. Open a VT terminal session.
   The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ribbon or Reflection Browser</td>
<td>With a session open in Reflection, from the Quick Access Toolbar, click</td>
</tr>
<tr>
<td>TouchUx</td>
<td>Tap the Gear icon and then select <code>Document Settings</code></td>
</tr>
</tbody>
</table>

2. Under Terminal Configuration, click Configure Terminal Settings.

Set values specific to the type of terminal you are emulating. Changing the Terminal type resets all associated settings (that is, any setting from the Terminal Setup dialog box or the Advanced Options dialog box). These options apply to most VT terminal types.

Emulation Options

**Host character set**
Select a character set to load as the default when a soft reset is performed; or when you invoke the DECSTR sequence. The Host character set may also be specified by the Select Character Set (SCS) sequence.
PC character set
If you need the DOS character set for file transfer or printing, select **DOS** from this list.

Terminal ID
Determines the response that **InfoConnect** sends to the host after a primary device attributes (DA) request. This response lets the host know what terminal functions it can perform. This setting is independent of the **Terminal type** setting.

When set to **WRQ**, **InfoConnect** responds to a primary DA request with the set of features it supports. The responses that **InfoConnect** sends for each terminal ID are listed in the VT Terminal Reference .pdf file.

**InfoConnect** does not support the VT420 feature of multiple sessions over a single serial line.

Terminal IDs that end with the letter J (such as VT101J) indicate Japanese terminal support. These terminal IDs cause **InfoConnect** to send the correct DA response for Japanese terminals, and to size the DBCS (double-byte) characters appropriately.

Online
Select to have **InfoConnect** function as a terminal (also called "remote mode").

Clear this option to enter local mode. In local mode, **InfoConnect** does not attempt to communicate with a host computer. Characters entered from the keyboard appear on the screen, but are not transmitted to the host; nor is any data received from the host (for example, notification of a mail message).

This value is not saved with your session document.

New line
Select to send both a carriage return and line feed when you press Enter (known as new line mode). When **InfoConnect** receives a line feed, form feed, or vertical tab, it moves the cursor to the first column of the next line. When this option is cleared (linefeed mode), the Enter key sends only a carriage return. A line feed, form feed, or vertical tab received from the host moves the cursor down one line in the current column.

If lines on the display keep getting overwritten (that is, the host is not sending a line feed along with a carriage return), select this option. If this option is selected, but the host does not expect to receive a line feed with each carriage return, lines are double-spaced on the display.

Autowrap
Select to make characters wrap to the next line automatically when the cursor reaches the right margin of the display.

This setting is different from the VAX host's terminal wrap characteristic, which is set with the following DCL command:

```
SET TERMINAL/ [NO] WRAP
```

The host command determines whether characters wrap automatically when they reach the maximum terminal width set by the host's SET TERMINAL/WIDTH command (instead of using the right margin of the display, like this setting).

- If terminal wrap is set on the host, characters wrap when they reach the maximum terminal width, regardless of whether **Autowrap** is selected.
- If terminal wrap is not set and **Autowrap** is cleared, new characters overwrite the character at the right margin until a carriage return is entered.

Use ANSI color
Select to use ANSI color in the **InfoConnect** terminal display under **InfoConnect** VT emulations. When selected, the **ANSI Color Mapping** section of the **Modify Theme** dialog box becomes enabled.
Related Topics

- “Advanced Options Dialog Box for VT Terminal Types” on page 287
- “Select Terminal Type Dialog Box” on page 281

Emulation Tab for IBM 3151 Terminals

Index Term
Primary: IBM 3151 emulation options

Getting there

1. Open a VT terminal session.
   The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ribbon or Reflection Browser</td>
<td>With a session open in Reflection, from the Quick Access Toolbar, click</td>
</tr>
<tr>
<td>TouchUx</td>
<td>Tap the Gear icon and then select Document Settings.</td>
</tr>
</tbody>
</table>

2. Under Terminal Configuration, click Select Terminal Type.
3. Under Terminal Type, under Other, select IBM 3151.

IBM 3151 Emulation options

Host character set
Select a character set to load as the default when a soft reset is performed; or when you invoke the DECSTR sequence. The Host character set may also be specified by the Select Character Set (SCS) sequence.

PC character set
If you need the DOS character set for file transfer or printing, select DOS from this list.

Insert Character
Select the way you want the INSERT key to behave.

<table>
<thead>
<tr>
<th>Select</th>
<th>To cause the INSERT key to</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insert Space</td>
<td>Insert a Space character.</td>
</tr>
<tr>
<td>Mode Toggle</td>
<td>Toggle between Insert mode and Replacement mode.</td>
</tr>
</tbody>
</table>

Tab
Select the way you want the TAB key to behave.
Select to move the cursor to

Column
The next tab stop.

Field
The next field of a formatted screen.

**Received LF**
Select how you want a received line feed to be interpreted: as a line feed (LF), or as a carriage return followed by a line feed (LFCR).

**Online**
Select to have InfoConnect function as a terminal (also called "remote mode").
Clear this option to enter local mode. In local mode, InfoConnect does not attempt to communicate with a host computer. Characters entered from the keyboard appear on the screen, but are not transmitted to the host; nor is any data received from the host (for example, notification of a mail message).

This value is not saved with your session document.

**New line**
Select to send both a carriage return and line feed when you press Enter (known as new line mode). When InfoConnect receives a line feed, form feed, or vertical tab, it moves the cursor to the first column of the next line. When this option is cleared (linefeed mode), the Enter key sends only a carriage return. A line feed, form feed, or vertical tab received from the host moves the cursor down one line in the current column.

If lines on the display keep getting overwritten (that is, the host is not sending a line feed along with a carriage return), select this option. If this option is selected, but the host does not expect to receive a line feed with each carriage return, lines are double-spaced on the display.

**Autowrap**
Select to make characters wrap to the next line automatically when the cursor reaches the right margin of the display.

This setting is different from the VAX host's terminal wrap characteristic, which is set with the following DCL command:

```
SET TERMINAL/W [NO]WRAP
```

The host command determines whether characters wrap automatically when they reach the maximum terminal width set by the host's `SET TERMINAL/WIDTH` command (instead of using the right margin of the display, like this setting).

- If terminal wrap is set on the host, characters wrap when they reach the maximum terminal width, regardless of whether Autowrap is selected.
- If terminal wrap is not set and Autowrap is cleared, new characters overwrite the character at the right margin until a carriage return is entered.

**Advanced**
Click to open the Advanced Options dialog box, from which you can configure advanced options for this terminal type.

### Related Topics
- “Advanced Options Dialog Box for IBM 3151 Terminals” on page 289
- “Select Terminal Type Dialog Box” on page 281

### Emulation Tab for Wyse Terminal Types

**Index Term**
Primary: Wyse emulation options
Index Term
Primary: delimiters
Secondary: end-of-transmission

Getting there

1 Open a VT terminal session.
The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ribbon or Reflection Browser</td>
<td>With a session open in Reflection, from the Quick Access Toolbar, click</td>
</tr>
<tr>
<td>TouchUx</td>
<td>Tap the Gear icon and then select Document Settings.</td>
</tr>
</tbody>
</table>

2 Under Terminal Configuration, click Select Terminal Type.
3 Under Terminal Type, select a Wyse terminal type.
4 Under Terminal Settings, click Terminal Setup.

Wyse Emulation options

- **Host character set**: Select a character set to load as the default when a soft reset is performed; or when you invoke the DECSTR sequence. The Host character set may also be specified by the Select Character Set (SCS) sequence.

- **PC character set**: If you need the DOS character set for file transfer or printing, select DOS from this list.

- **Received CR**: Select how you want a received carriage return to be interpreted, as a carriage return alone (CR) or a carriage return followed by a line feed (CRLF).

- **Block terminator**: Select the end-of-transmission delimiter for block sends. This is typically set by the host application. The default value, US/CR, sends a US at the end of a line and a CR at the end of a page/block. CRLF/ETX sends a CR and LF at the end of a line and an ETX at the end of a page.

- **Return key**: Select the character the RETURN key transmits.

- **Enter key**: Select the character the ENTER key transmits.

- **Online**: Select to have InfoConnect function as a terminal (also called "remote mode").

  Clear this option to enter local mode. In local mode, InfoConnect does not attempt to communicate with a host computer. Characters entered from the keyboard appear on the screen, but are not transmitted to the host; nor is any data received from the host (for example, notification of a mail message).

  This value is not saved with your session document.
New line

Select to send both a carriage return and line feed when you press Enter (known as new line mode). When InfoConnect receives a line feed, form feed, or vertical tab, it moves the cursor to the first column of the next line. When this option is cleared (linefeed mode), the Enter key sends only a carriage return. A line feed, form feed, or vertical tab received from the host moves the cursor down one line in the current column.

If lines on the display keep getting overwritten (that is, the host is not sending a line feed along with a carriage return), select this option. If this option is selected, but the host does not expect to receive a line feed with each carriage return, lines are double-spaced on the display.

Autowrap

Select to make characters wrap to the next line automatically when the cursor reaches the right margin of the display.

This setting is different from the VAX host's terminal wrap characteristic, which is set with the following DCL command:

```
SET TERMINAL/[NO] WRAP
```

The host command determines whether characters wrap automatically when they reach the maximum terminal width set by the host's `SET TERMINAL/WIDTH` command (instead of using the right margin of the display, like this setting).

- If terminal wrap is set on the host, characters wrap when they reach the maximum terminal width, regardless of whether `Autowrap` is selected.
- If terminal wrap is not set and `Autowrap` is cleared, new characters overwrite the character at the right margin until a carriage return is entered.

Recognize del

Select this option if you want InfoConnect to interpret a received `DEL` character.

Advanced

Click to open the Advanced Options dialog box, from which you can configure advanced options for this terminal type.

Related Topics

- “Advanced Options Dialog Box for Wyse Terminal Types” on page 291
- “Select Terminal Type Dialog Box” on page 281

Advanced Options Dialog Box for VT Terminal Types

Index Term
Primary: answerback message

Getting there

1. Open a VT terminal session.
   The steps depend on your user interface mode (page 120).
Under **Terminal Configuration**, click **Configure Terminal Settings**.

These options change depending on the terminal type selected.

### VT features

**User features locked**
Select to lock the following items so that they cannot be changed by the host:
- Tab stops
- Keyboard lock
- Screen background
- Scrolling speed
- Auto repeat

**User-defined keys locked**
Select to prevent the host from clearing or redefining user-defined keys.

This value is not saved with your session document.

**Status line**
Select a status line type.

### National Replacement Characters

**National Replacement Set**
Available only when, from the **Terminal Setup** dialog box, ISO-Latin 1 or DEC Supplemental is specified as the Host character set.

Select one of the 12 national replacement character sets built into InfoConnect. National replacement sets are used in 7-bit operating environments, when characters from the supplemental character sets cannot be accessed by 8-bit codes. Each national replacement set replaces certain characters from the ASCII set with accented characters and symbols for a specific national language.

**Use NRC (7-bit) Set**
In an 8-bit operating environment, you can enable a national replacement set with this option.

### Answerback message

**Answerback message**
If the host expects an answer in response to an ENQ character, type the answer here.

**Insert special characters**
Select to allow escape sequences and ASCII control codes in the message (for example, press Enter to include a CR character).

**Auto answerback**
Select to cause the answerback message to be sent to the host automatically after a communications line connection. You may transmit the answerback message at any time by pressing Alt+F7 (this method of sending the message replaces the VT320 keystroke Ctrl+Break).
Clear

Click to clear the answerback message.

Conceal

Click to replace the message with the word <Concealed>. Once a string is concealed, there is no way to unconceal it; you have to replace the text by typing new text, or click Clear to start again.

Serial device to host

Select to maintain a serial connection to the configured port and send any characters received from this serial connection to the existing host connection. This setting is typically enabled by the host application when it is required.

Configure

Click to select and configure a serial port.

The Configure button from the Terminal Setup Advanced Options dialog box is equivalent to the Configure button from the Logging Settings dialog box. You can use the button from either dialog box to configure your serial device port.

Related Topics

- “Emulation Tab for VT Terminal Types” on page 282
- “Select Terminal Type Dialog Box” on page 281
- “Configure Serial Device Port Dialog Box” on page 568

Advanced Options Dialog Box for IBM 3151 Terminals

Index Term
Primary: null suppress

Index Term
Primary: LineTurnAround (LTA) character

Index Term
Primary: block mode
Secondary: sending nulls to IBM 3151 hosts

Getting there

1. Open a VT terminal session.
   The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ribbon or Reflection Browser</td>
<td>With a session open in Reflection, from the Quick Access Toolbar, click</td>
</tr>
<tr>
<td>TouchUx</td>
<td>Tap the Gear icon and then select Document Settings.</td>
</tr>
</tbody>
</table>

2. Under Terminal Configuration, click Select Terminal Type.
3. Under Terminal Type, under Other, select IBM 3151.
The options are:

**IBM 3151 features**

*Null Suppress*  
Send trailing nulls to the system. Clear this option to convert trailing nulls to spaces before sending them to the system.

*Send Null Suppress*  
When in Block mode, InfoConnect won’t send null characters in terminal memory in a Send operation (Send line, Send page, Send memory). Clear this option to have null characters sent as spaces (in Block mode only).

*Line Turnaround Char*  
Define the LineTurnAround (LTA) character.

<table>
<thead>
<tr>
<th>Specify</th>
<th>To define the LTA as</th>
</tr>
</thead>
<tbody>
<tr>
<td>CR (default)</td>
<td>A carriage return</td>
</tr>
<tr>
<td>ETX</td>
<td>End Of Text character, ASCII 3</td>
</tr>
<tr>
<td>EOT</td>
<td>An End Of Transmission Character, ASCII 4</td>
</tr>
<tr>
<td>DC3</td>
<td>A Device Control 3 (XOFF), ASCII 19</td>
</tr>
</tbody>
</table>

*Force Insert Line*  
Insert a null line at the selected line. This happens when an insert line operation is performed by either InfoConnect or the host under IBM 3151 emulation.

Select this option to force off the last line on a screen when a line insertion operation is performed and there is no null line that can be deleted to accommodate the insertion.

*Force Insert Char*  
Insert a null character at the selected character. This happens when an insert character operation is performed by either InfoConnect or the host under IBM 3151 emulation.

Select this option to force a character off a row (or off the end of the screen if Autowrap is on) when a character insertion operation is performed and there is no null character that can be deleted to accommodate the insertion.

**Answerback message**

*Answerback message*  
If the host expects an answer in response to an ENQ character, type the answer here.

*Insert special characters*  
Select to allow escape sequences and ASCII control codes in the message (for example, press Enter to include a CR character).

*Auto answerback*  
Select to cause the answerback message to be sent to the host automatically after a communications line connection. You may transmit the answerback message at any time by pressing Alt+F7 (this method of sending the message replaces the VT320 keystroke Ctrl+Break).

*Clear*  
Click to clear the answerback message.

*Conceal*  
Click to replace the message with the word <Concealed>. Once a string is concealed, there is no way to un conceal it; you have to replace the text by typing new text, or click **Clear** to start again.
Serial device to host
Select to maintain a serial connection to the configured port and send any characters received from this serial connection to the existing host connection. This setting is typically enabled by the host application when it is required.

Configure
Click to select and configure a serial port.

The Configure button from the Terminal Setup Advanced Options dialog box is equivalent to the Configure button from the Logging Settings dialog box. You can use the button from either dialog box to configure your serial device port.

Related Topics

- “Emulation Tab for IBM 3151 Terminals” on page 284
- “Emulation Tab for Wyse Terminal Types” on page 285
- “Configure Serial Device Port Dialog Box” on page 568

Advanced Options Dialog Box for Wyse Terminal Types

Index Term
Primary: label lines

Getting there

1 Open a VT terminal session.
The steps depend on your user interface mode (page 120).

   User Interface Mode | Steps
   ----------- | -------------
   Ribbon or Reflection Browser | With a session open in Reflection, from the Quick Access Toolbar, click 🔗.
   TouchUx | Tap the Gear icon and then select Document Settings.

2 Under Terminal Configuration, click Select Terminal Type.
3 Under Terminal Type, select a Wyse terminal type.
4 Under Terminal Settings, click Terminal Setup.

The options are:

Wyse Features

Label lines
The terminal decides how many label lines are visible by how many display rows are requested. InfoConnect allows you to always have two. If only one label line is visible, use the Shift key to display the second line.

Status line
Select a status line type.

Answerback message

Answerback message
If the host expects an answer in response to an ENQ character, type the answer here.
Insert special characters

Select to allow escape sequences and ASCII control codes in the message (for example, press Enter to include a CR character).

Auto answerback

Select to cause the answerback message to be sent to the host automatically after a communications line connection. You may transmit the answerback message at any time by pressing Alt+F7 (this method of sending the message replaces the VT320 keystroke Ctrl+Break).

Clear

Click to clear the answerback message.

Conceal

Click to replace the message with the word <Concealed>. Once a string is concealed, there is no way to unconceal it; you have to replace the text by typing new text, or click Clear to start again.

Serial device to host

Select to maintain a serial connection to the configured port and send any characters received from this serial connection to the existing host connection. This setting is typically enabled by the host application when it is required.

Configure

Click to select and configure a serial port.

The Configure button from the Terminal Setup Advanced Options dialog box is equivalent to the Configure button from the Logging Settings dialog box. You can use the button from either dialog box to configure your serial device port.

Related Topics

- “Emulation Tab for Wyse Terminal Types” on page 285
- “Select Terminal Type Dialog Box” on page 281
- “Configure Serial Device Port Dialog Box” on page 568

Keyboard & Mouse Tab (Terminal Setup Dialog Box)

Index Term
Primary: warning bells

Index Term
Primary: mouse
Secondary: VT configuration

Index Term
Primary: local echo (VT)
Secondary: keyboard mode

Index Term
Primary: keyboard
Secondary: VT configuration

Index Term
Primary: format bell (VT)

Index Term
Primary: echo, local (VT)
Secondary: keyboard mode

Index Term
Primary: break (VT keyboard)
Getting there

1. Open a VT terminal session.
   The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ribbon or Reflection Browser</td>
<td>With a session open in Reflection, from the Quick Access Toolbar, click</td>
</tr>
<tr>
<td>TouchUx</td>
<td>Tap the Gear icon and then select Document Settings.</td>
</tr>
</tbody>
</table>

2. Under Terminal Configuration, click Configure Terminal Settings.
Keyboard modes

Auto repeat
Select to make most keys repeat when pressed. The Shift, Return, and Ctrl keys do not auto repeat.

Break enabled
Select to enable the Break function. When cleared, both the Break command and the VtF5 (Break) keystroke (Ctrl+Break) are disabled.

Local echo
Select to cause each character typed at the keyboard to be immediately displayed on the screen. When you're communicating with the host computer, each character typed at the keyboard is transmitted to the host. Most host systems (for example, a VAX running VMS) immediately send the same character back to the terminal (that is, echo the character). The character is not displayed on the screen until it is received back from the host.

When you're online and you select this option, each character is sent two places: directly to display memory (the screen), and to the host computer. On an echoing host system, this means that each character you type appears twice on the screen. Select this option only when communicating with host systems that do not echo each typed character; for example, some public networks.

Bells

Margin bell
Select to have your computer beep when the cursor is eight characters from the right margin.

Warning bell
Select to have your computer beep when the ASCII bell character (Bel, decimal 7) is received from the host or entered from the keyboard.

To disable the format bell (which beeps, for example, when InfoConnect encounters an unprotected field), clear the Warning bell option.

Terminal keys

VT backspace sends
Select the function that you want your Backspace key to send.

You can also remap the Backspace key using the Keyboard Mapper. Doing so has no effect on the VT backspace sends option. However, this option is affected when you remap the VtBackArrow terminal keystroke.

Cursor keys
This option controls the characters that the four Arrow keys (on both the numeric and editing keypad) transmit. This setting is typically set by the host and is not saved to the session document.

If the Arrow keys aren't working properly, it may mean that this option remained incorrectly set to Application when a host program terminated abnormally. If changing this setting back to Normal doesn't fix the problem with the Arrow keys, check the value set for Terminal ID, and verify that it matches the type of terminal the host expects. The VT52 setting, for instance, sends different cursor key codes than the other (ANSI) modes.

NOTE: This feature is unavailable for WYSE emulation.
Keypad

This option controls the characters that the numeric keypad keys transmit. This setting is typically set by the host and is not saved to the session document.

If the number or PF keys aren’t working properly, it may mean that this option remained incorrectly set to Application when a host program terminated abnormally. If changing this setting back to Numeric doesn’t fix the numeric keypad, check the VT operating level Mode and make sure it matches that of the host. The VT52 setting, for instance, sends different keypad codes than the other (ANSI) modes.

NOTE: This feature is unavailable for WYSE emulation.

Keyboard shortcuts

NOTE: Settings in the Keyboard Mapper override these options.

<table>
<thead>
<tr>
<th>Standard File and Edit menu shortcuts</th>
<th>Select to enable the following keyboard shortcuts:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PC keystroke</strong></td>
<td><strong>Terminal function</strong></td>
</tr>
<tr>
<td>Ctrl+A</td>
<td>Select All</td>
</tr>
<tr>
<td>Ctrl+C</td>
<td>Copy</td>
</tr>
<tr>
<td>Ctrl+F</td>
<td>Find</td>
</tr>
<tr>
<td>Ctrl+Shift+F</td>
<td>Find Next</td>
</tr>
<tr>
<td>Ctrl+O</td>
<td>Open File</td>
</tr>
<tr>
<td>Ctrl+P</td>
<td>Print File</td>
</tr>
<tr>
<td>Ctrl+V</td>
<td>Paste</td>
</tr>
<tr>
<td>Ctrl+X</td>
<td>Cut</td>
</tr>
</tbody>
</table>

Hold Screen shortcuts

Select to have InfoConnect use Ctrl+Q to start and Ctrl+S to stop the processing of data from the host.

Clear Hold Screen shortcuts if you use a host application (such as EMACS) that requires the use of the Ctrl+S and Ctrl+Q characters. Cleaning this option allows the Ctrl+S keystroke to send to the host a Ctrl+S character (ASCII decimal 19), and the Ctrl+Q keystroke to send to the host a Ctrl+Q character (ASCII decimal 17).
Mouse shortcuts

- **Always copy selected text to the clipboard**
  Text selected using the left mouse button and drag action is copied to the Clipboard when you release the mouse button.

- **Right-click pastes clipboard text**
  The contents of the Clipboard are pasted into InfoConnect at the cursor location when the right mouse button is clicked.

  **NOTE:** Settings in the Mouse Mapper override these options.

- **Middle button pastes clipboard text**
  The contents of the Clipboard are pasted into InfoConnect at the cursor location when the middle mouse button is clicked.

  **NOTE:** Settings in the Mouse Mapper override these options.

- **Rectangular Selection**
  Dragging the mouse across an area selects only the text within that area. When this option is cleared (unchecked), the selection wraps to line ends.

Related Topics

- “Select Terminal Type Dialog Box” on page 281
- “Specifying a Custom Keyboard Map” on page 177
- “Specifying a Mouse Map” on page 184

Keyboard & Mouse Tab for IBM 3151 Terminals

**Index Term**

- **Primary:** mouse
- **Secondary:** IBM 3151 configuration

**Index Term**

- **Primary:** local echo (VT)
- **Secondary:** keyboard mode (IBM 3151)

**Index Term**

- **Primary:** keyboard
- **Secondary:** IBM 3151 configuration

**Index Term**

- **Primary:** echo, local (VT)
- **Secondary:** keyboard mode (IBM 3151)

Getting there

1. **Open a VT terminal session:**
   The steps depend on your [user interface mode](page 120).

   **User Interface Mode**
   **Steps**
   - **Ribbon or Reflection Browser**
     With a session open in Reflection, from the **Quick Access Toolbar**, click 🠆.
   - **TouchUx**
     Tap the Gear icon and then select 🠆 **Document Settings**.

2. **Under Terminal Configuration, click Configure Terminal Settings.**
Keyboard modes

Auto repeat
Select to make most keys repeat when pressed. The Shift, Return, and Ctrl keys do not auto repeat.

Break enabled
Select to enable the Break function. When cleared, both the Break command and the VtF5 (Break) keystroke (Ctrl+Break) are disabled.

Local echo
Select to cause each character typed at the keyboard to be immediately displayed on the screen. When you're communicating with the host computer, each character typed at the keyboard is transmitted to the host. Most host systems (for example, a VAX running VMS) immediately send the same character back to the terminal (that is, echo the character). The character is not displayed on the screen until it is received back from the host.

When you're online and you select this option, each character is sent two places: directly to display memory (the screen), and to the host computer. On an echoing host system, this means that each character you type appears twice on the screen. Select this option only when communicating with host systems that do not echo each typed character; for example, some public networks.

Bells

Margin bell
Select to have your computer beep when the cursor is eight characters from the right margin.

Warning bell
Select to have your computer beep when the ASCII bell character (Bel, decimal 7) is received from the host or entered from the keyboard.

To disable the format bell (which beeps, for example, when InfoConnect encounters an unprotected field), clear the Warning bell option.

Terminal keys
Select how the following keys act when pressed under IBM 3151 emulation.

Send Key
The default value transmits the entire page to the host. Select Line to have InfoConnect transmit only the selected line to the host.

Return Key
The default value transmits a newline request to the host. Select Field to have InfoConnect move to the next field of a formatted screen.

Enter Key
The default value acts as a Send key. Select Return to have the Enter key act as a Return key.

Backspace Key
Select a value to send when the Backspace key is pressed.

The values available represent the unshifted/shifted states you can choose from. For example, selecting BS/DEL means pressing Backspace sends a Backspace to the host. Pressing the Shift key and then pressing Backspace will send a Delete to the host.

<table>
<thead>
<tr>
<th>This value</th>
<th>Designates</th>
</tr>
</thead>
<tbody>
<tr>
<td>BS</td>
<td>Backspace, ASCII 8.</td>
</tr>
<tr>
<td>DEL</td>
<td>Delete, ASCII 127.</td>
</tr>
<tr>
<td>CAN</td>
<td>Cancel, ASCII 24.</td>
</tr>
</tbody>
</table>
Keyboard shortcuts

NOTE: Settings in the Keyboard Mapper override these options.

<table>
<thead>
<tr>
<th>Standard File and Edit menu shortcuts</th>
<th>Select to enable the following keyboard shortcuts:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>PC keystroke</td>
</tr>
<tr>
<td></td>
<td>Ctrl+A</td>
</tr>
<tr>
<td></td>
<td>Ctrl+C</td>
</tr>
<tr>
<td></td>
<td>Ctrl+F</td>
</tr>
<tr>
<td></td>
<td>Ctrl+Shift+F</td>
</tr>
<tr>
<td></td>
<td>Ctrl+O</td>
</tr>
<tr>
<td></td>
<td>Ctrl+P</td>
</tr>
<tr>
<td></td>
<td>Ctrl+V</td>
</tr>
<tr>
<td></td>
<td>Ctrl+X</td>
</tr>
</tbody>
</table>

Hold Screen shortcuts

Select to have InfoConnect use Ctrl+O to start and Ctrl+S to stop the processing of data from the host.

Clear Hold Screen shortcuts if you use a host application (such as EMACS) that requires the use of the Ctrl+S and Ctrl+Q characters. Clearing this option allows the Ctrl+S keystroke to send to the host a Ctrl+S character (ASCII decimal 19), and the Ctrl+Q keystroke to send to the host a Ctrl+Q character (ASCII decimal 17).

Mouse shortcuts

Always copy selected text to the clipboard
Text selected using the left mouse button and drag action is copied to the Clipboard when you release the mouse button.

Right-click pastes clipboard text
The contents of the Clipboard are pasted into InfoConnect at the cursor location when the right mouse button is clicked.

NOTE: Settings in the Mouse Mapper override these options.

Middle button pastes clipboard text
The contents of the Clipboard are pasted into InfoConnect at the cursor location when the middle mouse button is clicked.

NOTE: Settings in the Mouse Mapper override these options.

Rectangular Selection
Dragging the mouse across an area selects only the text within that area. When this option is cleared (unchecked), the selection wraps to line ends.

Related Topics
- “Keyboard & Mouse Tab (Terminal Setup Dialog Box)” on page 292
- “Emulation Tab for IBM 3151 Terminals” on page 284
- “Advanced Options Dialog Box for IBM 3151 Terminals” on page 289
Tabs Tab (Terminal Setup Dialog Box)

Index Term
Primary: tabs
Secondary: setting stops for VT sessions

Getting there

1. Open a VT terminal session.
   The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ribbon or Reflection Browser</td>
<td>With a session open in Reflection, from the Quick Access Toolbar, click .</td>
</tr>
<tr>
<td>TouchUx</td>
<td>Tap the Gear icon and then select Document Settings.</td>
</tr>
</tbody>
</table>

2. Under Terminal Configuration, click Configure Terminal Settings.

Tab Stops

Tab stops
Use the mouse, cursor keys, or Spacebar to move the scroll bar to the desired column and click; a T appears on the ruler. Repeat the procedure until all tabs are set. If you're in 132-column mode, use the scroll bars to move beyond the 81st column to set a tab stop.

To clear a single tab stop, click the tab position with the mouse (each click of the mouse toggles between setting a tab stop and clearing it).

Clear All
Click to clear all tabs set on the tab ruler.

The left margin is always an implicit tab stop and is not affected by Clear All.

Set Every
To set tab stops at equidistant positions, enter a number in the box and click Set Every.

Graphics Tab (Terminal Setup Dialog Box)

Index Term
Primary: VGA dithering (VT graphics)

Index Term
Primary: Tektronix

Index Term
Primary: sixel graphics emulation
Secondary: configuring

Index Term
Primary: scrolling (VT)
Secondary: sixel images

Index Term
Primary: ReGIS Graphics support
Secondary: configuring
Index Term
Primary: macrograph reports

Index Term
Primary: graphics
Secondary: output cursor

Index Term
Primary: dithering, VGA (VT graphics)

Index Term
Primary: cursor
Secondary: graphics output

Getting there

1 Open a VT terminal session.
The steps depend on your user interface mode (page 120).

User Interface Mode Steps
Ribbon or Reflection Browser With a session open in Reflection, from the Quick Access Toolbar, click .
TouchUx Tap the Gear icon and then select Document Settings.

2 Under Terminal Configuration, click Configure Terminal Settings.

ReGIS

Terminal type
Select which terminal is emulated and how many shades or colors are available in ReGIS:

- The VT240 and VT330 are monochrome graphics terminals, providing up to four shades of gray at once.
- The VT241 and VT340 are color graphics terminals; the VT241 provides up to four different colors at once, while the VT340 provides up to 16 different colors.

This value is independent of the settings for Terminal ID on the Emulation tab.

Graphics output cursor
Clear this option to hide the graphics output cursor.

ReGIS displays two types of graphic cursors: an input cursor and an output cursor. The input cursor appears when ReGIS is waiting for graphics input, such as a cursor position report. You can position the input cursor with the mouse or the Arrow keys. A graphics output cursor appears when ReGIS is waiting for commands from the host (or from the ReGIS command line).

Displaying the graphics output cursor can also be controlled by the ReGIS command $ (C<n>). The ReGIS command option controls the style of the graphics output cursor.
Macrograph reports

Clear this option to disable macrograph reporting for security or other reasons.

A macrograph is a way to define and store a set of ReGIS commands as a single character; that is, as a graphics macro. By default, ReGIS can report the contents of a specific macrograph.

Sixel

Print mode

Select how sixel data is sent to the host or a Digital printer.

<table>
<thead>
<tr>
<th>Select</th>
<th>To do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compress</td>
<td>Print an image pixel-for-pixel.</td>
</tr>
<tr>
<td>Rotate</td>
<td>Rotate the image 90 degrees (from portrait to landscape orientation).</td>
</tr>
<tr>
<td></td>
<td>If you want the actual output to print rotated,</td>
</tr>
<tr>
<td></td>
<td>from the Print Setup dialog box, select Landscape as the Orientation option.</td>
</tr>
<tr>
<td>Expand</td>
<td>Print each pixel twice as wide and twice as high.</td>
</tr>
<tr>
<td></td>
<td>Expanded printing applies only when sending sixel data to the host (selected by the Destination), not to a PC printer.</td>
</tr>
</tbody>
</table>

Destination

When you print a graphics image using the ReGIS hard copy command, the image can be sent either to the host or a Digital printer.

When the graphics image is sent to the host, it is sent as a stream of sixel data. The host must be ready to accept the data; for example, by collecting it in a file.

When the image is sent to a host printer, it is printed as a bitmap image. If Bypass Windows print driver is selected from the Print Setup dialog box, a sixel data stream is sent to the printer (assuming you are printing to a Digital printer).

Graphics level

With this option, you can match InfoConnect to Digital printer capabilities, such as aspect ratio, horizontal grid size, background printing, and color printing. The sixel data string sent to the host varies based on the graphics level for details about the sixel data format.

This setting applies only when sending sixel data to the host or a Digital printer when Bypass Windows printer driver is selected from the Print Setup dialog box.

This setting also affects saving display sixels from the Save Display As dialog box.

Color printing

Select Color or Mono (black and white) printing.

This setting applies only when sending sixel data to the host or a Digital printer when Bypass Windows printer driver is selected from the Print Setup dialog box.

This setting also affects saving display sixels from the Save Display As dialog box.
### Color specification

If you are printing in color, select the color coordinate system to use for color sixel printing.

This setting applies only when sending sixel data to the host or a Digital printer when **Bypass Windows printer driver** is selected from the **Print Setup** dialog box.

This setting also affects saving display sixels from the **Save Display As** dialog box.

### Scrolling

A sixel is a vertical column of six pixels used to display graphic images. When scrolling is enabled, the sixel image begins at the current text position. A sixel image will scroll the display when the image reaches the bottom margin of the display (if it doesn't fit, the image may also scroll off the top of the display). A graphics newline character is sent immediately after the sixel dump, and the text cursor is set at the same position as the sixel cursor when you exit sixel mode.

When this option is cleared, the sixel image begins at the upper left of the display. When the image reaches the bottom margin, the display does not scroll, and additional sixel commands are ignored. Upon exiting sixel mode, the text cursor is set at the same position as when sixel mode was entered.

### Tektronix

#### CR processing

When you select CR-LF, a linefeed character is appended to each carriage return character. This is useful when you're operating in local mode (when, from the **Terminal Setup** dialog box, on the **Emulation** tab, the **Online** option is cleared).

#### LF processing

When you select LF-CR, a carriage return character is appended to each linefeed character. This is useful when you're operating in local mode (when, from the **Terminal Setup** dialog box, on the **Emulation** tab, the **Online** option is cleared).

#### Del processing

InfoConnect interprets DEL characters as valid ASCII characters. To have InfoConnect ignore DEL characters, select **Ignored**.

#### GIN terminator

Select which character or characters act as a terminator for cursor address information.

#### Destructive overwrite

By default, a character typed over another one in Tektronix emulation does not erase the first one; the second character is superimposed on the first. Select this option to specify that you want a character cell blanked out before a character is drawn.
Printing

Print graphics
Select this option to print graphics along with the text when sending sixels to the host or to a Digital printer.

This setting also affects saving display sixels from the Save Display As dialog box.

Print background
Select whether to print the graphics image with or without the background color when sending sixels to the host or a Digital printer.

Clear this option to print to a printer that can print only a black and white bitmap, and no shades of gray. The colors of the screen image are inverted for printing. This makes light-colored graphics print as black images on white paper. If you’re printing 16-color graphics, the resulting images may be unpredictable as a 16-color image must be converted to a 2-color (black and white) bitmap. This applies to sixels generated as well as graphics printed on Windows printers.

This setting also affects saving display sixels from the Save Display As dialog box.

Copying

VGA dithering
Select to cause bitmaps copied to the Clipboard to be dithered to standard VGA colors. This is useful for pasting graphic images into Windows applications that are not palette-aware (for example, Windows Paint).

Select the level of dithering to be applied when a 256-color image is pasted into the terminal window from the Clipboard. Because InfoConnect emulates a 16-color terminal, it uses an algorithm to determine exactly how colors should be mapped. The best dithering choice for an image may vary depending on the image.

Select To produce this
Half A pasted image that takes a middle course between the None and Full values.
Full The most accurate color translation. However, the pasted image could have a grainy, textured appearance.
None A pasted image with a color specified for each individual pixel. This option produces the crispest image. However, there may be no distinct color boundaries.

NOTE: Selecting None as the level of VGA dithering does not have the same effect as clearing the VGA dithering check box. The state of the check box controls whether the image is converted to a VGA-displayable image when it is copied — if the check box is cleared, the exact image is copied (including its exact colors). This works well when pasting graphics into applications that are palette-aware (such as Photoshop).

For applications that are not palette-aware (such as Windows Paint), select this check box and pick a dithering option (explained above) that determines how InfoConnect processes the pixels.
Copy background

When cleared, bitmaps copied to the Clipboard are edited so that the background color is set to white, and all near-white colors are set to black. This is useful for pasting graphic images into word processing documents.

Related Topics

- “ReGIS Graphics Support” on page 264
- “Select Terminal Type Dialog Box” on page 281

Set Up Display Settings Dialog Box

Index Term
Primary: scrolling (VT)
Secondary: configure

Index Term
Primary: scrollback (VT)
Secondary: configure

Index Term
Primary: display memory (VT)
Secondary: configure

Index Term
Primary: control characters (VT)

Getting there

1 Open a VT terminal session.
   The steps depend on your user interface mode (page 120).

   User Interface Mode Steps
   Ribbon or InfoConnect Browser
   With a session open in InfoConnect, from the Quick Access Toolbar, click .

   TouchUX
   Tap the Gear icon and then select Document Settings.

2 Under Terminal Configuration, click Set Up Display Settings.
The options are:

**Display Memory**

Display memory contains both the information visible on the display and (if Enable scrollback is selected) information that has scrolled off of the display. It is a log of what has recently been sent from the host to the PC. Display memory stores only text; if you have graphics on the display, they are not scrolled into display memory.

**Memory blocks (8K/block)**

Type the number of memory blocks to allocate for display memory.

The default is 9 blocks of 8 kilobytes each, or 72K of display memory. This holds approximately 22 pages of display memory when each line is exactly 80 characters long.

The number of bytes you are currently using is calculated on each character of text; you’ll have more “pages” of display memory when your text lines do not run all the way out to the right margin.

**Enable scrollback**

With scrollback enabled, the session maintains a buffer of lines that have scrolled off the terminal screen. This allows the user to scroll back through this buffer and read or copy it. A real terminal does not have this extra memory and clearing this selection will accurately emulate the behavior of the terminal.

**NOTE:** This setting does not affect VT420 or Wyse paged memory.

**Compress blank lines**

Select to save room in display memory by compressing multiple blank lines into a single blank line.

**Save display before clearing**

Select to move the data on the display into display memory when you or the host clear the display. Otherwise, the data is discarded.

**Save from scrolling regions**

When a scrolling region is set on the display, by default, text that scrolls out of the scrolling region is not saved in display memory. If you want the text from the scrolling region moved into display memory, select this option.

If a scrolling region is set by a text editor, selecting this option can cause display memory to fill quickly; every time you scroll down your document, text that scrolls off the top of the display is moved into display memory. For most situations, it’s best to leave this option cleared.

**Scrolling**

**Smooth scrolling**

Select to display all lines in sequence as they are received from the host, even when doing so results in a delay between receiving a line and displaying it.

**Jump scrolling**

Select to display incoming lines of data as quickly as they are received from the host, even when doing so results in some lines being “jumped over” and not displayed. The jumped-over lines are captured in the display memory, so you can still see them by scrolling back through display memory.

You’ll notice the effect of this setting only when data from the host is arriving faster than it can be displayed.

**Jump scroll speed**

Select the number of lines to "jump over" if it becomes necessary to catch up with data coming in from the host.
Control Characters

The VT terminal character set includes 65 control characters with decimal values 0-31 and 127-159.

Interpret control characters
Select to interpret control characters as they are received from the host. For example, the carriage return character moves the cursor to the left margin.

Display control characters
Select to display control characters rather than interpret them. This lets you see exactly which characters are received from the host and which control characters are generated by the keyboard.

Dimensions

Number of rows
Specify the number of lines on the display, not including the status line. This defines the display size, and the host can position and write characters anywhere within this area. The maximum number of rows you can enter depends on the display resolution; the higher the screen resolution your video adapter provides, the more rows you can fit on the screen.

When you change the number of rows, characters are scaled vertically to fit the desired number of rows, or lines, in the terminal window. The display is erased (all of display memory is cleared) before the new setting takes effect.

Setting rows here does not change the number of rows the host can recognize.

Number of characters per row
Specify the number of characters per row (that is, columns) in the scrolling region in the terminal window (between 80 and 999).

When you change the number of characters per row, the font size is adjusted in an attempt to fit all the characters in the terminal window. If all the characters cannot be displayed, a horizontal scroll bar appears to the right of the status bar.

Setting the number of characters per row here does not change the number of characters per row the host can recognize.

NOTE: Changing the number of characters per row in the display automatically changes the number of columns used by your printer in the Columns per row box in the Page Options dialog box.

Set Up Safeguards Dialog Box

Index Term
Primary: scrollback (VT)
Secondary: clear

Index Term
Primary: safeguards

Index Term
Primary: display memory (VT)
Secondary: clear
Getting there

1 Open a VT terminal session.
   The steps depend on your user interface mode (page 120).

   **User Interface Mode**
   - Ribbon or InfoConnect Browser: With a session open in InfoConnect, from the Quick Access Toolbar, click Document Settings.
   - TouchUx: Tap the Gear icon and then select Document Settings.

2 Under Terminal Configuration, click Set Up Safeguards.

**Safeguards**

- Clear display and scrollback buffer when disconnected: Delete all data from display memory when a session is disconnected from the host.
- Save Secure Shell user name: Clear this option to prevent the user name you provide for this host session from being saved into the settings file, or recorded in a macro.
- Cache Secure Shell user name: Select to temporarily store the user name entered for a Secure Shell session until the Reflection workspace is closed. (When this option is selected, users are not prompted for a user name when they reconnect unless they reopen the workspace. When it is unselected, the user name is cleared from memory immediately after a successful connection and users are prompted for a user name when they reconnect.)

**Related Topics**
- “Set Up Display Settings Dialog Box” on page 304

**Connect to Host Dialog Box**

This dialog box appears when you start a session for which no host has been specified.

The options are:

- **Host name**: Type the host name or IP address of the terminal to which you want to connect.
- **OK**: Click to connect the session immediately.
- **Cancel**: Click to configure more than just the host name for this session.

On the Quick Access Toolbar at the top of the workspace, click Document Settings. Then, under Host connection, click Configure Connection settings.

**Performing a Trace**

Your Technical Support analyst may ask you to trace InfoConnect events to troubleshoot problems. These instructions show how to perform traces on IBM 3270, IBM 5250, and VT sessions.
Run a Trace for an IBM 3270 or 5250 Session

While troubleshooting a problem in an IBM 3270 or 5250 session, technical support may request that you obtain one or more traces. Three kinds of traces can be done: host-data, command, and HLLAPI.

<table>
<thead>
<tr>
<th>Trace File Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host-data trace (*.hst)</td>
<td>Captures information passed between a terminal, or printer, session and the host. This type of trace is useful when a host connection is working, but the terminal or printer session does not behave as expected. Host traces are not useful when a connection to the host cannot be established.</td>
</tr>
<tr>
<td>Command trace (*.cmd)</td>
<td>Captures actions within InfoConnect. Each action, such as clicking a button or entering text, represents an individual command. Command traces are useful in determining if commands are correct in a script, macro, or program using OLE automation. Command traces can also be used to determine which command to use when writing a script. Use a text editor to view the command trace and determine which commands are needed to accomplish the task.</td>
</tr>
<tr>
<td>HLLAPI trace</td>
<td>Enables you to see the HLLAPI calls the application is making, including return codes. (HLLAPI is an API specified by IBM for automating terminal tasks.)</td>
</tr>
</tbody>
</table>
To generate a host-data or command trace

1. Open a session or create a new session.

2. **Open the Start Trace dialog box.**
   The steps depend on your user interface mode (page 120).

   - **User Interface Mode**
     - **InfoConnect Ribbon**
       On the Tools ribbon, from the Tracing group, click **Start Trace**.
     - **InfoConnect Browser**
       On the InfoConnect menu, choose Tools, Trace, and then **Start Trace**.
     - **TouchUx**
       Tap the Wrench icon and then under Trace, select **Start Trace**.

3. In the Start Trace dialog box, specify a name for the trace file. If you have spoken with a support technician, use your service request number as the name of your trace file.

   - **For this type of trace**
     - Host data .HST
     - Command .CMD

4. Click **Save**.
   "Tracing started..." displays in the InfoConnect status bar, indicating the trace is active.

5. Perform the actions that reproduce the problem you want recorded in the trace.

6. **Stop the Trace.**
   The steps depend on your user interface mode (page 120).

   - **User Interface Mode**
     - The **InfoConnect Ribbon**
       On the Tools ribbon, from the Tracing group, click **Stop Trace**.
     - The **InfoConnect Browser**
       On the InfoConnect menu, choose Tools, Trace, and then **Stop Trace**.
     - **TouchUx**
       On the InfoConnect menu, tap the Wrench icon and then under Trace, select **Stop Trace**.

7. Upload the trace file as a binary file to http://upload.attachmate.com. If the problem relates to a service request you are currently working on with a technician, include the Attachmate service request number with the trace and let the technician know when the file is uploaded.

To generate a HLLAPI trace

1. Click the Windows Start button.

2. In the Start Search box, type win.ini and press Enter to open your Win.ini file in Notepad.

3. Add the following two lines to the end of the Win.ini file:

   ```ini
   [Reflection HLLAPI]
   ExtTraceOn=1
   ```
4 In the **InfoConnect** Workspace, open a session or create a new session to connect to your IBM host.

5 Start the HLLAPI application.

6 Perform the actions that reproduce the problem you want recorded in the trace.

7 Close the HLLAPI application.

   The trace file is automatically named HLL*.TMP, where * is a randomly generated hex number. The file is located in the PC’s TEMP directory, if a TEMP directory has been defined in the System Environment settings. Otherwise, it is located in the root Windows directory.

8 Re-open the Win.ini file, and change the ExtTraceOn setting to zero by changing the last line of the ini file:

   ```
   ExtTraceOn=0
   ```

9 Upload the trace file as a binary file to [http://upload.attachmate.com](http://upload.attachmate.com). If the problem relates to a service request you are currently working on with a technician, include the Attachmate service request number with the trace and let the technician know when the file is uploaded.

### Perform an Event Trace (VT)

Your Technical Support analyst may ask you to perform an event trace. An event trace "captures" all communications activity (except for modem commands), and all keystrokes, commands, and menu and dialog box selections. This data is saved in an event file.

To use the trace data, you will need to process it to create a report of the data or to create a file that "plays" the trace.

**To perform an event trace**

1 **Open the Start trace dialog box.**

   With a VT session open in the workspace, open the Start Trace dialog box as follows:

   The steps depend on your user interface mode (page 120).

   **User Interface Mode** | **Steps**
   --- | ---
   Ribbon | On the **Tools** tab, in the **Tracing** group, click **Start Trace**.
   **InfoConnect** Browser | On the Browser **InfoConnect** menu, choose **Tools**, **Trace** and then **Start Trace**.
   **TouchUx** | Tap the Wrench icon, and then under **Trace**, select **Start Trace**.

2 In the Start Trace dialog box, enter a path and file name for the event (.rev) file and click **Save**. (If you have spoken with a support technician, use your service request number as the name of your trace file.)

3 Perform the actions required to demonstrate the problem.

4 After the problem is demonstrated, click **Stop Trace** in the **Tracing** group (if using the Ribbon) or on the **Tools, Trace** menu (if using the Browser).
The trace data is saved in the event file.

5 Upload the trace file as a binary file to http://upload.attachmate.com (http://upload.attachmate.com). If the problem relates to a service request you are currently working on with a technician, include the Attachmate service request number with the trace and let the technician know when the file is uploaded.

To process trace data

After creating the event file, follow these steps to create a report or a script that "plays" the trace.

1 Open the Process Event Trace dialog box.

With a VT session open in the workspace, open the Process Event Trace dialog box as follows:
The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ribbon</td>
<td>On the Tools tab, in the Tracing group, click Process Trace.</td>
</tr>
<tr>
<td>InfoConnect</td>
<td>In the search box, enter P and then, under Actions, select Process Trace.</td>
</tr>
<tr>
<td>TouchUX</td>
<td>Tap the Wrench icon and then, under Trace, select Process Trace.</td>
</tr>
</tbody>
</table>

2 Select how to process the trace:

<table>
<thead>
<tr>
<th>To</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a InfoConnect Basic script that you can use to play the trace.</td>
<td>Select Generate script.</td>
</tr>
<tr>
<td>Create a report in a text-based file format.</td>
<td>Select Generate report and then select options to format the report under Report format. (See Process Event Trace Dialog Box (VT Sessions.) (page 312)</td>
</tr>
</tbody>
</table>

3 Click OK. The Open Events dialog box appears.

4 In the File name box, select the event file to process, and click Open.
   - If you selected Generate script, the Save Event Commands dialog box opens.
   - If you selected Generate report, the Save Event Report dialog box opens.

5 Enter the file name and click Save.

   Scripts are saved as InfoConnect Basic .rbs files.
   Reports are saved in .txt files. The report is automatically displayed after it is saved.

To play trace data

1 Open the Play Trace dialog box.

   The steps depend on your user interface mode (page 120).
In the Play Trace dialog box, select an event trace .rbs file and click Open.

Related Topics

- “Configure Connection Settings Dialog Box (VT)” on page 265
- “Configure Serial Device Port Dialog Box” on page 568

## Process Event Trace Dialog Box (VT Sessions)

**Getting there**

With a VT session open in the workspace, open the Process Event Trace dialog box as follows:

The steps depend on your user interface mode (page 120).

### User Interface Mode  Steps

<table>
<thead>
<tr>
<th>Ribbon</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>On the Tools ribbon, from the Tracing group, click Process Trace.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>InfoConnect Browser</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>In the search box, enter P and then, under Actions, select Process Trace.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TouchUX</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tap the Wrench icon and then, under Trace, select Process Trace.</td>
<td></td>
</tr>
</tbody>
</table>

This dialog box allows you to process a trace created when troubleshooting a problem in a VT session.

**NOTE:** For instructions that show how to trace events, process a trace, generate a trace report, or play a trace, see “Perform an Event Trace (VT)” on page 310
The options are:

- **Generate script**
  Create a report with a .rbs file extension in the folder you select. Use this option to process the trace (.rev) file into a Reflection Basic script file.

- **Generate report**
  Create a report with a .txt file extension in the folder you select. Use this option to process the trace (.rev) file into a text-based file format.

### Report format

If you selected **Generate report**, you can also select any of these options:

- **Settings details and system information**
  Select to include settings and information about the operating system of your machine.

- **Timing**
  Select to put a time stamp beside each event item performed during the trace.

- **Display memory**
  Select to include all the information in the display memory buffer.

- **Network protocol details**
  Select to include details about the network protocol used for the connection.

- **Code page details**
  Select to include the code page information used by the PC.

- **Redact**
  Select to expunge sensitive information from traces. Specifically, this option replaces alpha characters with X's and numeric characters with 9's. Control and escapes sequences are not affected, only application data.

- **String syntax**
  Select the format used to display strings. Choose from **Traditional**, **Visual Basic**, or **C** string syntax.
Navigation

Easily navigate the InfoConnect 2014 workspace by clicking tabs to switch between sessions, or to access controls. Navigate within sessions using Screen History controls. With the multi-level search capabilities, you can search everything from InfoConnect dialog boxes to Web content on Google.

In this Chapter

- “Open a Web Session” on page 315
- “Navigate the Ribbon” on page 317
- “Search” on page 318
- “Capture Screen History” on page 320
- “Capture Screens Manually” on page 322
- “Navigate Screen History From the Ribbon” on page 323
- “Configure Screen History Dialog Box” on page 324
- “Create New Web Session Document Dialog Box” on page 325

Open a Web Session
InfoConnect includes an integrated browser based on Microsoft Internet Explorer, allowing you to open a Web page in a tab in the InfoConnect workspace.

To create a Web session document

1. Open the Create New Document dialog box.
   The steps depend on your user interface mode (page 120).

   **User Interface Mode**
   - **Ribbon or Reflection Browser**
     From the Quick Access Toolbar, click the **New Document** button.

   - **TouchUx**
     Tap the Folder icon and then under **File**, select **New**.

2. From the **Create New Document** dialog box, select **Web**, and then click **Create**.

3. From the **Create New Web Session Document** dialog box, under **URL**, type the address of the Web page you want to open.
   It is not necessary to type "http:" before the address.

4. Click **OK**.

5. From the **Quick Access** toolbar, click the **Save** button.

The Web page specified will open within the workspace just like a terminal session document, except that the Ribbon will have only one tab. This Ribbon tab shows which application features work within Web pages (Clipboard and Macro), and includes a Navigation group with typical browser controls such as Back and Home buttons.

You can open the same Web page later by clicking the **Open** button on the **Quick Access** toolbar.
Using the Integrated Browser

One of the main benefits of having an integrated browser is the ability to incorporate Web pages into automated tasks. For example, you could create a macro that copies data from an address field in a customer database on the host, then paste that data into a roadmap Web site such as MapQuest.com, and then display a map to a customer site automatically.

Another key benefit it offers is the automated inclusion of Web sites in your daily workspace. By saving a Web page document with one or more session documents in a InfoConnect layout, you can instantly create a custom workspace to meet a particular business need. For more information, see the “Create or Modify a Layout” on page 43 topic.

The integrated browser in InfoConnect is based on Microsoft Internet Explorer, and many of its important features are only accessible through Internet Explorer settings; for example, Internet Explorer security and home page settings affect the InfoConnect browser.

Related Topics

- “Create New Web Session Document Dialog Box” on page 325
- “Open a Layout” on page 51
- “Create or Modify a Layout” on page 43
- “Creating and Using Macros” on page 871

Navigate the Ribbon

Index Term
Primary: sessions
Secondary: navigating between

Index Term
Primary: Ribbon
Secondary: navigating

Index Term
Primary: navigating
Secondary: Ribbon

The Ribbon contains tools that you use to complete tasks in the selected document. Tools are represented as button and menu controls, which light up when you select them or move the pointer over them. Related controls are organized into feature groups, such as Productivity and Screen History. Groups are located on tabs, which are organized by function, such as changing the document appearance.

The appearance of the Ribbon and the features available from it depend on the document type and changes you've made to the Ribbon for that document type.
To navigate the ribbon

- Do any of the following:

  **To** | **Do this**
  --- | ---
  View the entire Ribbon | Expand the workspace by dragging the lower-right corner.
  Show or hide the Ribbon | - Double-click any tab in the Ribbon. *(This method is temporary. The Ribbon is maximized when InfoConnect is reopened.)*
  | - Click **Full Screen** from the **Status bar**.
  | - Map a keyboard shortcut to show or hide the Ribbon with a keystroke. Sessions using the default 3270 or 5250 keyboard map already have this action mapped to CTRL+F1.
  | - On the Quick Access Toolbar menu, choose **Minimize the Ribbon**.
  View a description of a task | Place the pointer over the button.
  Open settings for a task | Click the launcher in the lower-right corner of a group.
  Go to the next session document or Web page | Press CTRL+TAB.
  Go to the previous session document or Web page | Press CTRL+SHIFT+TAB.
  Go to the next pane in the current session document | Press CTRL+1.
  Use your keyboard to interact with the Ribbon | Press ALT to display the KeyTips.

**NOTE:** You can change the interface appearance from the **Configure User Interface** dialog box. When using the Classic UI, only one document can be open in a workspace, and other features may not be available.

**Related Topics**

- “Use a Keyboard to Interact with InfoConnect” on page 61
- “Configure Workspace Defaults Dialog Box” on page 125
- “Configure Color Settings” on page 35
- “Customize the Ribbon” on page 74
- “Customize the Quick Access Toolbar” on page 42

**Search**

**Index Term**
- **Primary:** workspace
- **Secondary:** searching
InfoConnect features a **Search** box at the upper right corner of the workspace, in the Help frame, and in some settings dialog boxes.

**Workspace**

From the workspace, you can use the **Search** box to perform a search of the open documents and screen history in InfoConnect, and for content on your desktop and on the Web.

The following commands are available from the workspace **Search** menu:

- **Current Document Search**
  - Searches only the selected document. Text matches are highlighted in the session (on-screen).

- **All Documents Search**
  - Searches all open session or Web page documents.
  - Search results appear in a separate pane at the bottom of the workspace. Double-click an item to highlight it in the session (on-screen).
### Screen History Search
Searches the screen history of open terminal session documents. Search results appear in a separate pane at the bottom of the workspace. Double-click an item to highlight it in the session (onscreen).

### Windows Desktop Search
Searches files and folders — including the content of text files and Microsoft Office files — on the desktop, using the Windows Desktop engine. (In Windows XP, for this option to be available, Windows Desktop Search must be installed.) Search results appear in a separate pane at the bottom of the workspace. Double-click a file to open it in the associated application.

### Google Web Search
Searches the Internet using the Google search engine. Results appear in a new tab (Web page document) in the workspace.

### Bing Web Search
Searches the Internet using the Microsoft Windows Bing search engine. Results appear in a new tab (Web page document) in the workspace.

### Help Search
Searches the **InfoConnect** Help system.

### Help
You can search the product Help from the **Search** box in the Help frame, or from the **Search** tab in the help navigation pane. From the **Search** box in the Help frame, you can also search the Attachmate Support Site.

### Settings Dialog Boxes
You can use the **Search** box from a dialog box to look for a word or part of a word in the various **InfoConnect** settings dialog boxes. At the top of the dialog box, search results that match your text, together with a navigation path, are displayed in a separate pane. Double-click an item to navigate to and highlight it in the identified settings dialog box.

This search finds only terminal session settings that are included in primary dialog boxes (those that have a **Search** box in the upper right-hand corner). It does not search settings in secondary dialog boxes (which include those dialog boxes associated with printer sessions, FTP client sessions, or file transfer). If you cannot find the setting for which you are looking with the settings search, use the index, or search the Help. The Help topic for the dialog box includes instructions for finding it in the product.

In some instances, the dialog box search may find settings that are functionally equivalent to the term you typed in the **Search** box. For example, if you enter **DBCS** in the **Search** box, the results will include the check box for **Support double-byte character set**.

### Capture Screen History

<table>
<thead>
<tr>
<th>Index Term</th>
<th>Primary: snapshot</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Index Term</th>
<th>Primary: screen history</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secondary: capture</td>
<td></td>
</tr>
</tbody>
</table>
Screen History creates recordings of IBM 3270 and 5250 host screens as you navigate to them. VT screens can be recorded using manual capture. You can view and/or verify the information from those screens, and send multiple host screens to Microsoft Word, PowerPoint, and Outlook (Email Message and Note only), if they are installed on your computer.

**NOTE:** Only text areas of the host screen are included in the recorded image; host graphics images are not included.

To view past screens

1. **Open the Screen History task pane.**
   The steps depend on your **user interface mode** (page 120).

   **User Interface Mode** | **Steps**
   --- | ---
   Ribbon | On the **Session** ribbon, click the **Screen History** button.
   Reflection Browser | On the **Reflection** menu, choose **View** and then **Screen History**.
   TouchUx | Tap the Wrench icon and then under **View**, select **Screen History**.

2. **Click a screen thumbnail.**
   The screen snapshot appears in the main window.

The following commands are also available from the toolbar in the Screen History task pane:

**Click** | **To do this**
--- | ---
Save screen snapshot as a file (.RSHX). When you close your session, your screen history is not maintained unless you save it to a separate file. | Save the contents of the Screen History task pane as a file (.RSHX). When you close your session, your screen history is not maintained unless you save it to a separate file.
To reopen the file later, it must be saved in a trusted location. | To reopen the file later, it must be saved in a trusted location.
Copy the selected screen to the Clipboard as text or a bitmap image. | Open a previously saved Screen History file.
Open the Office Tools dialog box to send one or more host screens from your screen history to Microsoft Word, PowerPoint, or Outlook (Email Message and Note only), if they are installed on your computer. | Copy the selected screen to the Clipboard as text or a bitmap image.
Create a manual screen capture within the Screen History task pane. (This is helpful for when you want to capture any text you've entered before you leave the screen.) | Open the Office Tools dialog box to send one or more host screens from your screen history to Microsoft Word, PowerPoint, or Outlook (Email Message and Note only), if they are installed on your computer.
Return to the currently active host screen. | Create a manual screen capture within the Screen History task pane. (This is helpful for when you want to capture any text you've entered before you leave the screen.)
There are two reasons you might want to capture a screen manually: you disabled screen history recording in the **Configure Screen History** dialog box, but need to capture a screen; or you modified one or more unprotected fields in a screen, and want to capture the screen with the modifications.

**NOTE:** Only text areas of the host screen are included in the recorded image; host graphics images are not included.

### To capture a screen manually

- From the **Screen History** task pane, click the **Manual Capture** toolbar button.

  The current screen, including any data you have entered, is captured and included in your Screen History list.

**Related Topics**

- “**Configure Screen History Dialog Box**” on page 324
- “**Capture Screen History**” on page 320
Navigate Screen History From the Ribbon

You can navigate “Screen History” on page 889 one screen at a time in the main InfoConnect window directly from the Session ribbon without opening the Screen History gallery or task pane.

NOTE: Only text areas of the host screen are included in the recorded image; host graphics images are not included.

To navigate screen history

- Do one of the following:

  **On the Session ribbon, click**
  - The **Back** button
  - The **Forward** button
  - The **Live Screen** button

  **To navigate**
  - Among captured screens.
  - Forward one screen at a time (if you navigated back, away from the current live screen).
  - Directly back to the current, live screen.

Related Topics

- “Capture Screen History” on page 320
- “Capture Screens Manually” on page 322
- “Configure Screen History Dialog Box” on page 324
Configure Screen History Dialog Box

Getting there

1. Open the Document Settings dialog box. The steps depend on your user interface mode (page 120).

   **User Interface Mode**  
   Ribbon or **InfoConnect Browser**  
   TouchUx

   **Steps**  
   With a session open in **InfoConnect**, from the **Quick Access Toolbar**, click **.**
   Tap the Gear icon and then select **Document Settings**.

2. On the Settings dialog box, under **Productivity**, click **Configure Screen History**.

   Screen History creates recordings of IBM 3270 and 5250 host screens as you navigate to them. VT screens can be recorded using manual capture. You can view and/or verify the information from those screens, and send multiple host screens to Microsoft Word, PowerPoint, and Outlook (Email Message and Note only), if they are installed on your computer.

   **NOTE:** Only text areas of the host screen are included in the recorded image; host graphics images are not included.

Options

**Maximum screens to capture**  
Set the maximum number of screens to record and keep at any one time in the current session’s screen history.

**Manual capture only**  
Select this check box to disable automatic screen history recording. Because VT supports manual capture only, this check box is not displayed for VT sessions.

**Clear screen history when disconnected**  
When selected, the screen history is deleted when the session is disconnected for any reason. When cleared, the screen history is deleted when the session is closed.

   **NOTE:** If the screen history has been saved to a file, the screen history file is not affected.

Related Topics

- “Capture Screens Manually” on page 322
Create New Web Session Document Dialog Box

Index Term
Primary: Web
Secondary: Create New Web Session Document dialog box

Getting there

1. Open the Create New Document dialog box.
   The steps depend on your user interface mode (page 120).

   **User Interface Mode**  
   **Steps**
   Ribbon or InfoConnect Browser  
   From the Quick Access Toolbar, click the **New Document** button.
   TouchUx  
   Tap the Folder icon and then under **File**, select **New**.

2. From the Create New Document dialog box, select a Web session, then click **Create**.

**URL**  
Type the address of the Web page you want to open.
It is not necessary to type "http://" before the address.

Related Topics
- “Open a Web Session” on page 315
Secure Connections

InfoConnect provides a variety of features to ensure the security of your communications when you are connecting over an unsecured network.

In this Chapter

- “FIPS Mode” on page 327
- “Protecting Data and Information Privacy” on page 328
- “SSL/TLS Connections” on page 337
- “Secure Shell Connections” on page 347
- “Certificate Authentication (PKI)” on page 437
- “SOCKS or HTTP” on page 454
- “Kerberos Connections” on page 461
- “Security Properties Dialog Box” on page 511

FIPS Mode

When you run in FIPS mode, all connections are made using security protocols and algorithms that meet FIPS 140-2 standards. In this mode some standard connection options are not available.

The following security configurations are allowed in FIPS mode:

- SSL/TLS connections using 3DES (168-bit) or AES (128-bit) encryption and SHA-1 hash.
- Secure Shell connections using 3DES (168-bit) or AES (128, 192, or 256-bit) encryption and SHA-1 hash.
- Kerberos connections, for user authentication only, using 3DES encryption and SHA-1 hash.
To run **Reflection** in FIPS mode

1. Run the Group Policy editor using one of the following techniques:
   - Type the following at the command line:
     ```
     Gpedit.msc
     ```
   - In the **Active Directory Users and Computers** console, open the properties for an **Organizational Unit**, click the **Group Policy** tab, and edit or create a new policy object.

2. Install the Reflection template (**ReflectionPolicy.adm**) if you have not already done so.

   **NOTE:** For information about how to download and install the Reflection policy template, see Technical Note 2216 (http://support.attachmate.com/techdocs/2216.html).

3. Under **Local Computer Policy** > **User Configuration** > **Administrative Templates** > **Reflection Settings**, disable the setting **Allow non-FIPS mode**.

**What is FIPS 140-2?**

The United States Government's Federal Information Processing Standard (FIPS) 140-2 specifies security requirements for cryptographic modules. Cryptographic products are validated against a specific set of requirements and tested in 11 categories by independent, U.S. Government-certified testing laboratories. This validation is then submitted to the National Institute of Standards and Technology (NIST), which reviews the validation and issues a certificate. In addition, cryptographic algorithms may also be validated and certified based on other FIPS specifications. The list of validated products and the vendor's stated security policy (the definition of what the module has been certified to do) can be found at: http://csrc.nist.gov/groups/STM/cmvp/validation.htm.

**IMPORTANT:** If you are configuring Reflection to use FIPS mode, you should ensure that you are running a version that has met all FIPS 140-2 standards. Contact technical support for more information.

**Related Topics**

- “SSL/TLS Connections” on page 337
- “Secure Shell Connections” on page 347
- "Kerberos Connections" on page 461

**Protecting Data and Information Privacy**

**Index Term**

**Primary:** Trust Center

Use the Trust Center to protect your working environment from information theft, and your data from potential damage caused by opening documents from non-trusted sources.

From the Trust Center, you can protect your data using the following methods.

- Set up trusted locations, from which you can safely open (and store) documents.
- Set up Information Privacy to mask sensitive data (such as credit card numbers) with privacy filters.
- Set up API and macro security to control access to the Reflection API and control the execution of actions invoked by a macro or API call.
Add Trusted Locations

A trusted location is a directory that is designated as a secure source for opening files. By default, Reflection InfoConnect 2014 allows users to open documents only in directories specified as trusted locations in the Reflection settings. InfoConnect 2014 specifies three trusted locations in the workspace Application.settings file in the program directory.

When you add other locations, these locations are saved in the Application.settings file in the user data directory folder. If you add trusted locations, you will need to deploy this file.

To set up a trusted location

1. On a workstation on which you have installed Reflection, open the Attachmate Customization Tool from a desktop shortcut (if you set up a shortcut) or from a command line as follows:
   
   `<path_to_setup>\setup.exe /admin`

2. In the Select Customization dialog box, select Create a new Companion installer, and then click OK.

3. On the navigation pane, click Specify install locations.

4. Under Installation type, select Installs only for the user who installs it.

5. On the navigation pane, click Modify User Settings.

6. In the Make changes to user settings panel, under Application - Settings, select Reflection 2014 Workspace Settings and then click Define.

7. Under Trust Center, click Specify Trusted Locations and then click Add new location.

8. Under Path, browse to the location you want to add.

9. To trust all folders within the trusted location, click Subfolders.

10. Click OK to close the Reflection Workspace dialog box.

11. Save the companion file on your administrative installation point.

Custom settings are automatically saved in the Application.settings file. The companion installer file is automatically configured to deploy this file to

- [AppDataFolder]\Attachmate\Reflection\Workspace\data_folder (for a single user) or to
- [CommonAppDataFolder]\Attachmate\Reflection\Workspace\data_folder (for all users) where data_folder is specific to the version of Reflection. For example, for Reflection 2014 R1, this folder is R2014_R1.

Specify Trusted Locations Dialog Box

Index Term

Primary: trusted locations
Secondary: specifying

Getting there

1. Open Workspace Settings.

   The steps depend on your user interface mode (page 120).
2 Under **Trust Center**, click **Specify Trusted Locations**.

A trusted location is a directory that’s designated as a secure source for opening files. By default, **InfoConnect** allows you to open documents only in directories specified as trusted locations in the **InfoConnect** settings.

During installation **InfoConnect** specifies three trusted locations on your local hard disk. The paths for these trusted locations cannot be modified or deleted. However, you can add your own trusted locations to the list.

### Trusted Locations

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ribbon (Office 2007)</td>
<td>On the Reflection button , choose <strong>Reflection Workspace Settings</strong>.</td>
</tr>
<tr>
<td>Ribbon (Office 2010)</td>
<td>On the <strong>File</strong> menu, choose <strong>Reflection Workspace Settings</strong>.</td>
</tr>
<tr>
<td>InfoConnect Browser</td>
<td>On the <strong>InfoConnect</strong> menu, choose <strong>Settings</strong> and then <strong>Reflection Workspace Settings</strong>.</td>
</tr>
<tr>
<td>TouchUx</td>
<td>Tap the Gear icon and then select <strong>Reflection Workspace Settings</strong>.</td>
</tr>
</tbody>
</table>

Open files only from trusted locations (recommended) When selected, **InfoConnect** prompts you to save files to trusted locations.

**Path**
The complete path for the trusted location. You can change, edit, or delete any trusted locations you add.

**Subfolders**
Trust all folders located within the trusted location.

**Description**
When a path is selected, you can add text that will be associated with the trusted location.

**Add New Location**
Creates another box in the list for you to add the path for a new trusted location.

**Allow trusted locations on my network (not recommended)**
Select to add a network path to the list of trusted locations.

2 Under Trust Center, click Specify Trusted Locations.

### Set Up Information Privacy Dialog Box

- “Protecting Data and Information Privacy” on page 328
Getting there

1 Open Workspace Settings.
The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>InfoConnect Browser</td>
<td>On the InfoConnect menu, choose Settings and then Reflection Workspace Settings.</td>
</tr>
<tr>
<td>TouchUx</td>
<td>Tap the Gear icon and then select Reflection Workspace Settings.</td>
</tr>
</tbody>
</table>

2 Under Trust Center, click Set Up Information Privacy.
You can configure Information Privacy features to protect sensitive data so that it is not displayed on the screen or in productivity features, such as Screen History.

If you need to... | Do this...
----------------------------------|----------------------------------|
Redact certain patterns of data that are outside the realm of credit card formats (e.g., US Social Security numbers). | Set up Privacy Filter Redaction Rules and Privacy Filters. |
Redact credit card Primary Account Numbers (PANs) to meet “PCI DSS” on page 891 requirements. | Set up Primary Account Number (PAN) Redaction Rules and Primary Account Number (PAN) Detection Rules. |
Require secure connections (as may be required for PCI DSS compliance). | Set up PCI DSS Rules. |

NOTE

- You can use Privacy Filters together with Primary Account Number (PAN) detection. To improve performance, do not duplicate existing PAN patterns in privacy filters.
- Information Privacy settings do not apply to IBM host printer emulation.
- If redaction is enabled, HLLAPI functions are disabled to prevent access to unredacted data through HLLAPI.

For detailed explanations, instructions, and examples that show how to set up Information Privacy features, see Setting up Information Privacy at [http://support.attachmate.com/manuals/reflection2014.html](http://support.attachmate.com/manuals/reflection2014.html)

Privacy Filters Redaction Rules

Use privacy filters when you need to:

- Redact certain patterns of data that are outside the realm of credit card formats (for example, US Social Security numbers or proprietary sensitive account numbers).
- Redact Primary Account Numbers (PANs) that are outside of a 13-16 digit range. (PAN detection does not detect PANs that are outside of this range.)
The redaction rules specify how to redact sensitive data, based on the filters that you specify in Privacy Filters.

| Redact data when used outside the terminal | Redacts sensitive data so that it is not displayed in productivity features, such as Office Tools integration, Screen History, Recent Typing, and Auto Complete. This option also obscures data from the Print Screen and Cut/Copy/Paste commands. |
| Redact display data (IBM terminals only) | Redacts data on screens after you navigate out of the current field. |

Privacy Filters

Add

Opensthe Add Privacy Filter dialog box where you can define the filter.

Modify

Opens the Modify Privacy Filter dialog box where you can modify the regular or simple expression that defines the filter.

Delete

Deletes the selected filter.

Primary Account Number (PAN) Redaction Rules

You can set up redaction rules to redact PANs (credit card numbers) that appear in screen histories, the clipboard, and Microsoft Office applications. You can also choose to redact PAN data displayed on screens, either as the PAN is typed or after it is entered.

Enable Redaction

Redacts sensitive data, based on the rules that you specify in Primary Account Number (PAN) Detection Rules.

Portion of PAN to redact

Specifies how many digits of the PAN to redact.

Redact display data (IBM terminals only)

Redacts data after it is entered.

Redact data while typing (IBM terminals only)

Redacts data as it is typed.

Do not store typed PANs

Prevents PAN data from being saved in an external file or any component that saves screen data. This includes the data saved for the Screen History, Recent Typing, Auto Complete, Auto Expand, and Macro Recording features. It also includes data returned by the Reflection API CreditCardRecognized event.

Primary Account Number (PAN) Detection Rules

Custom Detection Rules

Add, modify, or delete the regular expressions used by the PAN Detection methods to detect PAN data.

Reflection PAN detection

InfoConnect PAN detection allows you to set up regular expressions to detect PAN data. Use this option when:

- You need to define custom card issuer patterns to detect, such as oil company or department store cards.
- PANs in your application appear in a non-contiguous format, such as multiple input fields of data arranged in a vertical table, or are entered using non-standard digit group separators.
NOTE: For more about how to use regular expressions to define rules or exceptions for PAN data, see Setting up Information Privacy at http://support.attachmate.com/manuals/reflection2014.html

Custom Exception Expressions

Use regular expressions to define additional exclusion patterns that prevent false positives or preserve data that you do not want to redact.

NOTE: By default InfoConnect does not redact digit patterns such as North American phone numbers containing area code information and optional country code, common short date/time formats (MM/DD/YYYY, YYYY/MM/DD, HH:MM:SS, HH:MM, etc), and US Social Security numbers.

Simple PAN detection

Simple PAN detection matches either a credit card number sequence (a 13-16 digit number) or preceding text (e.g., keywords like "Account") followed by a credit card number sequence. Use Simple PAN detection when:

- All credit card data in host applications are always displayed and entered as a single continuous string (e.g. 1211-1441-1311-1551).
- You need to redact account numbers only from: Visa, MasterCard, American Express, Discover, Diner's Club, Carte Blanche, Voyager, JCB, or enRoute. (If you need to detect other card issuers, use Reflection PAN detection or Privacy Filters.)
- All host application screens containing credit cards are very well defined, and credit card information is always "labeled" in predictable ways. (For instance, credit card numbers are always preceded by a label such as "Account: ").

Detect PANs based on 13-16 digit numbers with separators matches a credit card number sequence.

Detect PANs based on preceding text matches preceding text followed by a credit card number sequence. To use this option, you will need to add the preceding text (e.g., Account) to the Text Items box.

PCI DSS Rules

You can configure InfoConnect to require secure connections for all network connections or for only wireless connections. You can also choose to fire a InfoConnect API event when an unredacted PAN (or credit card number) is displayed.

Do not require secure host connections

Allow non-secure connections, such as Telnet. Select this option only when testing or when your sessions do not require PCI DSS compliance.

Require secure host connections on all networks

Allows only secure connections, regardless of the type of network. This applies to wired, wireless, and VPN connections.

Require secure host connections on wireless networks

Allows non-secure connections on wired networks but requires secure connections for wireless networks.

NOTE: VPN connections are not subject to the wireless restrictions. Because of VPN's inherent security, VPN connections are handled in the same way as wired connections. To secure VPN connections, choose the Require secure host connections on all networks option.
Add (or Modify) Privacy Filter Dialog Box

Getting there

1 Open Workspace Settings.
   The steps depend on your user interface mode (page 120).

   **User Interface Mode** | **Steps**
   --- | ---
   InfoConnect Browser | On the InfoConnect menu, choose Settings and then Reflection Workspace Settings.
   TouchUx | Tap the Gear icon and then select Reflection Workspace Settings.

2 Under Trust Center, click Set Up Information Privacy.
3 Under Privacy Filters, click Add or Modify.

**Description** | Enter the name of the filter. This is displayed under Privacy Filters in the Set Up Information Privacy dialog box.

**Regular expression** | Enter (or modify) the regular expression that defines the filter.

**Simple expression** | Enter (or modify) the simple expression that defines the filter. For example, the following filter redacts US Social Security numbers:

###-##-####

**NOTE:** For more about how to use regular expressions to define privacy filters, ask customer support (http://www.attachmate.com/Support/) for a copy of Setting up Information Privacy.

Add (or Modify) Custom Detection Rule or Exception Dialog Box

Getting there

1 Open Workspace Settings.

Enable API events when PANs are viewed by the user

Fires the CreditCardRecognized .NET API and VBA event when unredacted PAN data is copied from the terminal to the clipboard or to a productivity tool. For IBM systems, the event is also fired when unredacted PAN data is displayed on the screen.

You can handle this event to create logs or perform other actions required for compliance. (See the InfoConnect VBA Guide or the InfoConnect .NET API Guide.)

**NOTE:** This event is fired only when a PAN is copied or displayed in its entirety (“in the clear”). It is not fired when only redacted PANs are copied or displayed.
The steps depend on your user interface mode (page 120).

**User Interface Mode**  
<table>
<thead>
<tr>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ribbon (Office 2007)</strong></td>
</tr>
<tr>
<td><strong>Ribbon (Office 2010)</strong></td>
</tr>
<tr>
<td><strong>InfoConnect Browser</strong></td>
</tr>
<tr>
<td><strong>TouchUx</strong></td>
</tr>
</tbody>
</table>

2. Under **Trust Center**, click **Set Up Information Privacy**.
3. Under **Reflection PAN detection**, next to either **Custom Detection Rules** or **Custom Exception Expressions**, click **Add** or **Modify**.

**Description**  
Enter the name of the rule or exception. This is displayed under **Reflection PAN detection** in the Set up Information Privacy dialog box.

**Regular expression**  
Enter (or modify) the regular expression that defines the custom rule or exception.

*NOTE:* For more about how to use regular expressions to define rules or exceptions for PAN data, see Setting up Information Privacy at http://support.attachmate.com/manuals/reflection2014.html

### Set Up API and Macro Security Dialog Box

**Index Term**  
Primary: security  
Secondary: API

**Index Term**  
Primary: permissions for API calls

**Index Term**  
Primary: legacy  
Secondary: API preference

**Index Term**  
Primary: GetObject()  
Secondary: COM objects

**Index Term**  
Primary: API  
Secondary: access settings

**Index Term**  
Primary: API  
Secondary: security

**Index Term**  
Primary: API  
Secondary: preference for legacy APIs
Index Term
Primary: API
Secondary: port

Index Term
Primary: API
Secondary: COM objects

Getting there

1 Open Workspace Settings.
   The steps depend on your user interface mode (page 120).

   **User Interface Mode** | **Steps**
   --- | ---
   InfoConnect Browser | On the InfoConnect menu, choose Settings and then Reflection Workspace Settings.
   TouchUx | Tap the Gear icon and then select Reflection Workspace Settings.

2 Under Trust Center, click Set Up API and Macro Security.

From this dialog box, you can enable the InfoConnect .NET API, and specify corresponding settings.

**NOTE:** If you need to use the API in multiple instances of InfoConnect simultaneously, use layouts.
You can specify different settings for the IPC channel name for each layout in the Layout Settings dialog box.

### API Settings*

**Disable API**
Select to prevent custom applications from accessing this installation of InfoConnect.

**Legacy API preference**
Use this setting to determine if InfoConnect legacy macros are supported, and to determine which legacy API has preference for the GetObject() method used to retrieve API COM objects. InfoConnect supports multiple APIs, but can accept GetObject() calls for only one type of legacy API object at a time.

**Select** | **If you**
--- | ---
No Legacy API | Don't use legacy InfoConnect macros, or if your code doesn't use GetObject() to access legacy API COM objects.
Reflexion

Use legacy InfoConnect macros, or if you use GetObject() to access legacy InfoConnect API COM objects. Each session document that you subsequently open or create has legacy macro capability; it includes a legacy VBA project in addition to the standard VBA project in the Visual Basic Editor.

**NOTE:** Legacy API support is provided in all InfoConnect settings files that you open in the workspace (including settings files saved as InfoConnect session documents), regardless of this setting.

**EXTRA!**

Use GetObject() to access legacy EXTRA! API COM objects.

**Action Permissions**

Specify what you want to happen if an action that has been restricted through Group Policy or the Permissions Manager is initiated through a macro or API call.

**Require elevated rights; do not execute on XP**

On a computer running Windows Vista, select to control restricted actions with User Account Control (UAC).

-or-

On a computer running Windows XP, select to prevent restricted actions from running.

**Execute the action**

Select to run restricted actions that are initiated through a macro or API call as expected. The same actions won't run if they are initiated through the user interface.

**Related Topics**

- “Layout Settings Dialog Box” on page 72
- “Using Layouts” on page 72
- “Protecting Data and Information Privacy” on page 328

**SSL/TLS Connections**

**In this Section**

- “SSL/TLS Overview” on page 337
- “Connect Using SSL/TLS” on page 339
- “Digital Certificates in SSL/TLS Sessions” on page 341
- “Troubleshooting SSL/TLS Error Messages” on page 342

**SSL/TLS Overview**

Index Term

Primary: SSL/TLS
Secondary: SSL/TLS overview
The Secure Sockets Layer protocol (SSL) and its compatible successor, the Transport Layer Security protocol (TLS), enable a client and server to establish a secure, encrypted connection over a public network. When you connect using SSL/TLS, the client authenticates the server before making a connection, and all data passed between InfoConnect and the server is encrypted. Depending on the server configuration, the server may also authenticate the client.

Authentication is accomplished by sending an X.509 security certificate. Authentication occurs automatically and invisibly as the first step of establishing an SSL/TLS connection. SSL/TLS connections require the client to authenticate the server. It is optional for the server to authenticate the client.

Once an encrypted connection is established, data is transmitted using the encryption level you have specified in the Reflection Security Properties dialog box.

**Supported Cryptographic Algorithms**

Reflection supports TLS version 1.2, TLS version 1.0 (the default) and SSL version 3.0. The supported cipher suites are listed below.

**NOTE:** The list of cipher suites available for a given connection depends on the SSL/TLS version you specify, the encryption strength setting, and whether or not you are configured to run in FIPS mode.

- TLS_SRP_SHA_DSS_WITH_AES_256_CBC_SHA (0xc022)
- TLS_SRP_SHA_RSA_WITH_AES_256_CBC_SHA (0xc021)
- TLS_DHE_DSS_WITH_AES_256_GCM_SHA384 (0x00a3)
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x009f)
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x006b)
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA256 (0x006a)
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA (0x0038)
- TLS_SRP_SHA_WITH_AES_256_CBC_SHA (0xc020)
- TLS_DH_anon_WITH_AES_256_GCM_SHA384 (0x00a7)
- TLS_DH_anon_WITH_AES_256_CBC_SHA256 (0x006d)
- TLS_DH_anon_WITH_AES_256_CBC_SHA (0x003a)
- TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
- TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- TLS_SRP_SHA_DSS_WITH_3DES_EDE_CBC_SHA (0xc01c)
- TLS_SRP_SHA_RSA_WITH_3DES_EDE_CBC_SHA (0xc01b)
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x001b)
- TLS_SRP_SHA_WITH_3DES_EDE_CBC_SHA (0xc01a)
- TLS_DH_anon_WITH_3DES_EDE_CBC_SHA (0x000a)
- TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x0009)
- TLS_SRP_SHA_DSS_WITH_AES_128_GCM_SHA256 (0x00a2)
- TLS_SRP_SHA_RSA_WITH_AES_128_GCM_SHA256 (0x009e)
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x000e)
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x0067)
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA256 (0x0069)
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
The Secure Sockets Layer protocol (SSL) and its compatible successor, the Transport Layer Security protocol (TLS), enable a client and server to establish a secure, encrypted connection over a public network. When you connect using SSL/TLS, the client authenticates the server before making a connection, and all data passed between InfoConnect and the server is encrypted. Depending on the server configuration, the server may also authenticate the client.

InfoConnect 2014 supports SSL/TLS connections for IBM 3270, IBM 5250, and VT terminals.

NOTE: SSL/TLS connections use digital certificates for authentication. Depending on how your certificate was issued and the way your host is configured, you may need to install a host and/or personal certificate before you can connect using SSL/TLS.

Before you start

Make sure your system has an SSL/TLS host (server or servers) and that you know how certificates are handled for your server (see “SSL/TLS Connections” on page 337).

The following instructions show how to configure a connection for a host that requires server authentication (but not client authentication) and uses a certificate from a trusted certification authority (CA).
This procedure shows how to import the certificate into the Reflection certificate store. To set up this connection, you need:

- The SSL/TLS host name.
- A user name and password.
- The port used by the SSL/TLS server.
- Access to a CA certificate for the server.

**To configure a secure terminal session using SSL/TLS**

1. **Open the Create New Document dialog box.** The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ribbon or Reflection Browser</td>
<td>From the Quick Access Toolbar, click the New Document button.</td>
</tr>
<tr>
<td>TouchUx</td>
<td>Tap the Folder icon and then under File, select New.</td>
</tr>
</tbody>
</table>

2. From the Create New Document dialog box, select a session template and click Create.

3. For **Host Name/IP Address**, enter the fully qualified host name.

   **NOTE:** By default, the host name you enter must exactly match one of the host names entered in either the CommonName or the SubjectAltName field of the host's certificate. The setting Certificate host name must match host being contacted is configured from the PKI Configuration (page 523) dialog box. Leave this setting selected for maximum security.

4. In the Port box, set the port your host uses for SSL/TLS connections. In most cases you will have to change the default port value. Contact the host system administrator for this information. (For connections to an AS/400, the SSL/TLS port will typically be 992.)

5. Select **Configure additional settings**, and then click OK.

6. Do one of the following:

   - If you are setting up a 3270 and 5250 terminal session, under Host Connection, click Set Up Connection Security. Then, in the Configure Advanced Connection Settings dialog box, click Security Settings.
   - If you are setting up a VT terminal session, click Configure Connection Settings, confirm Network Connection Type is set to Telnet, and click the Back arrow button. Then, under Host Connection, click Set Up Connection Security.

7. From the Security Properties dialog box, select the SSL/TLS tab, and select Use SSL/TLS security.

8. (Optional) To specify the minimum allowable level of encryption for SSL/TLS connections, select a level in the Encryption strength list. The connection fails if this level cannot be provided.

   **NOTE:** If you select Default, any encryption level is permitted, and InfoConnect negotiates with the host system to choose the strongest encryption level supported by both the host and the PC.

9. (Optional) Click Configure PKI.
The PKI Configuration dialog box opens, from which you can manage the digital certificates used for authentication.

1. Click **Reflection Certificate Manager**.
2. In the Reflection Certificate Manager dialog box, select the **Trusted Certificate Authorities** tab.
3. Click **Import** and browse to select the CA certificate for the server.
4. Modify default settings as required. (For example, to use only the InfoConnect store, you might choose to clear **Use System Certificate Store for SSL/TLS connections**. When this option is selected, InfoConnect looks for certificates in both the InfoConnect store and the Windows certificate store.)

When you customize any of the default PKI settings, the pki_config file is created.

5. Close the Certificate Manager dialog box and click **OK** to close the other open dialog boxes.

The imported certificate is saved in the trust_store.p12 file.

6. After a connection is established, click the Save button on the Quick Access toolbar and save the session document.

7. Click **OK** to close the open dialog boxes and return to the workspace.

![](Note: A padlock icon appears on the status bar when you have configured a secure connection. After you have established a secure connection, double-clicking this icon opens the host certificate.

**Related Topics**

- “SSL/TLS Overview” on page 337
- “Digital Certificates in SSL/TLS Sessions” on page 341
- “Troubleshooting SSL/TLS Error Messages” on page 342
- “SSL/TLS Tab (Security Properties Dialog Box)” on page 518
- “FIPS Mode” on page 327
- “Configure SSL/TLS (FTP Client)” on page 760

**Digital Certificates in SSL/TLS Sessions**

**Index Term**

Primary: PKI
Secondary: SSL/TLS configuration

Before making an SSL/TLS connection, Reflection must authenticate (page 887) the host (server). In addition, some servers may also require the user (client) to present a certificate for user authentication. When Reflection is configured to use SSL/TLS security, authentication is handled with digital certificates. These certificates are part of the same Public Key Infrastructure (PKI) (page 438) that is used to secure internet transactions.

Your computer must be configured to recognize the digital certificate presented by your host and, if necessary, to provide a certificate for client authentication. If your computer is not properly configured, or if the certificates presented for authentication are not valid, you will not be able to make SSL/TLS connections.
Depending on how your digital certificates are issued, you may need to install certificates on your computer before you can connect using SSL/TLS security.

- If your host certificates were acquired from a well-known certification authority (CA), such as VeriSign or Thawte, and you have configured Reflection to support host authentication using the Windows system certificate store (page 439), you do not need to install any host certificates on your computer. A certificate identifying the issuer as a trusted CA should already be included in the Trusted Root Certification Authorities list on your system.

- If you have configured Reflection to require authentication using the Reflection store (page 439), each client computer must import required CA certificate(s) into the “Reflection Certificate Manager” on page 446.

- If your enterprise has created its own certification authority, each client computer must import the root certificate for your CA. Depending on your configuration, import it into either the Windows (page 447) or Reflection (page 446) certificate store.

- If the host creates its own self-signed certificates, each client computer must install any needed certificates. Depending on your configuration, import them into either the Windows or Reflection certificate store.

- If the host requires a client certificate for user authentication, you need to import the personal certificate. You can use either the Reflection or the Windows personal certificate store.

NOTE: By default, Certificate host name must match host being contacted is enabled in the PKI Configuration (page 523) dialog box. When this setting is enabled, the host name you configure in Reflection must exactly match one of the host names entered in the either the CommonName or the SubjectAltName fields of the certificate. If you are using a hosts file, check to be sure that the name in your hosts file exactly matches the name in the certificate.

Troubleshooting SSL/TLS Error Messages

Index Term
Primary: troubleshooting SSL/TLS errors

Index Term
Primary: SSL/TLS
Secondary: troubleshooting SSL/TLS errors

Index Term
Primary: error messages
Secondary: troubleshooting SSL/TLS errors

These messages apply to all SSL/TLS connections.

Reflection SSL/TLS could not establish an encrypted connection to the Reflection security proxy. Invalid authorization token

The authorization token generated by the Reflection for the Web management server, and required by the Reflection security proxy, was received by the proxy but either was not valid or has expired.

Possible causes

- You are attempting to reconnect your Windows-based Reflection session after your authorization token has expired.

- You are attempting to initiate a Reflection session from a settings file on your local disk instead of clicking on the web page link, and your authorization token has expired.

The proxy server does not trust the Reflection for the Web management server's security certificate.
Troubleshooting steps

1. Always start and reconnect your sessions by clicking on the Reflection for the Web link for the host and session you want.
2. Reload and/or reauthenticate to the Reflection for the Web links list page for your valid sessions.
3. Contact your Reflection for the Web system administrator for additional troubleshooting assistance.

Reflection SSL/TLS could not establish an encrypted connection to the Reflection security proxy. Missing authorization token

The authorization token generated by the Reflection for the Web management server, and required by the Reflection security proxy, was not received by the proxy.

Possible causes

- You are attempting to initiate a Reflection session from a settings file on your local disk instead of clicking on the web page link.

The Reflection for the Web management server does not have a security certificate installed.

Troubleshooting steps

1. Always start and reconnect your sessions by clicking on the Reflection for the Web link for the host and session you want.
2. Reload and/or reauthenticate to the Reflection for the Web links list page for your valid sessions.
3. Contact your Reflection for the Web system administrator for additional troubleshooting assistance.

Reflection SSL/TLS could not establish an encrypted connection

The SSL/TLS handshake failed.

Cause(s)

1. If encryption strength was explicitly set, the server may not have accepted the requested encryption strength.
2. The server does not support SSL/TLS connections.
3. You are trying to connect using the wrong host port.
4. The server is not accepting connections or is down.
5. Your server does not support the SSL/TLS version running on your Windows operating system.

Your client is running in FIPS mode and this connection does not meet FIPS requirements. Troubleshooting steps

1. Select a different value for Encryption Strength, or set this to Default and try again. Check with your server’s system administrator to determine the type(s) of encryption supported by the server.
2. Check with your system administrator to determine that the server is functioning properly. Disable SSL/TLS encryption in the Security Properties dialog box if you want to make an insecure connection.
3. Check the port you are using to make your connections. Reflection defaults to port 23 for Telnet connections and 1570 for VT-MGR connections. In most cases, you will need to change this value for SSL/TLS connections. Check with your system administrator to find out what port value to use for your host.
4 Check with the system administrator for system status or try connecting later.

5 Configure Reflection to connect without sending a version-specific handshake.

6 Check to see if the server’s certificate is unsupported in FIPS mode. The server certificate key size must meet FIPS standards for protecting the shared secret key that will be exchanged and used for encrypting the session. The host certificate key length requirements are:

<table>
<thead>
<tr>
<th>Shared Key</th>
<th>Host Certificate Key Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>3DES (168-bit, but effectively 112-bit)</td>
<td>RSA or DSA key with a minimum size of 1024 bits</td>
</tr>
<tr>
<td>AES (128-bit)</td>
<td>RSA or DSA key with a minimum size of 3072 bits</td>
</tr>
</tbody>
</table>

**Reflection SSL/TLS could not find user credentials**

The SSL/TLS client failed to find user credentials. The host you are connecting to requires that you authenticate using your personal certificate, but no personal certificate was found.

**Troubleshooting steps**

1. If you do not have a client certificate contact your system administrator to provide you with one.
2. If you have a client certificate containing both a public and private key, you must install it to the Personal store of either the Windows Certificate store or the Reflection Certificate store.

**Reflection SSL/TLS timed out while trying to establish an encrypted connection**

The SSL/TLS handshake did not complete within the specified timeout period.

**Cause(s)**

1. Network load or slow connections did not allow the SSL/TLS handshake to complete within the timeout period. Because the SSL/TLS timeout period is comparable to the TCP/IP timeout, it is unlikely that you will encounter an SSL/TLS timeout problem without also encountering a timeout making your telnet connection.
2. Server or network is down.
3. Your server does not support the SSL/TLS version running on your Windows operating system.

**Troubleshooting steps**

1. It is not possible to reset the SSL/TLS timeout period.
2. Check with server or network administrator for status, or try connecting later.
3. Configure Reflection to connect without sending a version-specific handshake.

**Session disconnected due to corrupted message digest**

The session has been disconnected due to a corrupted message digest. The message digest is a mechanism that is used to detect whether the content of a message was changed while in transit from host to client.

**Cause(s)**

1. The message digest was corrupted due to a “dirty” network connection.
2. The message digest was corrupted due to an attempted hacker attack.
Troubleshooting steps

- Reestablish the network connection. Contact a network administrator if you see this error repeatedly, as it could indicate hacker activity or bad network hardware somewhere between the client and server.

The host's SSL/TLS certificate is not from a trusted Certificate Authority or has expired

The certificate presented by the server was invalid or was not issued by a certification authority (CA) trusted by this user.

Cause(s)

1. The host's server certificate is not in your Trusted Root Certification Authorities list. If you have enabled use of the Windows certificate store, you can determine which trusted certification authorities are configured for your PC using the Certificate Manager. To launch this utility, open the Windows Control Panel, double-click Internet Options, select the Content tab, then click Certificates.

2. If you have disabled use of the Windows certificate store, you may see this message if you have not yet imported certificates into the Reflection certificate store. Use the Trusted Certification Authorities tab of the Reflection Certificate Manager to manage your list of trusted CAs.

3. The host's server certificate has expired.

4. Certificate revocation checking is not returning a valid response. This message is displayed if the certificate is no longer valid. If the certificate is valid, you may see this message if Reflection is not able to reach the OCSP responder or retrieve the CRL file.

Troubleshooting steps

1. Add the certification authority to the Trusted Certificate Authority list to either the Reflection or the Windows certificate store.

2. Add the certification authority to the Trusted Certificate Authority list to the Reflection certificate store.

3. Notify the host's system administrator to acquire a new certificate.

The host name in the SSL/TLS certificate does not match the name of the host being contacted

The certificate presented by the server does not contain a host name that exactly matches the host name that you (or your definitive local security provider, such as DNS) specified as the connection target.

Before making an SSL/TLS connection, Reflection authenticates the host system. The certificate presented by the host for this purpose must be from a trusted certificate authority. If your PC does not recognize the certificate authority, you will not be able to make SSL/TLS connections.

Cause(s)

The host name you configure in Reflection must exactly match one of the host names entered in the CommonName field of the certificate.

Troubleshooting steps

If you entered an IP address instead of a host name, try entering the host name, then reconnect.

If you entered an aliased hostname (for example, "myhost"), try entering the fully qualified host name (for example, "myhost.domain.com") and then reconnect. If you are contacting a host in another domain, you must use the fully qualified host name, rather than the shortened alias name.
Contact your system administrator to determine if your certificate should include the host name. If no host name is required, open the SSL/TLS tab of the Security Properties (page 511) dialog box, click Configure PKI, and clear Certificate host name must match host being contacted. Do not make this change without consulting a system administrator. If you clear this setting when host names are used, you will reduce the level of security of your connections.

These messages apply only to connections configured to use the Windows Crypto API.

**Reflection SSL/TLS encryption strength requested not available on this PC**

You have specified a higher level of encryption algorithm strength (or are using a settings file that specifies a higher strength) than is available on your system. This will usually occur in multi-national environments, where the system administrator has specified U.S. encryption strengths, but the end user's international operating system only has export level encryption.

**Troubleshooting steps**

- Select a lower level of encryption strength or accept the default strength.

**Reflection SSL/TLS library (RSCAPI.DLL) missing or damaged**

Rscapi.dll failed to load.

**Cause(s)**

Rscapi.dll is corrupted or missing.

**Troubleshooting steps**

1. Use the Microsoft Windows Installer to repair the damaged file. Use Add/Remove programs to repair your Reflection installation.

**Required Microsoft SSL/TLS cryptographic libraries missing or damaged**

This system is missing one or more dynamic link libraries (DLLs) required for the Microsoft Cryptographic API Provider.

**Cause(s)**

1. Your system has corrupted versions of one or more of the Microsoft cryptographic libraries. Someone may have tampered with these files, or they may be corrupted for unknown reasons.

2. Your system does not have some or all of the required libraries. You may be using an operating system (such as Windows 95/98) which does not support access to the cryptographic libraries.

**Troubleshooting steps**

1. Reinstall Internet Explorer and/or your operating system to correct this problem.

2. Upgrade the operating system.

**Required Microsoft SSL/TLS library (SECURITY.DLL) missing or damaged**

This machine is missing the Microsoft file Security.dll.

**Cause(s)**

1. Your system has corrupted versions of the Microsoft SSPI library. Someone may have tampered with this files, or it may be corrupted for unknown reasons.

2. Your system does not have the required Microsoft provided SSPI library. You may be using an operating system (such as Windows 95/98) which does not support access to the cryptographic libraries.
Troubleshooting steps

1. Reinstall Internet Explorer and/or your operating system to correct this problem.
2. Upgrade the operating system.

Required Microsoft SSPI library is missing or damaged

This machine is missing dynamic link libraries (DLLs) required for the Microsoft Security Service Provider Interface (SSPI).

Cause

Your system does not have the required Microsoft DLLs for access to SSPI. This indicates serious damage to one or more of your operating system files.

Troubleshooting steps

You may need to reinstall the operating system.

Secure Shell Connections

In this Section

- “Secure Shell Overview” on page 347
- “Connect using Secure Shell (SSH)” on page 349
- “Configure Secure Shell Settings” on page 351
- “Understanding Secure Shell” on page 352
- “Reflection Secure Shell Settings Dialog Box” on page 353
- “Authentication” on page 359
- “Public Key Authentication” on page 363
- “Certificate Authentication in Secure Shell Sessions” on page 385
- “GSSAPI (Kerberos) Authentication for Secure Shell Sessions” on page 387
- “Port Forwarding” on page 391
- “Secure Shell Configuration Files” on page 402
- “Command Line Utilities” on page 423
- “Troubleshooting Secure Shell” on page 435

Secure Shell Overview

Index Term
Primary: Secure Shell
Secondary: overview

Index Term
Primary: encryption
Secondary: Secure Shell (SSH) encryption standards
You can configure Secure Shell connections when you need secure, encrypted communications between a trusted host and your PC over an insecure network. Secure Shell connections ensure that both the client user and the host computer are authenticated; and that all data is encrypted. Passwords are never sent over the network in a clear text format as they are when you use Telnet, FTP, or rlogin.

Reflection supports the following cryptographic algorithms

**Data Encryption Standards**

Encryption protects the confidentiality of data in transit. This protection is accomplished by encrypting the data before it is sent using a secret key and cipher. The received data must be decrypted using the same key and cipher. The cipher used for a given session is the cipher highest in the client's order of preference that is also supported by the server. You can use the Encryption (page 357) tab of the Reflection Secure Shell Settings dialog box to specify which ciphers the Secure Shell connection should use.

Attachmate Reflection 2014 supports the following data encryption standards:

- DES (56-bit) - Available with SSH protocol 1 only
- Arcfour, Arcfour128, and Arcfour258 (stream mode)
- TripleDES (168-bit) CBC mode
- Cast (128-bit)
- Blowfish (128-bit) CBC mode
- AES (also known as Rijndael) (128-, 192-, or 256-bit) CBC mode and CTR mode

**Data Integrity**

Data integrity ensures that data is not altered in transit. Secure Shell connections use MACs (message authentication codes) to ensure data integrity. The client and server independently compute a hash for each packet of transferred data. If the message has changed in transit, the hash values are different and the packet is rejected. The MAC used for a given session is the MAC highest in the client's order of preference that is also supported by the server. Reflection supports the following MAC standards:

- hmac-sha1
- hmac-md5
- hmac-sha1-96
- hmac-md5-96
- hmac-ripemd-160
- hmac-sha256
- hmac-sha2-256
- hmac-sha512
- hmac-sha2-512

**Digital Signatures**

Digital signatures are used for public key authentication (including certificate authentication). The authenticating party uses the digital signature to confirm that the party being authenticated holds the correct private key. The Secure Shell client uses a digital signature to authenticate the host. The Secure Shell server uses a digital signature to authenticate the client when public key authentication is configured. Reflection supports the following digital signature algorithms:

- x509v3-rsa2048-sha256
You can configure Secure Shell connections when you need secure, encrypted communications between a trusted host and your PC over an insecure network. Secure Shell connections ensure that both the client user and the host computer are authenticated; and that all data is encrypted. Passwords are never sent over the network in a clear text format as they are when you use Telnet, FTP, or rlogin. You can use this procedure to connect securely to UNIX and Linux hosts.

**NOTE:** Secure Shell connections are available for VT terminal sessions.

**Before you start**

By default, Secure Shell connections use public key authentication for the host and username/password authentication for the user. To configure a connection using these defaults, you need to make sure your system has a Secure Shell server or servers and that you know the following information:

- The host name.
- The User name and password.
- The port used by the Secure Shell server (the default is 22).

**To configure a secure terminal session using Secure Shell (SSH)**

1. Open the Create New Document dialog box.
   
   The steps depend on your user interface mode (page 120).
2 From the **Create New Document** dialog box, select the **VT Terminal** template and click **Create**.

3 In the **Create New** dialog box, under **Connection**:
   - Select **Secure Shell**.
     The Port value changes to 22, which is the standard port for Secure Shell connections. If you need to connect to a different port, select **Configure additional settings**, or use the procedure below to change the default Secure Shell settings.
   - (Optional) Enter the **Host name/IP address**. If you omit this, you will be prompted for a host name when you connect.
   - (Optional) Enter your **User name**. If you omit this, you will be prompted for a host name when you connect.

4 Click **OK**.

5 The first time you connect, you are prompted to verify the host key authenticity. Verify the host key fingerprint and select **Always**.

   **NOTE:** Host authentication (performed with public key authentication) enables the Secure Shell client to reliably confirm the identity of the Secure Shell server. If the host public key is not installed on the client, the host fingerprint is displayed and users are prompted to contact the system administrator to verify the fingerprint. This confirmation prevents risk of a "man-in-the-middle" attack, in which another server poses as the host. After the host key is added to the client, **Attachmate InfoConnect 2014** can authenticate the server without requiring user confirmation, and the unknown host prompt does not appear again. The key is saved in a file called **known_hosts**, which is created in the folder `personal_documents_folder\Attachmate\Reflection\.ssh`.

6 When prompted, enter your password.

7 Click the **Save** button on the **Quick Access** toolbar and save the session document.
   The file is saved in `[PersonalFolder]\Attachmate\Reflection`.

**To configure username and password prompts to appear in the terminal window**

1 Open a session that you have configured to use Secure Shell. Disconnect if you are connected.

2 **Open the Document Settings dialog box.**
   The steps depend on your **user interface mode** (page 120): 
   
<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ribbon or Reflection Browser</td>
<td>With a session open in Reflection, from the <strong>Quick Access Toolbar</strong>, click <img src="image" alt="Document Settings" /></td>
</tr>
<tr>
<td>TouchUx</td>
<td>Tap the Gear icon and then select <img src="image" alt="Document Settings" /></td>
</tr>
</tbody>
</table>
3 Under **Host Connection**, click **Configure Connection Settings**.

4 Under **Connection Options**, select **Handle SSH user authentication in terminal window**.

**To configure non-default Secure Shell settings**

1 Open a session that you have configured to use Secure Shell. Disconnect if you are connected.

2 Open the **Document Settings** dialog box.

   The steps depend on your **user interface mode** (page 120).

   **User Interface Mode** | **Steps**
   --- | ---
   Ribbon or Reflection Browser | With a session open in Reflection, from the **Quick Access Toolbar**, click ![Reflection icon].
   TouchUx | Tap the **Gear icon** and then select ![Document Settings].

3 Under **Host Connection**, click **Set up Connection Security**.

4 In the **Reflection Secure Shell Settings** dialog box, configure any non-default settings and then click **OK**.

**NOTE**

- When you click OK, changes to the default settings are saved in the Secure Shell **config** file in `[PersonalFolder]\Attachmate\Reflection\.ssh`

- If you want to deploy the session to all users of a computer, first rename the **config** file to `ssh_config` and the **known_hosts** file to `ssh_known_hosts`.

**Related Topics**

- “Configure Secure Shell Settings” on page 351
- “Connect Using Secure Shell (FTP Client)” on page 756
- “Managing Host Keys” on page 371

**Configure Secure Shell Settings**

**Index Term**

Primary: SSH
Secondary: configure Secure Shell settings

**Index Term**

Primary: Secure Shell
Secondary: configure Secure Shell settings

In most cases **Reflection** will connect to your host and allow you to log in with your password using the default Secure Shell configuration. Use the **Reflection Secure Shell Settings** dialog box if you need to configure alternate user authentication methods or to make other changes to your Secure Shell configuration.

**To modify the Secure Shell settings for a terminal session**

1 Open the terminal session you want to modify.

2 Disconnect from the host.
3 Open the Document Settings dialog box.
   The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ribbon or Reflection Browser</td>
<td>With a session open in Reflection, from the Quick Access Toolbar, click.</td>
</tr>
<tr>
<td>TouchUX</td>
<td>Tap the Gear icon and then select Document Settings.</td>
</tr>
</tbody>
</table>

4 Click Configure Connection Settings.

5 Under Network Connection Type, select Secure Shell.

6 Under Connection Options, enter a host name.

7 (Optional) Specify a value for SSH configuration scheme.
   If you leave this blank, changes you make to your Secure Shell settings are saved to Secure Shell configuration file under the current host name, and the settings you configure are applied by default to all Secure Shell connections to this host. If you specify a scheme name, changes you make to your Secure Shell settings are saved to the Secure Shell configuration file under the specified scheme name, and the settings you configure are applied to subsequent connections whenever you specify this scheme name.

8 Click Security.

9 Use the Reflection Secure Shell Settings dialog box to configure your settings, then click OK.

   **NOTE:** Changes you make to the default values are saved to the Secure Shell configuration file when you click OK.

Related Topics

- “Connect using Secure Shell (SSH)” on page 349
- “Secure Shell Configuration Files” on page 402

**Understanding Secure Shell**

Index Term

Primary: SSH
Secondary: understanding Secure Shell

Index Term

Primary: Secure Shell
Secondary: understanding Secure Shell

This diagram outlines the basic steps involved in creating a Secure Shell channel and using it to transmit data securely.
1 Establish a secure connection.
The client and server negotiate to establish a shared key and cipher to use for session encryption, and a hash to use for data integrity checking.

2 Authenticate the server.
Server authentication enables the client to confirm the identity of the server. The server has only one chance to authenticate to the client during the authentication process. If this authentication fails, the connection fails.

3 Authenticate the client.
Client authentication enables the server to confirm the identity of the client user. By default, the client is allowed multiple authentication attempts. The server and client negotiate to agree on one or more authentication methods.

4 Send data through the encrypted session.
Once the encrypted session is established, all data exchanged between the Secure Shell server and client is encrypted. Users now have secure remote access to the server and can execute commands and transfer files securely through the secure channel.

5 Use port forwarding to secure communications between other clients and servers.
Port forwarding, also known as tunneling, provides a way to redirect communications through the Secure Shell channel of an active session. When port forwarding is configured, all data sent to a specified port is redirected through the secure channel.

Reflection Secure Shell Settings Dialog Box
A2D removed a broken link to: reflection_secure_shell_settings_topic_gta in an excluded topic.A2D removed a broken link to: t_24022 in an excluded topic.Getting there (page 354)A2D unwrapped a non-popup link to getting there section: secure_shell_settings_ftp_clientA2D unwrapped a non-popup link to getting there section: secure_shell_settings_ftp_client

Use the Reflection Secure Shell Settings dialog box to manage Secure Shell settings and keys.
NOTE

- The settings you configure in this dialog box are saved to the A2D removed a broken link to: t_13406 in an excluded topic. Secure Shell configuration file (page 402). You can also configure Secure Shell settings by editing this file manually in any text editor.
- Within the configuration file, these settings are saved for the currently specified SSH configuration scheme (page 403).

Options

- “General Tab (Secure Shell Settings)” on page 355
- “Encryption Tab (Secure Shell Settings)” on page 357
- “Tunneling Tab (Secure Shell Settings)” on page 398
- “User Keys Tab (Secure Shell Settings)” on page 367
- “Host Keys Tab (Secure Shell Settings)” on page 373
- “GSSAPI Tab (Secure Shell Settings)” on page 390
- “Multi-hop Tab (Secure Shell Settings)” on page 401
- “PKI Tab (Secure Shell Settings)” on page 386
- “Host Data Tab (Secure Shell Settings)” on page 358

Related Topics

- “Connect using Secure Shell (SSH)” on page 349
- “Configure Secure Shell Settings” on page 351
- “Connect Using Secure Shell (FTP Client)” on page 756

Getting to the Reflection Secure Shell Settings Dialog Box

The way you access the Reflection Secure Shell Settings dialog box depends on the session type you are in.

Terminal session

NOTE: Secure Shell connections are available for VT terminal sessions.

1. Open the Document Settings dialog box.
   The steps depend on your user interface mode (page 120).

   **User Interface Mode**  
   **Steps**
   - Ribbon or InfoConnect Browser
     - With a session open in InfoConnect, from the Quick Access Toolbar, click .
   - TouchUx
     - Tap the Gear icon and then select Document Settings.

2. Click Configure Connection Settings.
3. Under Network Connection Type, select Secure Shell.
4 Under **Connection Options**, enter a host name.

5 Click **Security**.

**FTP Client**

1 In the **Connect to FTP Site** dialog box, click to select an FTP server.

2 Click **Security**.

3 Click the **Secure Shell** tab. **Use Reflection Secure Shell** must be selected.

4 (Optional) Specify an **SSH config scheme**. (If you leave **SSH config scheme** blank, Reflection saves any changes you make to an **SSH configuration scheme (page 403)** with the same name as the **Host name**.)

5 Click **Configure**.

**General Tab (Secure Shell Settings)**

<table>
<thead>
<tr>
<th>Index Term</th>
<th>Primary: Secure Shell Settings dialog box</th>
<th>Secondary: General tab</th>
</tr>
</thead>
</table>

| Index Term | Primary: Port | Secondary: configuring for Secure Shell |

The options are:

**Port number**

Specifies the port to connect to on the server. The default is 22, which is the standard port for Secure Shell connections.

**Protocol**

Specifies which version of the Secure Shell protocol Reflection uses when it establishes a connection to the host. The most secure value for this setting is 2 only.

**User Authentication**

Click in the box next to any **authentication method (page 362)** to clear or enable that method. You must select at least one authentication method. For protocol 2 connections, you can use the arrows to specify your order of preference. Reflection attempts each method in order, starting from the top.

**Server Keep Alive**

When **Server Keep Alive** is selected, Reflection sends NOOP messages to the server through the secure tunnel at the specified interval. Use this setting to maintain the connection to the server. Use **Interval** to specify how frequently server alive messages are sent. If this setting is not enabled, the Secure Shell connection will not terminate if the server dies or the network connection is lost. This setting can also be used to keep connections that only forward TCP sessions from being timed out by the server, as the server may timeout these connections because it detects no SSH traffic.

The Secure Shell **Server Keep Alive** setting is not related to the TCP keep alive setting that can be set in the Windows registry to keep all TCP/IP connections from being timed out by a firewall. To change the TCP/IP keep alive behavior, you need to edit the Windows registry.
Enable compression

When **Enable compression** is selected, the client requests compression of all data. Compression is desirable on modern lines and other slow connections, but will only slow down response rate on fast networks. The compression level setting is available for protocol version 1 only and has no effect on protocol version 2 connections.

Reuse existing connection if available

By default, multiple sessions to the same host reuse the original Secure Shell connection, and therefore don’t require re-authentication. If you clear **Reuse existing connection if available**, Reflection establishes a new connection for each session, which means that each new connection repeats the authentication process.

Logging Level

Determines how much information is written to the Secure Shell configuration file (page 402). You can also configure Secure Shell settings by editing this file manually in any text editor.

NOTE

- The settings you configure in this dialog box are saved to the Secure Shell configuration file (page 402). You can also configure Secure Shell settings by editing this file manually in any text editor.
- Within the configuration file, these settings are saved for the currently specified SSH configuration scheme (page 403).

Related Topics

- “Configure Secure Shell Settings” on page 351
- “Encryption Tab (Secure Shell Settings)” on page 357
- “User Keys Tab (Secure Shell Settings)” on page 367
- “Host Keys Tab (Secure Shell Settings)” on page 373
- “Tunneling Tab (Secure Shell Settings)” on page 398
- “Host Data Tab (Secure Shell Settings)” on page 358

Proxy Tab (Secure Shell Settings)

Index Term

Primary: SOCKS
Secondary: in Secure Shell sessions

Index Term

Primary: HTTP proxy in Secure Shell sessions

Use the Proxy tab to enable proxy use for Reflection Secure Shell sessions.
The options are:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>No proxy is configured. (This is the default.)</td>
</tr>
<tr>
<td>SOCKS</td>
<td>Select SOCKS to configure a Secure Shell connection through a SOCKS proxy.</td>
</tr>
<tr>
<td>HTTP</td>
<td>Select HTTP to configure a Secure Shell connection through an HTTP proxy.</td>
</tr>
<tr>
<td>Configure</td>
<td>Configure proxy server settings.</td>
</tr>
</tbody>
</table>

**NOTE**

- For Secure Shell connections, proxy use is enabled for the currently specified SSH config scheme (page 403) using the Proxy setting in the Secure Shell configuration file. The proxy server address is stored in the Windows registry on a per-user basis and applies to all Reflection sessions.
- In the Reflection FTP Client, the Security Properties dialog box includes tabs for both SOCKS configuration and Secure Shell configuration. You cannot use the SOCKS tab of the Security Properties dialog box to configure SOCKS proxied connections when you have enabled Use Reflection Secure Shell on the Secure Shell tab. To configure your SOCKS proxy, use the SOCKS setting on the Proxy tab of the Reflection Secure Shell Settings dialog box.

**Encryption Tab (Secure Shell Settings)**

Use the Encryption tab of the Reflection Secure Shell Settings dialog box to specify what ciphers (page 887) the Secure Shell connection should use. Different options are available depending on which Secure Shell protocol is used for the connection.
The options are:

**SSH protocol 2**

**Cipher List**
Use this list to specify the ciphers (page 887) you want to allow for protocol 2 connections to the current host. When more than one cipher is selected, the Secure Shell client attempts to use ciphers in the order you specify, starting from the top. To change the order, select a cipher from the list, then click the up or down arrow. The cipher used for a given session is the first item in this list that is also supported by the server.

**HMAC List**
Specifies the HMAC (hashed message authentication code) methods you want to allow. This hash is used to verify the integrity of all data packets exchanged with the server. When more than one HMAC is selected, the Secure Shell client attempts to negotiate an HMAC with the server in the order you specify, starting from the top. To change the order, select an HMAC from the list, then click the up or down arrow.

**Key Exchange Algorithms**
Specifies which key exchange algorithms the client supports, and the order of preference.

In some cases, you may need to change the order of the key exchange algorithms to put DH Group14 SHA1 ahead of the other values. This is required if you want use the hmac-sha512 MAC, or if you see the following error during key exchange: “fatal: dh_gen_key: group too small: 1024 (2*need 1024)”.

Two additional encryption algorithms (gss-group1-sha1-*) are supported, but do not appear in the list of available key exchange algorithms. These two algorithms are automatically proposed by the client when you enable GSSAPI/Kerberos from the General (page 355) tab (under User Authentication), and you also select Reflection Kerberos from the GSSAPI (page 390) tab.

**Signature types**
Specifies the hash algorithm the client uses in the process of proving possession of the private key. This hash is used during public key user authentication. Use RSA to specify the hash used with RSA keys and DSA to specify the hash used with DSA keys.

**SSH protocol 1 Cipher**
Use this setting to select the cipher you want used for protocol 1 connections to the current host. The default is Triple DES and this option is recommended.

**Run in FIPS Mode**
When Run in FIPS mode is selected, Reflection enforces the United States government Federal Information Processing Standard (FIPS) 140-2 (page 327) for this connection. Options on the Encryption tab that do not meet this standard are not available when Run in FIPS mode is selected.

**NOTE**

- The settings you configure in this dialog box are saved to the A2D removed a broken link to: t_13406 in an excluded topic. Secure Shell configuration file (page 402). You can also configure Secure Shell settings by editing this file manually in any text editor.
- Within the configuration file, these settings are saved for the currently specified SSH configuration scheme (page 403).

**Host Data Tab (Secure Shell Settings)**

**Index Term**
Primary: Secure Shell Settings dialog box
Secondary: Host Data tab
Use the Host Data tab to set environment variables and run commands on the server.

The options are:

**Environment Variables**

- **Add**: Opens the New Environment Variable dialog box, from which you can specify a new variable and value.
- **Modify**: Edit the selected variable.
- **Delete**: Delete the selected variable.

**Remote Command**

- **Command**: Specifies one or more commands to run on the remote server. Use a semicolon (;) to separate multiple commands when connecting to a UNIX server. Use an ampersand (&) to separate commands when connecting to a Windows server. After a connection is established, the server executes (or attempts to execute) the specified command(s), and then the session terminates. The server must be configured to allow commands received from the client to run.

  The commands must be specified in the correct format for your server. For example, to capture a directory listing on a UNIX server, you might specify the following:

  `ls > list.txt`

  On a Windows server, the equivalent command would be one of the following, depending on how the Windows server is configured:

  `dir > list.txt`
  `cmd /c dir > list.txt`

**Authentication**

- **Index Term**
  - Primary: authentication (Secure Shell sessions)
  - Secondary: introduction

Authentication is the process of reliably determining the identity of a communicating party. Identity can be proven by something you know (such as a password), something you have (such as a private key or token), or something intrinsic about you (such as a fingerprint). Secure Shell connections require both host (server) and user (client) authentication. By default the host authenticates to the user using its private key, and then the user authenticates to the host using a password.

**In this Section**

- “Server Authentication using Public Keys” on page 360
- “Connection Reuse in Secure Shell Sessions” on page 360
- “Client Authentication Methods” on page 362
Server Authentication using Public Keys

Index Term
Primary: authentication (Secure Shell sessions)
Secondary: server

Reflection supports two types of server authentication: public key and certificate (a special form of public key authentication).

When public key authentication is used for host authentication, the following sequence of events takes place.

1. The Secure Shell client initiates a connection.
2. The server sends its public key to the client.
3. The client looks for this key in its trusted host key store.
4. To confirm that the server actually holds the private key that corresponds to the received public key, the client sends a challenge (an arbitrary message) to the server and computes a "hash" on page 887 based on this message text.
5. The server creates a digital signature based on the challenge message. To do this, the server independently computes the message hash, and then encrypts the computed hash using its private key. The server attaches this digital signature to the original challenge and returns this signed message to the client.
6. The client decrypts the signature using the public key and compares the hash with its own computed hash. If the values match, host authentication is successful.

Connection Reuse in Secure Shell Sessions

Index Term
Primary: connection reuse

Index Term
Primary: authentication (Secure Shell sessions)
Secondary: connection reuse
Connection reuse enables additional Secure Shell sessions to be added to an already established Secure Shell connection. A simple analogy for this is a fiber optic cable, in which the outside pipe represents the connection, through which the various fiber-optic strands (the sessions and tunnels) are routed. The additional sessions can be new Reflection Secure Shell terminal sessions, new Reflection SFTP file transfer sessions, forwarded X11 connections, any communications configured for port forwarding through the SSH tunnel, or any connection established using one of the Reflection Secure Shell command line utilities.

When you reuse an established Secure Shell connection, you don't need to repeat the authentication process. The new session always uses all the Secure Shell settings configured for the initial connection. Any differences in authentication methods, cipher or MAC settings, or port forward definitions are ignored.

Connection reuse is enabled by default for all Secure Shell connections made using the Reflection user interface. You can disable this feature by clearing the Reuse existing connection if available check box on the General (page 355) tab of the Secure Shell Settings dialog box.

After you have established a connection in which Reuse existing connection if available is enabled, subsequent Secure Shell sessions reuse the established connection if all of the following conditions are true:

- The host name in the new session must exactly match the host name in the established connection.
- The user name in the new session must exactly match the user name in the established connection.
- The port number in the new session must be the same as the port number in the established connection. (This condition will be true by default.)
- If the original session is configured to use an SSH configuration scheme (page 403) that is different from the host name, the new session must be configured to use the same scheme.

**NOTE:** If you are using command line utilities to make SSH connections, additional conditions must be met in order to reuse existing connections. These are outlined below.

**Connection Reuse in Reflection Command Line Sessions**

Connection reuse is useful for command line operations in which Secure Shell connections are required, numerous small operations are needed between a client and a single server, and the authentication and key exchange time interval is a significant part of the total connection time. This would be the case if you need to transfer multiple small files, or execute simple operating system commands that do not result in large quantities of returned output. In these cases it might be advantageous to create the original SSH connection using the `ssh` (or `ssh2`) command line utility, and then reuse the connection with subsequent command line utility operations.

By default, connection reuse is disabled for the Reflection Secure Shell client command line utilities (`ssh` (page 423), `scp` (page 432), `sftp` (page 426), `scp2`, and `sftp2`). To enable connection reuse with any of these command line utilities, you must use one of the following techniques.

- Add the switch `-o ConnectionReuse=yes` to each command line. You must use this switch when you establish the initial connection, and in all subsequent command lines that you want to reuse the initial connection. For example, with the following commands, the `sftp` connection will reuse the connection established by the `ssh` command.

```
ssh "-o connectionReuse=yes" myuser@myhost
sftp "-o connectionReuse=yes" myuser@myhost
```
In the DOS command window (or at the beginning of a batch script file), set the environment variable SSHConnectionReUse as shown here:

```
set SSHConnectionReUse=yes
```

If conflicting settings are present, the `-o` switch takes precedence.

**NOTE**

- OpenSSH servers support a MaxStartups parameter that can be used to limit the number of concurrent unauthenticated sessions. This setting will affect the number of Reflection sessions you can establish that reuse an existing connection. When you have reached the maximum number of sessions specified in the MaxStartups parameter, all subsequent sessions will require a separate SSH connection with authentication. Contact your ssh server administrator, if you need to establish more concurrent unauthenticated sessions than are currently allowed.

- Command line utilities cannot be configured for connection reuse in the Secure Shell. The `ConnectionReuse` keyword in this file is always ignored by Reflection command line utilities, even when the `-H` switch is used to specify an SSH configuration scheme that includes this setting.

---

**Client Authentication Methods**

Index Term
- Primary: authentication (Secure Shell sessions)
- Secondary: user

The Reflection Secure Shell Client supports four methods of user authentication: Kerberos (GSSAPI), Public Key, Keyboard Interactive, and Password. Use the Reflection Secure Shell Settings (page 353) dialog box to configure your authentication preferences. You must select at least one authentication method. When more than one method is selected, the Secure Shell Client tries to authenticate in the order you specify. By default, Reflection attempts Public Key authentication first, followed by Keyboard Interactive, and then Password.

**NOTE:** The Public Key and GSSAPI / Kerberos V5 authentication methods require both server and client configuration.

<table>
<thead>
<tr>
<th>Authentication method</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Password**               | Prompts the client user for the login password for that user on the Secure Shell server host.  
                            | The password is sent to the host through the encrypted channel.               |
| **Keyboard interactive**   | Supports any procedure in which authentication data is entered using the keyboard, including simple password authentication, thereby enabling the Secure Shell client to support a range of authentication mechanisms, such as RSA SecurID tokens or RADIUS servers.  
                            | A client administrator could, for example, configure keyboard interactive authentication to handle situations in which multiple prompts are required, such as for password updates.  
                            | Keyboard data is sent to the host through the encrypted channel.             |
Public Key Authentication

Public key authentication relies on public/private key pairs. Public key authentication can be used for both server (host) and client (user) authentication. To configure public key authentication for the Secure Shell client, you create (or import) a key pair for your client computer, then upload the public key to your host(s). You can create and manage public keys for client authentication using either the User Keys (page 367) tab in the Reflection Secure Shell Settings dialog box, or the “Reflection Key Agent” on page 375. Depending on how you have configured your key, you may be prompted to enter a "passphrase" on page 888 in order to complete a connection using public key authentication.

One form of public key authentication is accomplished using X.509 certificates. Reflection can be configured to authenticate using certificates managed by the “Reflection Certificate Manager” on page 446 and/or the Windows Certificate Manager. Public Key authentication must be enabled if you use certificates for authentication.

How Public Key Authentication Works

Public key cryptography uses a mathematical algorithm with a public/private key pair to encrypt and decrypt data. One of the keys is a public key, which can be freely distributed to communicating parties, and the other is a private key, which should be kept secure by the owner of the key. Data encrypted with the private key can be decrypted only with the public key; and data encrypted with the public key can be decrypted only with the private key.

When keys are used for authentication, the party being authenticated creates a digital signature using the private key of a public/private key pair. The recipient must use the corresponding public key to verify the authenticity of the digital signature. This means that the recipient must have a copy of the other party’s public key and trust in the authenticity of that key.

Related Topics

- "General Tab (Secure Shell Settings)" on page 355
- "Configure Public Key Authentication" on page 364
- "GSSAPI (Kerberos) Authentication for Secure Shell Sessions" on page 387
Managing User Keys

In this Section

- “Configure Public Key Authentication” on page 364
- “Add Keys to Your User Keys List” on page 365
- “Upload Client Public Keys to the Server” on page 366
- “Change a User Key Passphrase” on page 366
- “Export a User Key” on page 367
- "User Keys Tab (Secure Shell Settings)” on page 367
- “User Key Generation Dialog Box” on page 370

Configure Public Key Authentication

The following procedures configure client authentication using public keys.

To configure the client for public key authentication

1. A2D removed a broken link to: reflection_secure_shell_settings_topic_gta in an excluded topic. A2D removed a broken link to: t_24022 in an excluded topic. Open the Reflection Secure Shell Settings dialog box (page 354). A2D removed a broken link to: secure_shell_settings_ftp_clienta.

2. From the General tab, make sure that Public Key is selected under User Authentication. (If you want to ensure that only public key authentication is used, clear the other options.)

3. Click the User Keys tab. In the Use column, select the key or keys you want to use to authenticate to the currently specified host.

   **NOTE:** To add keys to this list, see Add Keys to your User Key list (page 365).

4. Click OK.

To configure the server for public key authentication

- Upload the public key(s) to the host(s) (page 366).
Add Keys to Your User Keys List

The User Keys (page 367) tab of the Reflection Secure Shell Settings dialog box displays a list of keys you can use for public key (page 363) authentication. You can add keys to the list by creating new keys or importing existing keys.

To create a new key pair using Reflection

1. Click the User Keys tab.
2. Click Generate Key.
3. Specify a key type and key length.
4. Either specify a “passphrase” on page 888, or select No passphrase.

   CAUTION: If you select No passphrase, the private key saved to your computer is unencrypted, and anyone who gains access to this key will be able to use it to authenticate as you.

5. Click Create.

By default, keys are created in your user .ssh folder (page 891). The default private key name identifies the key type, size, and the client host name. The public key is saved to the same location using the private key name with an added *.pub file extension.

To create a new key pair using the Key Agent

1. Start and unlock the Reflection Key Agent. (From the Windows Start menu, go to Programs > Attachmate Reflection > Utilities > Key Agent.)
2. Click Generate Keys.
3. Specify a key name, key type, and key length, and click OK.

   NOTE: Keys you create using the Key Agent are stored by the agent in encrypted form.

To Import keys into the Reflection key store

1. Open the Reflection Secure Shell Settings dialog box (page 354)
2. Click the User Keys tab.
3. Click Import.
4. Browse to locate the private key you want to import. Each key pair includes two files, one with a *.pub extension and one with no file extension. The private key is the file with no extension.

   NOTE: Imported keys are copied to the Reflection key store located in your user .ssh folder (page 891).
Upload Client Public Keys to the Server

Use the **Upload** button on the **User Keys** tab to upload a public key to the Secure Shell server. The public key is transferred using the secure SFTP protocol. You will need the ability to use password authentication (or another authentication method) in order to upload the public key. Once the public key is successfully uploaded, you may disable other authentication methods.

### To upload a key

1. A2D removed a broken link to: reflection_secure_shell_settings_topic_gta in an excluded topic. A2D removed a broken link to: t_24022 in an excluded topic. Open the Reflection Secure Shell Settings dialog box (page 354) A2D removed a non-popup link to getting there section: secure_shell_settings_ftp_clienta.
2. Select a key from the **User Keys** tab and click **Upload**. (The **Upload** button is not available if no key is selected, or if you have selected a certificate.)
3. If prompted, enter the host name, the name of the user who will authenticate, and the user password.
4. After the secure connection to the host has been established, a dialog box appears, displaying information about where on the host Reflection will upload this key. In most cases you do not need to change these settings. See the notes below for more information.

   The **Upload Public Key** dialog box displays information about the transfer.
5. Click **OK** to close this dialog box.

### NOTE

- Keys uploaded to hosts running Reflection for Secure IT, F-Secure, and SSH Communications (SSH Tectia) servers are exported using RFC 4716 compliant format. By default these are installed to the user's .ssh2 directory and an appropriate **Key** entry is made in the authorization file. If this file did not previously exist, it is created and given appropriate file permissions.
- Keys uploaded to hosts running OpenSSH servers are exported using OPENSSH format. By default they are added to the **authorized_keys** file located in the user's .ssh directory. If this file did not previously exist, it is created and given appropriate file permissions.

Change a User Key Passphrase

You can change the "passphrase" on page 888 used to protect a user key.
To change the passphrase.

1. A2D removed a broken link to: reflection_secure_shell_settings_topic_gta in an excluded topic.A2D removed a broken link to: t_24022 in an excluded topic.Open the Reflection Secure Shell Settings dialog box (page 354)A2D removed a non-popup link to getting there section: secure_shell_settings_ftp_clienta.

2. Click the User Keys tab and select a key from the list.

3. Click Change Passphrase. (This button is not available if no key is selected, or if you have selected a certificate managed by either the Reflection Certificate Manager or the Windows Certificate Manager.)

Export a User Key

Index Term
Primary: user keys
Secondary: exporting

Index Term
Primary: export
Secondary: user keys

Use the procedure below to export your user keys to a new location and/or format.

NOTE: If you want to upload a public key to a Secure Shell server, you do not need to use this procedure. Use the Upload button to do this in a single step. Reflection automatically determines the correct key format for the server you specify. See Uploading Keys to the Server (page 366) for more information.

To export a key

1. A2D removed a broken link to: reflection_secure_shell_settings_topic_gta in an excluded topic.A2D removed a broken link to: t_24022 in an excluded topic.Open the Reflection Secure Shell Settings dialog box (page 354)A2D removed a non-popup link to getting there section: secure_shell_settings_ftp_clienta.

2. From the User Keys tab, select a key and click Export. (This button is not available if no key is selected, or if you have selected a certificate managed by either the Reflection Certificate Manager or the Windows Certificate Manager.)

3. Enter the “passphrase” on page 888 for the selected key.

4. (Optional)

   To
   Include the private key in the export
   Export the key in OpenSSH format

   Do this
   Select Export Private Key.
   Select Save in OpenSSH format.

5. From the Public Key Filename dialog box, specify a name and location for the exported key.

6. Click Save.

User Keys Tab (Secure Shell Settings)

Index Term
Primary: user keys
Secondary: User Keys Tab (Secure Shell Settings)
The **User Keys** tab provides tools for creating and managing the keys that authenticate your client session to the host when you establish a Secure Shell connection using "Public Key Authentication" on page 363.

**NOTE:** Changes you make in this dialog box are saved to the currently specified SSH configuration scheme (page 403) when you click OK.

Reflection maintains a list of available user keys. To specify which key or keys you want Reflection to use for authentication to the current host, select one or more check boxes in the **Use** column (or enable **Use all keys for authenticating to the host**).

The list of keys includes:

- Keys you have created using the **User Key Generation** (page 370) dialog box.
- Keys you have added using the **Import** button.
- Keys you have copied manually to the Reflection Secure Shell folder (page 891).
- Keys and certificates in the "Reflection Key Agent" on page 375.
- User and Authentication Agent keys copied during migration of F-Secure settings to Reflection.
- Certificates in the A2D unwrapped a broken link to: t_5715 in an excluded topic.Windows Certificate Manager in your personal store.
- Certificates in the "Reflection Certificate Manager" on page 446 in your personal store.
The following key management tools are also available:

Select keys to use for authenticating to the host:

<table>
<thead>
<tr>
<th>Tool</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>View</strong></td>
<td>Displays the contents of the selected key or certificate.</td>
</tr>
<tr>
<td><strong>Generate</strong></td>
<td>Opens the User Key Generation (page 370) dialog box, which you can use to configure a public/private key pair for user key authentication.</td>
</tr>
<tr>
<td><strong>Upload</strong></td>
<td>Upload a public key (page 366) to the currently specified host.</td>
</tr>
<tr>
<td><strong>Import</strong></td>
<td>Add a private key to the list of available keys. You can use this feature to provide easy access within Reflection to keys created using other applications. Importing a key copies it to the Reflection Secure Shell folder (page 891).</td>
</tr>
<tr>
<td><strong>Export</strong></td>
<td>Export a public key (page 367), or public/private key pair.</td>
</tr>
<tr>
<td><strong>Delete</strong></td>
<td>Deletes the selected key.</td>
</tr>
<tr>
<td><strong>Change Passphrase</strong></td>
<td>Change the “passphrase” on page 888 used to protect the selected key.</td>
</tr>
<tr>
<td><strong>Add to Key Agent</strong></td>
<td>Adds the selected key to the “Reflection Key Agent” on page 375. If you have not yet started the Key Agent for the first time, or if the Key Agent is locked, you will be prompted to enter the Key Agent passphrase. In addition, you will be prompted to enter the private key’s passphrase before the key can be added to the agent.</td>
</tr>
</tbody>
</table>

Authentication options

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Use all keys for authenticating to the host</strong></td>
<td>When this option is selected, the client attempts to authenticate with all the listed keys, regardless of whether or not the Use checkbox is selected.</td>
</tr>
<tr>
<td><strong>Prefer SSH key signature over certificate signature</strong></td>
<td>This setting determines the order in which the client presents certificate signature types to the server during public key authentication. When this setting is selected (the default), the client sends the key using a standard ssh key signature first (ssh-rsa or ssh-dss). If that fails, the client tries again using a certificate signature (x509-sign-rsa or x509-sign-dss). When this option is cleared, the client presents the certificate signature first. This can be useful in situations where the certificate key type is required and the server doesn't allow the client to attempt a second authentication using the same key with a different signature type.</td>
</tr>
</tbody>
</table>
Key agent

**Allow Agent Forwarding** Enables forwarding of the “Reflection Key Agent” on page 375 connection. Agent forwarding should be enabled with caution. Users with the ability to bypass file permissions on the remote host (for the agent’s Unix-domain socket) can access the local agent through the forwarded connection. Attackers cannot obtain key material from the agent, however they can perform operations on the keys that enable them to authenticate using the identities loaded into the agent.

**Add key used for authenticating to host to key agent** This setting is available when Allow agent forwarding is enabled. When it is selected and public key authentication to the server is successful, the key or certificate that was used for authentication is automatically added to the “Reflection Key Agent” on page 375. This key is not saved in the Key Agent, but remains available as long as the Key Agent is running.

**Launch Key Agent** Launches the “Reflection Key Agent” on page 375.

**User Key Generation Dialog Box**

**Index Term**
Primary: user keys  
Secondary: User Key generation dialog box

**Getting there**

1 Open the Reflection Secure Shell Settings dialog box.
2 Click the User Keys tab.
3 Click Generate Key.

Use this dialog box to configure a public/private key pair for user key authentication.

The options are:

**Key Type**  
Specifies the algorithm used for key generation.

**Key Length**  
Specifies the key size. Up to a point, a larger key size improves security. Increasing key size slows down the initial connection, but has no effect on the speed of encryption or decryption of the data stream after a successful connection has been made. The length of key you should use depends on many factors, including: the key type, the lifetime of the key, the value of the data being protected, the resources available to a potential attacker, and the size of the symmetric key you use in conjunction with this asymmetric key. To ensure the best choice for your needs, we recommend that you contact your security officer.

**No passphrase**  
Select this check box if you want to connect without being prompted for a passphrase. Note: If you select No passphrase, the private key saved to your computer is unencrypted.

**Passphrase**  
Specify a “passphrase” on page 888 that will be required when you connect with this key. Note: If you don't want to use a passphrase, you must select the No passphrase setting.

**Verify**  
Retype the passphrase here for confirmation.
Secure Connections

Configure Host Key Checking

In this Section
- “Configure Host Key Checking” on page 371
- “Configure the Preferred Host Key Type” on page 372
- “The Known Hosts File” on page 373
- “Host Keys Tab (Secure Shell Settings)” on page 373
- “Host Key Authenticity Dialog Box” on page 374

Configure Host Key Checking

To configure host key checking

1. Open the Reflection Secure Shell Settings dialog box (page 354).
2. Click the Host Keys tab.
3. Click Enforce strict host key checking.
4. Select one of the following options:

<table>
<thead>
<tr>
<th>Select</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ask User (default)</td>
<td>Display the Host Key Authenticity (page 374) confirmation dialog box when you connect to an unknown host.</td>
</tr>
<tr>
<td>Yes</td>
<td>Enforce strict host key checking — Reflection does not connect if the host is not a &quot;trusted host&quot; on page 890. Before you can connect, you must add the host key to your list of trusted host keys.</td>
</tr>
<tr>
<td>No</td>
<td>Prevent enforcement of strict host key checking — Reflection connects without displaying a confirmation dialog box. The host key is not added to the list of trusted keys.</td>
</tr>
</tbody>
</table>
NOTE

- **Enforce strict host key checking** has no effect when the host has been configured to authenticate using X.509 certificates. If a host presents a certificate for host authentication and you do not have the required CA certificate in your Trusted Root store, the connection fails.

- Changes you make to this setting are saved to the currently specified **SSH configuration scheme** (page 403).

- Secure Shell settings are saved to the **Secure Shell configuration file** (page 402). You can also configure Secure Shell settings by editing this file manually in any text editor. The **keyword** (page 405) used to configure this setting is **StrictHostKeyChecking**.

Related Topics

- "Host Key Authenticity Dialog Box" on page 374
- "The Known Hosts File" on page 373

Configure the Preferred Host Key Type

Index Term
Primary: host keys
Secondary: prefer key or certificate

Use **Prefer ssh keys over certificates** to specify the order of preference for host key algorithms. This setting is useful when the server is configured for both certificate and standard host key authentication. SSH protocol allows only one attempt to authenticate the host. If the host presents a certificate, and the client is not configured for host authentication using certificates, the connection fails. (This is different from user authentication, in which multiple authentication attempts are supported.)

To configure the preferred host key type (standard SSH keys or certificates)

1. Open the **Reflection Secure Shell Settings** dialog box (page 354).

2. Click the **Host Keys** tab.

3. To have the host use standard host keys for authentication, select **Prefer ssh keys over certificates**.

   -or-

   To use certificates for authentication, clear **Prefer ssh keys over certificates**.

NOTE

- Changes you make to this setting are saved to the currently specified **SSH configuration scheme** (page 403).

- Secure Shell settings are saved to the **Secure Shell configuration file** (page 402). You can also configure Secure Shell settings by editing this file manually in any text editor. The keyword used to configure this setting is **HostKeyAlgorithms**.
The Known Hosts File

The Reflection Secure Shell Client maintains a list of known hosts in the known hosts file. Reflection supports both user-specific and global known hosts files.

The user known hosts file

The user-specific known hosts file is called known_hosts and is located in the user's .ssh folder (page 891). This is the default known hosts file. Reflection automatically updates this file when:

- You update the Trusted Host Keys list in the Host Keys (page 373) tab of the Secure Shell settings dialog box.
- or -
- You connect to a previously unknown host and answer Always in response to the Host Key Authenticity (page 374) prompt.

The global known hosts file

System administrators can add a system-wide known hosts file named ssh_known_hosts to the Reflection application data folder on page 891. In this location the known hosts file provides a list of hosts for all users of the PC. Keys in this list can be viewed, but not edited in the Global Host Keys list in the Host Keys (page 373) tab of the Secure Shell settings dialog box.

Related Topics

- “Configure Host Key Checking” on page 371
- “Deploy Secure Shell Settings with a Companion Installer” on page 421

Host Keys Tab (Secure Shell Settings)

Use the Host Keys tab to manage the keys that authenticate the host to your client session. You can use this tab to view the list of trusted hosts (page 890), add or delete host keys, and specify how you want Reflection to handle unknown hosts.

Host authentication enables the Secure Shell client to reliably confirm the identity of the Secure Shell server. This authentication is done using public key authentication. If the host public key has not previously been installed on the client, the first time you attempt to connect you see a message
indicating that this is an unknown host. This message includes a fingerprint that identifies the host. To be sure that this is actually your host, you should contact the host system administrator who can confirm that this is the correct fingerprint. Until you know that the host is actually your host, you are at risk of a “man-in-the-middle” attack, in which another server poses as your host. If you select Always in response to this prompt, the host is added to the Trusted Host Keys list. To avoid the need to contact the host administrator, you can add host keys to the Trusted Host Keys list before the first connection.

The options are:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enforce strict host key checking</td>
<td>Specifies how Reflection should handle host key checking (page 371) when connecting to an unknown host.</td>
</tr>
<tr>
<td>Prefer ssh keys over certificates</td>
<td>Specifies Reflection’s order of preference for host key algorithms (page 372). When this setting is unselected (the default), Reflection requests host certificates before host keys. When this setting is selected, Reflection requests host keys before host certificates.</td>
</tr>
<tr>
<td>Trusted Host Keys</td>
<td>Displays a list of trusted hosts for the current Windows user. You can modify the contents of this list using Import and Delete.</td>
</tr>
<tr>
<td>Import</td>
<td>Adds a host’s public key to your Trusted Host Keys list.</td>
</tr>
<tr>
<td>Delete</td>
<td>Removes the selected key from your Trusted Host Keys list.</td>
</tr>
<tr>
<td>CAUTION:</td>
<td>You will see no confirmation prompt and this action cannot be undone.</td>
</tr>
<tr>
<td>Global Host Keys</td>
<td>Displays a list of trusted host keys that are available to all users of the computer. Items on this list can be viewed but not edited.</td>
</tr>
<tr>
<td>System administrators can modify the Global Host Keys list using the global known hosts file (page 373).</td>
<td></td>
</tr>
</tbody>
</table>

**Host Key Authenticity Dialog Box**

This confirmation dialog box appears if the host you are connecting to is not a “trusted host” on page 890. Do you want to trust this new host key and continue connecting?

Host authentication enables the Secure Shell client to reliably confirm the identity of the Secure Shell server. This authentication is done using public key authentication. If the host public key has not previously been installed on the client, the first time you attempt to connect you see a message indicating that this is an unknown host. This message includes a fingerprint that identifies the host. To be sure that this is actually your host, you should contact the host system administrator who can confirm that this is the correct fingerprint. Until you know that the host is actually your host, you are at risk of a “man-in-the-middle” attack, in which another server poses as your host.
The options are:

- **Always**: Make the connection and add this host to the list of trusted hosts. You will not see this prompt for subsequent connections to the same host unless you remove the host from the trusted host list, or the host key changes.
- **Once**: Make the connection but do not add the host to the trusted host list. You will see this prompt again the next time you make a connection to the same host.
- **No**: Do not make the connection and do not add the host to the trusted host list.

**Reflection Key Agent**

- **Index Term**
  - Primary: Key Agent
  - Secondary: overview

The Reflection Key Agent is a tool for creating and managing Secure Shell user keys. The Key Agent:

- Stores keys securely in encrypted form.
- Enables you to access all stored keys and certificates with a single passphrase. Because keys are decrypted and stored in memory, only your initial passphrase is required. The agent handles all subsequent authentication using your stored keys and certificates.
- Supports agent forwarding to additional Secure Shell servers. This enables public key authentication to be used for additional Secure Shell connections without transporting the private key.
- Provides tools for key and certificate management including: creating new keys, importing existing keys, importing certificates from the Windows and Reflection certificate stores, deleting keys, and uploading the public key file to a specified server in the appropriate format.
- Maintains a log file to aid in troubleshooting.

**In this Section**

- “Start the Key Agent” on page 375
- “Configure Reflection to Authenticate Using the Key Agent” on page 376
- “Managing Keys and Certificates” on page 377
- “Working with the Key Agent” on page 382

**Start the Key Agent**

- **Index Term**
  - Primary: Key Agent
  - Secondary: starting

You can start the Reflection Key Agent from the Windows Start menu or from any Reflection application that supports Secure Shell connections.

---

**NOTE**: Whenever the Key Agent is running, the **Key Agent** icon is visible in the Windows system tray.

---

**To start the agent the first time**

1. In the Windows Start menu, locate the Reflection installation folder.
2 Go to Utilities > Key Agent.
3 Enter a passphrase (page 383). Use this phrase whenever you want to unlock the agent.

To start the agent from the Windows Start menu

1 In the Windows Start menu, locate the Reflection installation folder.
2 Go to Utilities > Key Agent.
3 Click Unlock to unlock the agent.

To start the agent from a Reflection Application

1 A2D removed a broken link to: reflection_secure_shell_settings_topic_gta in an excluded topic.A2D removed a broken link to: t_24022 in an excluded topic.Open the Reflection Secure Shell Settings dialog box (page 354)A2D removed a non-popup link to getting there section: secure_shell_settings_ftp_clienta.
2 Go to the User Keys tab, and click Launch Key Agent.
3 Click Unlock to unlock the agent.

-or-

- Start a connection that is configured to use a key stored in the Key Agent.

If the agent is not already running, Reflection launches it automatically and displays a prompt to unlock the agent.

Related Topics

- "Key Agent Passphrase" on page 383
- "Lock or Unlock the Key Agent" on page 383
- "Hide and View the Key Agent" on page 384
- "Stop the Key Agent" on page 384

Configure Reflection to Authenticate Using the Key Agent

Index Term
Primary: Key Agent
Secondary: configuring authentication

If your Reflection application supports Secure Shell connections, you can use this procedure to configure Reflection to authenticate using the Key Agent.

To configure Reflection to authenticate using a key in the agent

1 Add a private key (page 377) to the Key Agent, or import a certificate (page 380).
2 Configure the host:

If you are authenticating    Do this
Using keys                  Upload the public key (page 378).
Using certificates           Install the CA certificate on the host and configure the host for user authentication with certificates. (Refer to your Secure Shell server documentation for more information.)
3 Launch a Reflection application that supports Secure Shell connections and open the A2D removed a broken link to: reflection_secure_shell_settings_topic_gta in an excluded topic.A2D removed a broken link to: t_24022 in an excluded topic.**Reflection Secure Shell Settings** (page 354)A2D removed a non-popup link to getting there section: secure_shell_settings_ftp_clienta.

4 From the **General** tab, make sure that **Public Key** is selected under **User Authentication**. (If you want to ensure that only public key authentication is used, clear the other options.)

5 Click the **User Keys** tab. The keys and certificates in the Reflection Key Agent are included in the list of available keys.

6 In the **Use** column, select the key(s) or certificate(s) you want to use to authenticate to the currently specified host, and then click **OK**.

---

**NOTE**

- Secure Shell settings are saved in your Secure Shell configuration file (page 402) and apply to a specific SSH configuration scheme (page 403). (If you don't specify a scheme, settings apply to all connections to the current host.)

- You do not need to repeat the client configuration steps for new connections using the same SSH configuration scheme (or host name).

**Related Topics**

- "**Getting to the Reflection Secure Shell Settings Dialog Box**" on page 354

**Managing Keys and Certificates**

Use these procedures to manage keys and certificates in the Reflection Key Agent.

**In this Section**

- "Add Keys to the Key Agent" on page 377
- "Upload Keys to the Server" on page 378
- "Import Keys to the Key Agent" on page 379
- "Import Certificates to the Key Agent" on page 380
- "Export Public Keys" on page 380
- "Allow Adding Keys Remotely" on page 380
- "Allow Deleting Keys Remotely" on page 381
- "Confirm Remote Private Key Operations" on page 381
- "Enable Support for SHA256 Signatures" on page 382
- "Generate Key Dialog Box" on page 382

**Add Keys to the Key Agent**

**Index Term**

**Primary:** Key Agent

**Secondary:** adding keys

You can add keys to the Key Agent by generating keys using the Key Agent, or by importing keys that you have created using Reflection or other applications. Keys you create using the Key Agent are stored by the agent in encrypted form and can only be accessed by using the Key Agent. Keys you
create using the Reflection **Secure Shell Settings** dialog box are stored in your `<My Documents>\Reflection\.ssh` folder. When you import a key into the Key Agent, the imported key is stored within the agent in encrypted form, and the original key also remains available unless you delete it.

**To generate a new key pair using the Key agent**

1. Start and unlock (page 375) the Key Agent.
2. Click **Generate Key**.
3. Specify a key name, key type, and key length, and then click **OK**.

**To generate a new key pair using Reflection**

1. A2D removed a broken link to: reflection_secure_shell_settings_topic_gta in an excluded topic.A2D removed a broken link to: t_24022 in an excluded topic.Open the Reflection Secure Shell Settings dialog box (page 354)A2D removed a non-popup link to getting there section: secure_shell_settings_ftp_clienta.
2. On the **User Keys** tab, click **Generate Key**.
3. Specify a key name, key type, and key length. (Use the **Browse** button to specify a non-default name or location for the key.)
4. Either specify a passphrase, or select **No passphrase**.
5. Click **Create**.

**To import a private key into the Key Agent**

1. Start and unlock (page 375) the Key Agent.
2. From the **File** menu, click **Import Private Key**.
3. Select the key you want to add. The default location for keys you create using Reflection applications is:

   `personal_documents_folder\Attachmate\Reflection\.ssh`

   The Agent opens this folder by default when you click **Import Private Key**. Each key pair includes two files: one with a `.pub` extension; and one with no file extension. The private key is the file with no extension.
4. If the key is protected by a passphrase, you must enter the phrase correctly before you can import the key.
   
   After you import the key, it is protected by the Key Agent passphrase. The original key and passphrase are not changed.

**Related Topics**

- “Upload Keys to the Server” on page 378
- “Generate Key Dialog Box” on page 382
- “Import Certificates to the Key Agent” on page 380

**Upload Keys to the Server**

Index Term
Primary: Key Agent
Secondary: uploading keys to the server

Secure Shell key authentication uses a public/private (page 889) key pair. The public key must be added to the authorized keys on a host before you can authenticate to that host using the key pair. You can use the Key Agent to make the upload process easy. The agent automatically determines
what kind of Secure Shell server is running on the host you specify, exports your public key using the correct key type for that host, and installs it (using SFTP) to the correct location for the user you specify.

The public key is transferred using the secure SFTP protocol. You will need the ability to use password authentication in order to upload the public key.

To upload the public key to the server

1. Start and unlock (page 375) the Key Agent.
2. Select the key you want to use for authentication to the server, and click **Upload**.
3. Enter the name of the host to which you are uploading the key. (In most cases you can leave **SSH config scheme** blank. The Key Agent makes a Secure Shell connection to the host in order to upload the key. The **SSH configuration scheme** (page 403) you specify determines which SSH settings are used for this connection.) Click **OK**.
4. When prompted, enter the name and password of the user who will authenticate to the host using the key.

After the secure connection to the host has been established, a dialog box appears displaying information about where on the host Reflection will upload this key. In most cases you do not need to change these settings. See the notes below for more information.

NOTE

- **Upload** is not available if the Key Agent is locked.
- The **Upload Public Key** dialog box displays information about the transfer. Click **OK** to close this dialog box.
- Keys uploaded to hosts running Reflection for Secure IT, F-Secure, and SSH Communications (SSH Tectia) servers are exported to SECSH format. By default these are installed to the user's **.ssh2** directory and an appropriate **KEY** entry is made in the **authorization** file. If this file did not previously exist, it is created and given appropriate file permissions.
- Keys uploaded to hosts running OpenSSH servers are exported using OPENSSH format. By default they are added to the **authorized_keys** file located in the user's **.ssh2** directory. If this file did not previously exist, it is created and given appropriate file permissions.

---

**Import Keys to the Key Agent**

**Index Term**
- Primary: import
- Secondary: keys to the Key Agent

- Choose **File > Import Private Key**.

**NOTE:** **Import Private Key** is not available if the Key Agent is locked.

After the import, the original key remains in its original location. A copy is added in encrypted form to the agent. If the imported key is encrypted with a passphrase, you are prompted to enter it.

**Related Topics**

- “Configure Reflection to Authenticate Using the Key Agent” on page 376
Import Certificates to the Key Agent

1. Start and unlock (page 375) the Key Agent.
2. From the File menu, select Import Certificate from <store>.
   All certificates currently available in the certificate store you selected are displayed.
3. Select the certificate you want to import, and then click OK.

Export Public Keys

You can export plain text public keys from keys stored in the Reflection Key agent.

To export a plain text public key

1. Select the public key that you want to export.
2. Choose File > Export Public Key.
   The agent exports the public key for the currently selected key.

NOTE: The Key Agent exports keys using the Reflection native format by default.
3. (Optional) Select Save in OpenSSH format to save to the format used by OpenSSH servers.

NOTE

- If you want to upload a public key to a Secure Shell server, you can use the Upload button to do this in a single step; you do not need to export the public key first. Reflection automatically determines the correct key format for the server you specify.
- Export Public Key is not available if the Key Agent is locked.

Allow Adding Keys Remotely

You can configure Reflection to add keys to the Reflection Key Agent automatically when you add them to a remote host.
To enable this feature

1. From the Key Agent Options menu, select Allow Adding Keys Remotely.
2. A2D removed a broken link to: reflection_secure_shell_settings_topic_gta in an excluded topic.A2D removed a broken link to: t_24022 in an excluded topic.Open the Reflection Secure Shell Settings dialog box (page 354)
   A2D unwrapped a non-popup link to getting there section: secure_shell_settings_ftp_clienta
   Open the Reflection Secure Shell Settings dialog box.
3. From the User Keys tab, select Allow agent forwarding.

**NOTE:** Agent forwarding must also be enabled on the host.

Allow Deleting Keys Remotely

Index Term
Primary: Key Agent
Secondary: allow deleting keys remotely

Index Term
Primary: agent forwarding (Key Agent)
Secondary: allow deleting keys remotely

You can configure Reflection to remove keys from the Reflection Key Agent automatically when you delete them from a remote host.

To enable this feature

1. From the Key Agent Options menu, select Allow Deleting Keys Remotely.
2. A2D removed a broken link to: reflection_secure_shell_settings_topic_gta in an excluded topic.A2D removed a broken link to: t_24022 in an excluded topic.Open the Reflection Secure Shell Settings dialog box (page 354)
   A2D removed a non-popup link to getting there section: secure_shell_settings_ftp_clienta.
3. From the User Keys tab, select Allow agent forwarding.

**NOTE:** Agent forwarding must also be enabled on the host.

Confirm Remote Private Key Operations

Index Term
Primary: Key Agent
Secondary: confirm private key operations

You can configure whether to have the Key Agent confirm whenever a connection is made using a key in the agent.

To configure remote private key operations

* From the Key Agent Options menu, select or clear Confirm Remote Private Key Operations.

The Key Agent displays a confirmation dialog box whenever a connection is made using a key in the agent; when cleared, a key exchange occurs in the background, and connections are made with no prompting.
Enable Support for SHA256 Signatures

Index Term
Primary: Key Agent
Secondary: enable SHA256

You can configure how the Key Agent presents RSA signatures in response to the Agent Identities Request. When Use Only SHA1 Signatures is enabled (the default), the agent sends only ssh-rsa and x509v3-sign-rsa signatures. When this option is unchecked the agent also sends SHA256 signatures (x509v3-rsa2048-sha256 and ssh-rsa-sha2-256@attachmate.com).

To enable support for SHA256 Signatures

- From the Key Agent Options menu, uncheck Use Only SHA1 Signatures.

**NOTE:** Agent forwarding to some servers may not be supported when this option is unchecked because of the length of the reply to the list request.

Generate Key Dialog Box

Getting there

1. Start the Reflection Key Agent (page 375).
2. Click **Generate Key**.

Secure Shell key authentication uses a public/private (page 889) key pair. From this dialog box, you can create a new key pair and add it to the Key Agent. When you generate keys using the Key Agent, the private key is always kept in encrypted form for use by the Reflection Key Agent only.

The options are:

- **Name**
  - Enter a name to identify this key.

- **Type**
  - Specifies the algorithm used for key generation.

- **Length**
  - Specifies the key size. Up to a point, a larger key size improves security. Increasing key size slows down the initial connection, but has no effect on the speed of encryption or decryption of the data stream after a successful connection has been made. The length of key you should use depends on many factors, including: the key type, the lifetime of the key, the value of the data being protected, the resources available to a potential attacker, and the size of the symmetric key you use in conjunction with this asymmetric key. To ensure the best choice for your needs, we recommend that you contact your security officer.

**NOTE:** Only public keys can be exported from the agent.

Working with the Key Agent

In this Section

- “Key Agent Passphrase” on page 383
- “Change Passphrase Dialog Box” on page 383
- “Lock or Unlock the Key Agent” on page 383
- “Hide and View the Key Agent” on page 384
Key Agent Passphrase

You are prompted for a passphrase (page 383) the first time you use the Key Agent. Use this phrase whenever you need to unlock the agent.

A passphrase is similar to a password, except it can be a phrase with a series of words, punctuation, numbers, white space, or any string of characters you want. Passphrases improve security by limiting access to secure objects, such as private keys and the Reflection Key Agent.

Good passphrases are 10-30 characters long, are not simple sentences or otherwise easily guessable, and contain a mix of upper and lower case letters, numbers, and non-alphanumeric characters. The passphrase is case-sensitive.

NOTE

- Use Change Passphrase (page 383) to change your passphrase.
- There is no way to recover a lost passphrase. If the passphrase is lost or forgotten, you can reset the Key Agent using the Reset button in the Change Passphrase dialog box. When you do this you lose all the keys stored in the agent.

Change Passphrase Dialog Box

Getting there

1. Start the Reflection Key Agent (page 375).
2. Click Change Passphrase.

Use Change Passphrase to change the passphrase (page 383) you use to unlock the Key Agent.

Reset

There is no way to recover a lost passphrase. If the passphrase is lost or forgotten, you can use the Reset button to clear the current passphrase.

NOTE: Using Reset will also destroy all the keys in the agent. If you added keys to the agent using Import, the original keys remain available after a reset, protected by their original passphrase.

Lock or Unlock the Key Agent

When the Agent is locked, you cannot add, modify, or use the Key Agent keys. If you attempt to connect to a host that is configured to use keys in the agent, you will be prompted for your passphrase (page 383).

When you unlock the agent, it remains unlocked until you lock it, shut down the agent, or log off Windows.

To lock the Key Agent

- From Reflection Key Agent, choose the Lock button.
To unlock the Key Agent

- From Reflection Key Agent, choose the Unlock button, and then enter the passphrase (page 383).

-or-

1. Connect to a host that is configured to authenticate using the Key Agent.
2. When prompted, enter the correct passphrase.

**NOTE:** There is no way to recover a lost passphrase. If the passphrase is lost or forgotten, you can reset the Key Agent using the Reset button in the Change Passphrase dialog box. When you do this you lose all the keys stored in the agent.

**Hide and View the Key Agent**

**Index Term**
Primary: Key Agent
Secondary: hiding

**To hide the Key Agent window**

- From the File menu, click Hide. The key agent continues to run in the background.

**NOTE:** Whenever the Key Agent is running, the Key Agent icon is visible in the Windows system tray.

**To view the Key Agent window after it has been hidden**

- Right-click the Key Agent icon, and select Open Reflection Key Agent.

**Stop the Key Agent**

**Index Term**
Primary: Key Agent
Secondary: stopping

Do one of the following:

- From the Key Agent File menu, click Exit.
- Right-click the Key Agent icon in the system tray, then click Exit.
- Log off Windows.

**View the Key Agent Log File**

**Index Term**
Primary: troubleshooting
Secondary: viewing the Key Agent log file

**Index Term**
Primary: log files
Secondary: Reflection Key Agent

From the View menu, choose Log.
Certificate Authentication in Secure Shell Sessions

In this Section

- “PKI and Certificates” on page 385
- “Configure Client Authentication using Certificates” on page 385
- “PKI Tab (Secure Shell Settings)” on page 386

PKI and Certificates

Index Term
Primary: certificate authentication
Secondary: certificates and Secure Shell

A Public Key Infrastructure (PKI) is a system that helps facilitate secure communications through the use of digital certificates. Reflection supports the use of a PKI for both host and user authentication.

Like public key authentication, certificate authentication uses public/private key pairs to verify the host identity. However, with certificate authentication, public keys are contained within digital certificates (page 887), and in this case, two key pairs are used. For example, for server authentication, the host holds one private key and the CA holds a second. The host obtains a certificate from the CA. This certificate contains identifying information about the host, a copy of the host public key, and a “digital signature” on page 892 created using the CA’s private key. This certificate is sent to the client during the authentication process. To verify the integrity of the information coming from the host, the client must have a copy of the CA’s public key, which is contained in the CA root certificate. There is no need for the client to have a copy of the host public key.

Certificate authentication solves some of the problems presented by public key authentication. For example, for host public key authentication, the system administrator must either distribute host keys for every server to each client’s known hosts store, or count on client users to confirm the host identity correctly when they connect to an unknown host. When certificates are used for host authentication, a single CA root certificate can be used to authenticate multiple hosts. In many cases the required certificate is already available in the Windows certificate store.

Similarly, when public keys are used for client authentication, each client public key must be uploaded to the server and the server must be configured to recognize that key. When certificate authentication is used, a single CA root certificate can be used to authenticate multiple client users.

Related Topics

- “Certificate Authentication (PKI)” on page 437
- “Reflection Certificate Manager” on page 446

Configure Client Authentication using Certificates

Index Term
Primary: certificate authentication
Secondary: certificates in Secure Shell sessions

Index Term
Primary: SSL/TLS
Secondary: certificate configuration
Digital certificates (page 887) can be used for either host and/or client "authentication" on page 887 in Secure Shell client sessions. Certificates are not required and are not used by default. This topic describes how to configure the Reflection client for certificate authentication. For information about how to configure the Secure Shell server, consult the server documentation.

To configure certificate authentication on the client

1. Obtain a file that contains your personal certificate and an associated private key (such as a *.pfx or *.p12 file). (You can obtain certificates from a certification authority.)
2. Use this file to import the certificate into the personal tab of either the "Reflection Certificate Manager" on page 446 or the Windows certificate store.
3. From Reflection, open the Reflection Secure Shell Settings dialog box.
4. From the General tab, make sure that Public Key is selected under User Authentication (the default).
5. From the User Keys tab, locate the certificate you want to use from the list of available keys, and then to enable its use, select it in the Use column.

Related Topics
- "Certificate Authentication (PKI)" on page 437

PKI Tab (Secure Shell Settings)

A2D removed a broken link to: reflection_secure_shell_settings_topic_gta in an excluded topic.A2D removed a broken link to: t_24022 in an excluded topic.Getting there (page 354)A2D removed a non-popup link to getting there section: secure_shell_settings_ftp_client[<leave as jump link to support use in both RSIT and R200x>]

Use this tab to configure PKI (page 438) settings for Reflection Secure Shell sessions.

The options are:

- **Certificate host name must match host being contacted**: Specifies whether host name matching is required when validating host certificates. When this setting is enabled (the default), the host name you configure in Reflection must exactly match a host name entered in either the **CommonName** or the **SubjectAltName** field of the certificate.
Use OCSP

Specifies whether Reflection checks for certificate revocation using OCSP (page 888) (Online Certificate Status Protocol) responders when validating host certificates. OCSP responders may be specified in the AIA extension of the certificate itself. You can also specify OCSP responders using the OCSP (page 453) tab in the Reflection Certificate Manager.

Use CRL

Specifies whether Reflection checks for certificate revocation using CRLs (page 887) (Certificate Revocation Lists) when validating host certificates. CRLs may be specified in the CDP extension of the certificate itself. You can also specify CRL using the LDAP (page 451) tab in the Reflection Certificate Manager.

Note: The default value of this setting is based on your current system setting for CRL checking. To view and edit the system setting, launch Internet Explorer, and go to Tools > Internet Options > Advanced. Under Security, look for Check for server certificate revocation.

Reflection Certificate Manager

Opens the Reflection Certificate Manager, which you can use to manage certificates in the Reflection stores and to specify PKI settings.

View System Certificates

Opens the Windows Certificate Manager, which you can use to manage certificates in your system stores.

NOTE

- The settings you configure in this dialog box are saved to the A2D removed a broken link to: t_13406 in an excluded topic.Secure Shell configuration file (page 402). You can also configure Secure Shell settings by editing this file manually in any text editor.
- Within the configuration file, these settings are saved for the currently specified SSH configuration scheme (page 403).

Related Topics

- “PKI and Certificates” on page 385
- “Configure Client Authentication using Certificates” on page 385

GSSAPI (Kerberos) Authentication for Secure Shell Sessions

Index Term
Primary: Kerberos (Secure Shell connections)
Secondary: introduction

In this Section

- “Enable GSSAPI (Kerberos) Authentication for Secure Shell Sessions” on page 388
- “Use Windows SSPI for GSSAPI Authentication” on page 388
- “Use Reflection Kerberos for GSSAPI Authentication” on page 388
- “Specifying the Service Principals for GSSAPI Secure Shell Sessions” on page 389
- “Kerberos Ticket Forwarding in Secure Shell Sessions” on page 389
- “GSSAPI Tab (Secure Shell Settings)” on page 390
Enable GSSAPI (Kerberos) Authentication for Secure Shell Sessions

Kerberos is a security protocol that provides an alternate mechanism for both client and server authentication. Kerberos authentication relies on a trusted third party called the KDC (Key Distribution Center). The Secure Shell protocol supports Kerberos authentication via GSSAPI (Generic Security Services Application Programming Interface).

To enable GSSAPI (Kerberos) authentication

1. Open the Reflection Secure Shell Settings dialog box (page 354). (If you want to ensure that only public key authentication is used, clear the other options.) (The GSSAPI application programming interface is used to obtain Kerberos tickets for ssh2 connections.)

2. On the General tab, select GSSAPI/Kerberos under User Authentication. (If you want to ensure that only public key authentication is used, clear the other options.) (The GSSAPI application programming interface is used to obtain Kerberos tickets for ssh2 connections.)

3. Click the GSSAPI (page 390) tab to configure additional GSSAPI settings.

Use Windows SSPI for GSSAPI Authentication

This procedure configures Reflection to use your Windows domain credentials to authenticate to a Secure Shell server.

To configure Windows SSPI for GSSAPI authentication

1. Open the Reflection Secure Shell Settings dialog box (page 354). (If you want to ensure that only public key authentication is used, clear the other options.) (The GSSAPI application programming interface is used to obtain Kerberos tickets for ssh2 connections.)

2. From the General tab, under User Authentication, select GSSAPI/Kerberos.

3. From the GSSAPI tab, select SSPI.

4. (Optional) Use the Service principal setting to configure connections to hosts that are not in your Windows domain.

NOTE

- You must log into a supported Windows domain (Windows 2000 or later).
- The SSPI setting is supported for Secure Shell protocol version 2 connections only, and the server must support the GSSAPI-with-mic authentication method.

Use Reflection Kerberos for GSSAPI Authentication

Index Term
Primary: Kerberos (Secure Shell connections)
Secondary: how to configure

This procedure configures Reflection Kerberos to use your Windows domain credentials to authenticate to a Secure Shell server. Kerberos authentication for Secure Shell connections is enabled for the currently specified SSH configuration scheme in the Secure Shell configuration file.
If the system administrator has installed a Kerberos configuration file on your PC, Reflection Kerberos is automatically configured the first time you start a Reflection application. Reflection Kerberos settings are stored in the registry on a per-user basis and are available to all Reflection applications that use the Kerberos client.

To use Reflection Kerberos for GSSAPI Authentication

1. A2D removed a broken link to: reflection_secure_shell_settings_topic_gta in an excluded topic. A2D removed a broken link to: t_24022 in an excluded topic. Open the Reflection Secure Shell Settings dialog box (page 354) A2D removed a non-popup link to getting there section: secure_shell_settings_ftp_clienta.

2. On the General tab, select GSSAPI/Kerberos under User Authentication.

3. On the GSSAPI tab, select Reflection Kerberos.

4. Click Configure.

5. In the Initial Configuration dialog box, type the principal name, realm, and KDC host. If your system is already configured for Kerberos, Kerberos Manager starts instead.

NOTE: After authentication, Reflection Kerberos forwards your Kerberos Ticket Granting Ticket (TGT) to the host. To disable ticket forwarding, see “Kerberos Ticket Forwarding in Secure Shell Sessions” on page 389.

Related Topics

- “Specifying the Service Principals for GSSAPI Secure Shell Sessions” on page 389
- “Kerberos Ticket Forwarding in Secure Shell Sessions” on page 389

Specifying the Service Principals for GSSAPI Secure Shell Sessions

The service principal name is the name Reflection uses when it sends a request for a service ticket to the Kerberos Key Distribution Center (KDC). The format is:

hostname.domain.com@REALM

The name Reflection uses depends on settings you can configure on the GSSAPI (page 390) tab of the Secure Shell Settings dialog box. When Use default service principal name is selected (the default), the host name value is the name of the Secure Shell server to which you are connecting and the realm value depends on which GSSAPI provider you have selected:

- If you are using Reflection Kerberos (page 388), the realm name is the one you have specified in your default principal profile.
- If you are using SSPI (page 388), the realm name is your Windows domain name.

Use the Service principal setting to specify a non-default value. If you have selected SSPI as your GSSAPI provider, you can use this setting to specify a service principal in a realm that is different from the Windows domain. Use a fully qualified host name followed by @ then the realm name, for example:

myhost.myrealm.com@MYREALM.COM

Kerberos Ticket Forwarding in Secure Shell Sessions
By default, Reflection forwards your Kerberos Ticket Granting Ticket (TGT) to the host after authentication.

You can disable ticket forwarding using any of the following techniques.

- Clear the **Delegate credentials** setting on the **GSSAPI** (page 390) tab of the **Secure Shell Settings** dialog box. This setting affects only Secure Shell protocol version 2 connections.

- Edit the **Secure Shell configuration file** (page 402). Use one or both of the following lines, depending on which protocol(s) you use. The first line disables ticket forwarding for protocol version 1; the second for protocol version 2.

  ```
  KerberosTgtPassing no
  GssapiDelegateCredentials no
  ```

- To disable ticket forwarding for realms used by your principal profile, use the **Kerberos Manager** (if it is available on your system). While these changes affect Secure Shell sessions that are configured to use Reflection Kerberos, they do not affect sessions configured to use SSPI. Changes you make with the **Kerberos Manager** are ignored if you have configured ticket forwarding using either of the preceding techniques.

**GSSAPI Tab (Secure Shell Settings)**

Index Term
Primary: Secure Shell Settings dialog box
Secondary: GSSAPI tab

Index Term
Primary: Kerberos (Secure Shell connections)
Secondary: GSSAPI tab

A2D removed a broken link to: reflection_secure_shell_settings_topic_gta in an excluded topic.A2D removed a broken link to: t_24022 in an excluded topic.Getting there (page 354)A2D removed a non-popup link to getting there section: secure_shell_settings_ftp_clienta! [<leave as jump link to support use in both RSIT and R200x>]

Use the **GSSAPI** tab of the **Secure Shell Settings** dialog box to specify settings for GSSAPI authentication. Items on this tab are available only if **GSSAPI/Kerberos** is selected in the **User Authentication** list on the **General** (page 355) tab.
The options are:

**SSPI**
Use the Microsoft Security Services Provider Interface (SSPI), which lets you use your Windows domain login credentials to authenticate to the Secure Shell server. This setting simplifies setup, as there is no need to configure the Reflection Kerberos client.

**Reflection Kerberos**
Use the Reflection Kerberos client for Kerberos/GSSAPI authentication. Before you can make connections using the Reflection Kerberos client, you must configure Reflection Kerberos on your computer.

**Configure**
Configures the Reflection Kerberos client. This button is available only when Reflection Kerberos is the selected GSSAPI provider.

**Delegate credentials**
Specifies whether GSSAPI forwards your Kerberos ticket granting ticket (TGT) to the host.

**Use default service principal name**
Specifies the name Reflection uses when it sends a request for a service ticket to the Kerberos Key Distribution Center (KDC). The host name value is the name of the Secure Shell server to which you are connecting. The realm value depends on which GSSAPI provider you have selected.

**Service principal**
Specifies a non-default service principal value.

**Related Topics**
- “Use Reflection Kerberos for GSSAPI Authentication” on page 388
- “Kerberos Ticket Forwarding in Secure Shell Sessions” on page 389
- “Specifying the Service Principals for GSSAPI Secure Shell Sessions” on page 389

**Port Forwarding**

Port forwarding, also known as tunneling, provides a way to redirect communications through the Secure Shell channel of an active session. When port forwarding is configured, all data sent to a specified port is redirected through the secure channel. You can configure either local or remote port forwarding. The terms "local" and "remote" refer to redirected port locations with reference to the Secure Shell client. Reflection supports local port forwarding for both TCP and FTP communications. Remote port forwarding is supported for TCP communications only.

**Terminology**

Port forwarding involves two sets of client and server applications — the Secure Shell client and server, and the client/server pair whose data is being forwarded. In this guide, the following terms are used as defined below in reference to port forwarding:
Use local port forwarding to forward data securely from an application client running on the same computer as the Secure Shell client. When you configure local port forwarding, you designate an arbitrary local port to use for forwarding data, and a destination host and port to receive the data.
Local port forwarding works as follows:

1. When the Secure Shell connection is established, the Secure Shell client opens a listening 
   "socket" on page 891 on the local computer (the one running the Secure Shell client) using the 
designated local port. In most cases, this socket is available only to applications running on the 
Secure Shell client host.

   The gateway ports setting controls whether locally forwarded ports are available to remote 
applications. By default this setting is not enabled, and the client uses the loopback address 
("localhost" or 127.0.0.1) when it opens a socket for local port forwarding. This prevents 
applications running on other computers from connecting to the forwarded port. When you 
enable gateway ports, a remote application client can open a socket using the Secure Shell 
client's Ethernet address (such as an IP address, a URL, or a DNS name). For example, a 
Secure Shell client running on acme.com might be configured to forward port 8088. When 
gateway ports are not enabled, the forwarded socket is localhost:8088. When gateway ports are 
enabled, the forwarded socket is acme.com:8088.

   **CAUTION:** Enabling gateway ports reduces the security of your client host, network, and 
connection because it allows remote applications to use the forwarded port on your system 
without authenticating.

2. An application client is configured to connect to the forwarded port (rather than directly to the 
application server host and port). When that client establishes a connection, all data is sent to 
the listening port, and then redirected to the Secure Shell client.

3. The Secure Shell client encrypts the data and sends it securely through the Secure Shell 
channel to the Secure Shell server.

4. The Secure Shell server receives the data, decrypts it, and redirects it to the destination host and 
port used by the application server.

   **NOTE:** If the final destination host and port are not on the Secure Shell server host, data is sent 
in the clear between the Secure Shell host and the application server host.

5. The return data from the application server is directed to the Secure Shell server, which encrypts 
it and sends it securely to the Secure Shell client through the SSH tunnel. The Secure Shell 
client decrypts the data and redirects it to the original application client.

The general command-line syntax for local port forwarding is:

```
ssh -L listening_port:app_host:hostport user@sshserver
```
The diagrams that follow illustrate two ways to use this.

In the configuration shown above, the application client and the Secure Shell client both run on HostA. The Secure Shell server and application server both run on HostB. All data sent to port 2222 on HostA is forwarded to port 222 on HostB. In this arrangement, all data in transit is securely encrypted. The following command (in which localhost identifies the loopback address on HostB) configures this:

```
ssh -L 2222:localhost:222 user@HostB
```
The following diagram illustrates local port forwarding to a third host. In this configuration, the application server runs on a different host than the Secure Shell server. All data sent to port 2222 on HostA is forwarded to port 222 on HostC.

```
ssh -L 2222:HostC:222 user@HostB
```

**NOTE:** Data sent between HostB and HostC is not encrypted.

**Remote Port Forwarding**

Index Term  
Primary: tunneling  
Secondary: remote port forwarding

Index Term  
Primary: remote port forwarding

Index Term  
Primary: port forwarding  
Secondary: remote port forwarding

Use remote port forwarding to forward data securely from an application client running on the Secure Shell server host. When you configure remote port forwarding, you designate an arbitrary remote port to use for forwarding data and a destination host and port to receive the data.
Remote port forwarding works as follows:

1. When the Secure Shell connection is established, the Secure Shell server opens a listening "socket" on page 891 on the Secure Shell server host using the specified listening port.

2. A client application running on the Secure Shell server host is configured to connect to the listening port (rather than directly to the application server host and port). When that client establishes a connection, all data is sent to the listening port, and then redirected to the Secure Shell server.

3. The Secure Shell server encrypts the data and sends it securely through the SSH tunnel to the Secure Shell client.

4. The Secure Shell client receives data, decrypts it, and redirects it to the destination host and port (on the Secure Shell client host) that is used by the server application.

5. The return data from the server application is directed to the Secure Shell client, which encrypts it and sends it securely to the Secure Shell server through the SSH tunnel. The Secure Shell server decrypts the data and redirects it to the original client application.

The general command-line syntax for remote port forwarding is:

```
ssh -R listening_port:app_host:hostport user@sshserver
```

The diagram that follows illustrates one possible remote port forwarding configuration.

The application server and the Secure Shell client run on HostA. The Secure Shell server and application client both run on HostB. All data sent to port 222 on HostB is forwarded to port 222 on HostA. In this arrangement, all data in transit is securely encrypted. The following command configures this.

```
ssh -R 2222:localhost:222 user@HostB
```

### Forward TCP communications

Use this procedure to encrypt TCP communications that would otherwise be sent in the clear between an application client and server. (Examples given in parentheses configure the Reflection client to send data securely between a Web browser on the computer running Reflection, and a remote Web server.)
To forward TCP communications

1. Open the Reflection client and configure it to connect to your Secure Shell server host (for example, MySSHserver.com).
2. Under Local Forwarding, click Add.
3. For Forward local port, specify any available local port. You can typically enter any value greater than 1024 (for example, 8080). Ports with values less than or equal to 1024 are, by convention, reserved for services and may not be available.
4. Under Destination Host, specify the Name of the application server host (for example, WebServer.Acme.com).
5. For Port, specify the port used by the application server (for example, 80 for a Web server or 110 for a mail server).
6. Connect to the Secure Shell host.

After the Secure Shell connection is established, the application you specified in step 7 will launch. If it is correctly configured to connect to the forwarded local port (8080 in this example), data will be redirected from this port to the server application. The client will run exactly as if it had been configured to connect directly to that server.

Related Topics
- “Forward FTP communications” on page 758
Port forwarding (page 888) allows you to forward TCP/IP traffic through an SSH tunnel. This allows you to use the Reflection Secure Shell Client to secure data that would otherwise be sent over an unsecured TCP/IP channel.

The options are:

- **Tunnel X11 connections**: Specifies that all data sent from a remote X11 port is automatically forwarded through the secure tunnel to the correct local port.

- **Allow gateway ports**: Enables gateway ports. Remote hosts are allowed to connect to local forwarded ports. By default, Reflection Secure Shell binds local port forwardings to the loopback address (this is equivalent to using "localhost"). This prevents other remote hosts from connecting to forwarded ports. **Allow gateway ports** can be used to specify that Reflection Secure Shell should bind local port forwardings to the local ethernet address (such as an IP address, a URL, or a DNS name), thus allowing remote hosts to connect to forwarded ports.

  Be careful about enabling this setting. Using it can reduce the security of your network and connection because it allows remote hosts to use the forwarded port on your system without authenticating.

- **Local forwarding**: Displays local port forwarding you have configured. Click **Add** to open the **Local Port Forwarding** (page 399) dialog box.

- **Remote forwarding**: Displays remote port forwarding you have configured. Click **Add** to open the **Remote Port Forwarding** (page 400) dialog box.

---

**NOTE**

- The settings you configure in this dialog box are saved to the A2D removed a broken link to: reflection_secure_shell_settings_topic_gta in an excluded topic.A2D removed a broken link to: t_13406 in an excluded topic.Secure Shell configuration file (page 402). You can also configure Secure Shell settings by editing this file manually in any text editor.

- Within the configuration file, these settings are saved for the currently specified SSH configuration scheme (page 403).
Local Port Forwarding Dialog Box

Getting there

1. Open the **Reflection Secure Shell Settings** dialog box.
2. Click the **Tunneling** tab.
3. Under **Local Forwarding**, click **Add**.

Use this dialog box to configure A2D unwrapped a broken link to: t_7714 in an excluded topic.local port forwarding. Outgoing data sent to the specified local port is forwarded through the secure tunnel to the specified remote host and port.

You must specify all of the following:

- **Forward local port**: Specify any available port on your PC. Data sent to this port is forwarded through the SSH tunnel.
- **Destination Host Name**: Identify the host computer to which data will be sent. (You can specify `localhost` to forward data to a different port on the same remote host to which you have already established a Secure Shell connection.)
- **Port**: Specify the port on the remote host to which data will be sent. (This box is not available if you select **Tunnel Remote Desktop**, **Reflection** automatically configures the correct remote port.)
- **Forward Type**: Available options are TCP and FTP. Use TCP unless you are forwarding communications between an FTP client and server.

You may also configure the following optional settings:

- **Tunnel Remote Desktop**: Check this box to tunnel a Windows Remote Desktop session. When you select this option, other options become unavailable and **Reflection** automatically configures the correct settings to forward your session.
- **Use Reflection FTP**: This button is visible only when **Forward Type** is set to FTP. When you click it, the values for **Application to Launch** are automatically filled in with the correct values to launch the **Reflection FTP Client** and tunnel your FTP communications.
- **Application to Launch Name**: Enter a name to have **Reflection** automatically launch an application (for example a mail client, FTP client, or web browser) after the Secure Shell connection has been established. To use the secure tunnel, the application must be configured to connect to the port you set for **Forward local port**. With some applications you can do this using command line arguments, which you can specify in the **Arguments** text box.
- **Arguments**: Specify optional command line arguments to use when the specified application is launched.

**NOTE**: Port forwarding settings are saved to the currently specified **SSH configuration scheme** (page 403).

Related Topics

- “Getting to the Reflection Secure Shell Settings Dialog Box” on page 354
Remote Port Forwarding Dialog Box

Getting there

1. Open the Reflection Secure Shell Settings dialog box.
2. Click the Tunneled tab.

Use this dialog box to configure A2D unwrapped a broken link to: t_7715 in an excluded topic. remote port forwarding. Incoming data sent from the specified remote port is forwarded through the secure tunnel to the specified local computer and port.

You must specify all of the following:

**Forward remote server port**
- Specifies a port on a host computer. Data sent from this port is forwarded to the PC through the SSH tunnel.

**Name**
- Identifies the local computer to which data will be sent.

**Port**
- Specifies the port on the local host to which data will be sent.

**NOTE:** Port forwarding settings are saved to the currently specified SSH configuration scheme (page 403).

Related Topics

- "Getting to the Reflection Secure Shell Settings Dialog Box" on page 354

Configure Multi-hop Secure Shell Sessions

Use multi-hop connections when you need to establish secure connections through a series of Secure Shell servers. This is useful if your network configuration doesn't allow direct access to a remote server, but does allow access via intermediate servers. The diagram represents such a series. The Windows workstation needs secure access to ServerC, but cannot connect directly to either ServerB or ServerC. ServerA can connect to ServerB which, in turn, can connect to ServerC.

**Windows workstation ➔ ServerA ➔ ServerB ➔ ServerC**

When you configure a multi-hop list, Reflection creates a secure end-to-end connection by establishing a series of secure tunnels. Each tunnel is established within an existing tunnel, and goes one step further along the chain.

The last server in the chain is the host you specified when you set up your initial Secure Shell connection. Add the other servers in order (top to bottom starting from the client side) to your multi-hop server list. The following procedure describes how to do this.

**To configure multi-hop sessions**

1. Configure a Reflection Secure Shell session to your final destination host (ServerC in this example).
2 A2D removed a broken link to: reflection_secure_shell_settings_topic_gta in an excluded topic.A2D removed a broken link to: t_24022 in an excluded topic.Open the Reflection Secure Shell Settings dialog box (page 354)A2D removed a non-popup link to getting there section: secure_shell_settings_ftp_clienta.

3 Click the Multi-hop tab.

4 Click Add, and then configure the connection to the first multi-hop server in your configuration (ServerA in this example).

   4a For Host name specify the destination host for this hop (ServerA in this example).

   4b (Optional) Specify a value for User name if this host requires a user name that's not the same as the user you specified for your original host connection. (In this example, you would need to specify a user name if ServerA and ServerC require different user names.)

   4c (Optional) Modify the Port value if your host doesn't use port 22 for Secure Shell connections.

   4d (Optional) Click Configure, or specify an SSH configuration scheme (page 403) to use non-default Secure Shell settings for this connection.

   4e Click OK.

5 Click Add again to configure connections to any additional multi-hop servers (ServerB in this example).

NOTE: If you are using this connection to tunnel data for another application (such as a browser or mail client), use the Tunneling (page 398) tab to configure that port forwarding. For example, if your mail server runs on ServerC, after configuring this multihop, you can create a new local port forward as follows: for Local port to forward, specify any unused port (for example 1110), for the remote host Name, enter localhost ("localhost" in this context identifies the last server in the series-ServerC in the example above), and set the Port value equal to your mail server port (usually 110). When the Reflection multihop tunnel is established, you will be able to access the mail server securely by configuring your local mail client to connect to localhost:1110.

Multi-hop Tab (Secure Shell Settings)

Index Term
   Primary: Secure Shell Settings dialog box
   Secondary: Multi-hop tab

Use this tab to configure multi-hop (page 400) Secure Shell sessions.

The options are:

Multi-hop Servers Display the servers in your multi-hop sequence. Reflection establishes a new SSH tunnel to the specified port on the remote server from the specified local port. Each connection on the list is sent through the tunnel established by the connection above it. You can change the list order using the arrow buttons.

Add Add a new server to the list using the Configure Multi-hop Server (page 402) dialog box.

Modify Modify the selected server.

Delete Delete the selected server.
NOTE

- The settings you configure in this dialog box are saved to the A2D removed a broken link to: t_13406 in an excluded topic. Secure Shell configuration file (page 402). You can also configure Secure Shell settings by editing this file manually in any text editor.
- Within the configuration file, these settings are saved for the currently specified SSH configuration scheme (page 403).

Configure Multi-hop Server Dialog Box

Getting there

1. Open the Reflection Secure Shell Settings dialog box.
2. Click the Multi-hop tab.
3. Click Add.

Use this dialog box to add a server to your multi-hop (page 400) list. The options are:

Starting local port
   This is a port on your local Windows workstation. Multi-hop connections are forwarded from the specified port if it is available. If the port is in use, the port number is incremented until an available port is found.

Host name
   Identify the host computer through which data will be sent.

Configure
   Opens the Secure Shell settings dialog box, which you can use to configure non-default settings for this tunnel. Note: An alternate way to configure non-default settings is to specify an SSH config scheme for this connection.

Port
   Specifies a port on the remote host to which data will be sent. The default is 22, which is the port used by most SSH servers.

User name
   (Optional) Specify a name here if this host requires a user name that’s not the same as the one you specified for your original connection.

SSH config scheme
   (Optional) Specify an SSH configuration scheme (page 403) to use for this connection. (Reflection uses the host name by default.)

Related Topics

- “Getting to the Reflection Secure Shell Settings Dialog Box” on page 354

Secure Shell Configuration Files

The Secure Shell configuration files contain settings that are specific to Secure Shell connections.

The Default Configuration File

This default configuration user-specific configuration file is created and updated automatically when you modify your Secure Shell settings using the Reflection Secure Shell Settings dialog box. Settings are saved automatically when you close this dialog box. The filename and location is:

personal_documents_folder\Attachmate\Reflection\.ssh\config
Settings in this file are applied per host (or per SSH configuration scheme (page 403)) and affect terminal sessions and FTP Client sessions. For example, when you use the Reflection Workspace to configure non-default Secure Shell settings for a connection to Acme.com (and you don’t specify an SSH configuration scheme), the Secure Shell settings are saved in the configuration file in a section identified with the following line:

Host Acme.com

If you also configure the FTP Client to connect to Acme.com (and you don’t specify an SSH configuration scheme), the FTP Client uses the settings in the "Host Acme.com" section of the configuration file. (Settings are shared in the same way if you specify the same SSH configuration scheme in both applications.)

Global Configuration File

System administrators can also install a system-wide configuration file. The filename and location is:

common_application_data_folder\Attachmate\Reflection\ssh_config

Settings in this file affect Secure Shell connections for all users of the computer.

**NOTE:** You can edit the configuration files manually in any text editor. Refer to the Configuration File Keyword Reference (page 405) for details. For an example, see “Sample Configuration File” on page 404.

Related Topics

- “Deploy Secure Shell Settings with a Companion Installer” on page 421
- “Configuration File Keyword Reference - Secure Shell Settings” on page 405

### SSH Configuration Schemes

Primary: SSH
Secondary: SSH configuration schemes

Primary: Secure Shell
Secondary: SSH configuration schemes

All Reflection Secure Shell configuration information is saved to your A2D removed a broken link to: Secure Shell configuration file (page 402) using SSH configuration schemes. When you make a Secure Shell connection, Reflection uses the current SSH configuration scheme to determine how the connection should be made. Also, when you make any changes to your settings, Reflection saves those changes to the current SSH configuration scheme.

If you want to configure Secure Shell settings that are specific to a particular host, your SSH configuration scheme name should be the same as your host name.

**NOTE:** If you open the Secure Shell Settings dialog box without specifying a scheme, Reflection automatically creates a new SSH configuration scheme using the currently specified host name as soon as you change any of the Secure Shell settings.
If you want to use the same Secure Shell settings for connections to multiple hosts, enter a
descriptive name for your SSH configuration scheme before you open the **Secure Shell Settings**
dialog box, and then configure the settings you want to save to this scheme. Once you have created
and configured the scheme, you can specify this scheme when you configure subsequent host
sessions.

SSH configuration scheme names are case sensitive.

**How SSH Configuration Schemes are Saved**

Reflection Secure Shell configuration information is saved to your A2D removed a broken link to:
t_13406 in an excluded topic.Secure Shell configuration file (page 402). SSH configuration scheme
names are identified using the **Host** keyword. The configuration file is updated when you close the
**Secure Shell Settings** dialog box. All non-default settings you configure are saved to the current
scheme.

For an example, see "Sample Configuration File" on page 404.

**Related Topics**

- "Secure Shell Configuration Files" on page 402

**Sample Configuration File**

In this sample Secure Shell configuration file, there are two SSH configuration schemes —
**MyHost.Demo.com** and **GeneralSSH**.

The settings under **MyHost.Demo.com** identify a set of Secure Shell settings using an actual host
name. These settings will be used for all connections that specify MyHost.Demo.com as the SSH
configuration scheme, and also for connections to that host when no SSH configuration scheme is
specified.

Because **GeneralSSH** does not identify an actual host address, these settings will only be used if you
specify this SSH configuration scheme when you configure your session.

With this config file, if you configure a connection to a new host (not MyHost.Demo.com) and you
don't specify the **GeneralSSH** scheme, Reflection will connect using the default Secure Shell settings.

```
Host MyHost.Demo.Com
  Protocol 2
  KbdInteractiveAuthentication no
  ChallengeResponseAuthentication no
  PasswordAuthentication no
  RSAAuthentication no
  IdentityFile "C:\SSHusers\Joe\ssh\mykey"
  LogLevel VERBOSE
  #EndHost

Host GeneralSSH
  StrictHostKeyChecking yes
  ServerAlive yes
  #EndHost
```

**Related Topics**

- "Secure Shell Configuration Files" on page 402
- "SSH Configuration Schemes" on page 403
Configuration File Keyword Reference - Secure Shell Settings

Use this reference if you manually edit your Secure Shell configuration file. The configuration file is organized into sections, each identified by a Host keyword. Each section specifies Secure Shell settings to be used for all connections made using the specified host or SSH configuration scheme.

The configuration file consists of keywords followed by values. Configuration options may be separated by white space or by optional white space and exactly one equal sign (=). Keywords are case-insensitive and arguments are case-sensitive.

Any line starting with a number sign (#) is a comment. Any empty line is ignored.

NOTE: Items in this list configure features which affect the Secure Shell connection. Additional keywords are available for configuring terminal emulation for ssh command line sessions. Reference information about these keywords is available in “Configuration File Keyword Reference - Terminal Emulation Settings” on page 416.

AddAuthKeyToAgent

This setting affects how the client handles public key authentication when ForwardAgent is set to ‘yes.’ When public key authentication to the server is successful, and both ForwardAgent and AddAuthKeyToAgent are set to ‘yes’, the key or certificate that was used for authentication is automatically added to the Reflection Key Agent. This key is not saved in the Key Agent, but remains available as long as the Key Agent is running. When AddAuthKeyToAgent is set to ‘no’ (the default), keys and certificates are not automatically added to the Key Agent; it uses only those keys that have already been manually imported.

AuthUseAllKeys

This setting affects how the client handles public key authentication. When this setting is ‘no’ (the default), the client attempts to authenticate using only the key (or keys) you have specified using the IdentityFile keyword. When this setting is ‘yes’ the client attempts to authenticate using all available public keys.

BatchMode

Specifies whether or not to disable all queries for user input, including password and passphrase prompts, which is useful for scripts and batch jobs. The allowed values are ‘yes’ and ‘no’. The default is ‘no’.

NOTE: This keyword does not disable queries for user input when keyboard interactive authentication is configured, but connections that use keyboard interactive will fail when BatchMode is enabled.

BindAddress

Specifies the interface to transmit from on computers with multiple interfaces or aliased addresses.

ChallengeResponseAuthentication

Specifies whether to use challenge response authentication. The argument must be ‘yes’ or ‘no’. This authentication method is recommended if you are using SecurID, PAM authentication, or any other external authentication method that requires prompts from the server and responses from the user. The default is ‘yes’. This applies to SSH protocol version 2 only, which is supported, but not recommended. Use KbdInteractiveAuthentication for SSH protocol version 2.
CheckHostIP

If this flag is set to 'yes', the Reflection Secure Shell Client checks the host IP address in the known_hosts file in addition to checking the host public key. The connection is allowed only if the host IP in the known hosts lists matches the IP address you are using for the connection. The default is 'no'. Note: This setting has no effect if StrictHostKeyChecking = no.

CheckHostPort

If this flag is set to 'yes', the Reflection Secure Shell Client checks the host port in the known_hosts file in addition to checking the host public key. The connection is allowed only if the host port in the known hosts lists matches the port you are using for the connection. The default is 'no'. Note: This setting has no effect if StrictHostKeyChecking = no.

Cipher

Specifies the cipher to use for encrypting the session in protocol version 1. Currently, 'blowfish', '3des', and 'des' are supported. des is only supported by the Secure Shell client for interoperability with legacy protocol 1 implementations that do not support the 3des cipher. Its use is strongly discouraged due to cryptographic weaknesses. The default is '3des'.

Ciphers

Specifies the ciphers allowed for protocol version 2 in order of preference. Multiple ciphers must be comma-separated. The default is 'aes128-ctr,aes128-cbc,aes192-ctr,aes192-cbc,aes256-ctr,aes256-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour128,arcfour256,arcfour'. If the connection is set to run in FIPS mode, the default is 'aes128-ctr,aes128-cbc,aes192-ctr,aes192-cbc,aes256-ctr,aes256-cbc,3des-cbc'.

ClearAllForwardings

Clears any local, remote, or dynamically forwarded ports that have already been processed from either a configuration file or the command line. Note: scp and sftp clear all forwarded ports automatically regardless of the value of this setting. The allowed values are 'yes' and 'no'. The default is 'no'.

Compression

Specifies whether compression is enabled. Compression is desirable on modem lines and other slow connections, but will slow down response rates on fast networks. Compression also adds extra randomness to the packet, making it harder for a malicious person to decrypt the packet. The allowed values are 'yes' and 'no'. The default is 'no'.

CompressionLevel

Specifies the compression level to use if compression is enabled. This option applies to protocol version 1 only. The argument must be an integer from 1 (fast) to 9 (slow, best). The default level is 6, which is good for most applications. The meaning of the values is the same as in gzip.

ConnectionAttempts

Specifies the number of tries (one per second) to make before exiting. The argument must be an integer. This may be useful in scripts if the connection sometimes fails. The default is 1.

ConnectionReuse

Specifies whether multiple sessions to the same host reuse the original Secure Shell connection, and, therefore don't require re-authentication. The argument must be 'yes' or 'no'. When set to 'yes' new connections reuse the existing tunnel when the host name, user name, and SSH configuration scheme (if used) all match. When set to 'no', Reflection establishes a new connection for each session, which means that each new connection repeats the authentication process and also applies any modified connection-specific settings (such as forwards and ciphers). The default is 'yes' for connections made using the Reflection window to make your
connections. It is 'no' if you are using the Reflection A2D unwrapped a broken link to t_5789 in an excluded topic command line utilities to make your connections. For details, see "Connection Reuse in Secure Shell Sessions" on page 360.

**ConnectTimeout**

Specifies the maximum time (in seconds) that the client waits when trying to complete the connection to the server. The timer starts when the connection is established (before logon) and runs during the negotiation of settings, host key exchange, and authentication. For all practical purposes, the timed period is basically the authentication activities. The default is 120.

**DisableCRL**

Specifies whether CRL (Certificate Revocation List) checking occurs when validating host certificates. Setting this to yes disables Certificate Revocation List checking. The default value of this setting is based on your current system setting for CRL checking. To view and edit the system setting, launch Internet Explorer, and go to Tools > Internet Options > Advanced. Under Security, look for "Check for server certificate revocation."

**DynamicForward**

Specifies that a TCP/IP port on the local machine be forwarded over the secure channel, and the application protocol is then used to determine where to connect to from the remote machine. The argument must be a port number. Currently the SOCKS4 protocol is supported, and Reflection Secure Shell will act as a SOCKS4 server. Multiple forwardings may be specified, and additional forwardings can be given on the command line. Only a user with administrative privileges can forward privileged ports.

**EscapeChar**

Sets the escape character (default: `~`). The escape character can also be set on the command line. The argument must be a single character, `^` followed by a letter, or 'none' to disable the escape character entirely (making the connection transparent for binary data).

**FipsMode**

When this setting is 'yes' connections must be made using security protocols and algorithms that meet United States government's Federal Information Processing Standard (FIPS) 140-2. Options that don't meet these standards are not available on the Encryption tab.

**NOTE:** This setting affects the SSH configuration scheme specified by the Host keyword, and has no effect on subsequent Secure Shell sessions unless they are configured to use the same SSH configuration scheme (or host name).

**ForwardAgent**

Setting this to 'yes' enables forwarding of the Reflection Key Agent connection. Agent forwarding should be enabled with caution. Users with the ability to bypass file permissions on the remote host (for the agent's Unix-domain socket) can access the local agent through the forwarded connection. Attackers cannot obtain key material from the agent, however they can perform operations on the keys that enable them to authenticate using the identities loaded into the agent. This may need to be enabled on the server also. The default is 'no'.

**ForwardX11**

Specifies whether X11 connections are automatically redirected over the secure channel and DISPLAY set. The argument must be 'yes' or 'no'. The default is 'no'. (Note: If you configure Secure Shell using Reflection X, see ForwardX11ReflectionX.)
ForwardX11ReflectionX

This setting is used only if you are configuring Secure Shell connections for Reflection X (starting with 14.1). It specifies whether X11 connections are automatically redirected over the secure channel and DISPLAY set. The argument must be "yes" or "no". The default is "yes".

GatewayPorts

Specifies whether remote hosts are allowed to connect to local forwarded ports. By default, Reflection Secure Shell binds local port forwardings to the loopback address. This prevents other remote hosts from connecting to forwarded ports. GatewayPorts can be used to specify that Reflection Secure Shell should bind local port forwardings to the wildcard address, thus allowing remote hosts to connect to forwarded ports. Be careful about enabling this setting. Using it can reduce the security of your network and connection because it can allow remote hosts to use the forwarded port on your system without authenticating. The argument must be 'yes' or 'no'. The default is 'no'.

GlobalKnownHostsFile

Specifies a file to use for the global host key database instead of the default file named ssh_known_hosts located in the "Reflection application data folder" on page 891.

NOTE: Enclose the filename in quotation marks if any part of the path or filename includes spaces.

GssapiAuthentication

Specifies whether GSSAPI authentication is used to authenticate to a Kerberos KDC. This setting is applicable only if the protocol being used is protocol version 2. (The equivalent setting for protocol version 1 is KerberosAuthentication.) The allowed values are 'yes' and 'no'. The default is 'no'.

GssapiDelegateCredentials

Specifies whether GSSAPI is used to forward your ticket granting ticket (krbtgt) to the host. This setting is applicable only if the protocol being used is protocol version 2. (The equivalent setting for protocol version 1 is KerberosTgtPassing.) The allowed values are 'yes' and 'no'. The default is 'yes'.

GssapiUseSSPI

Specifies whether Microsoft's Security Support Provider Interface (SSPI) is used for GSSAPI authentication. This setting is applicable only if Kerberos/GSSAPI authentication is enabled (using GssapiAuthentication for protocol version 2 and KerberosAuthentication for protocol version 1). The argument to this keyword must be 'yes' or 'no'. When set to 'no' the Reflection Secure Shell Client uses the Reflection Kerberos Client for GSSAPI authentication. When set to 'yes' the Reflection Secure Shell Client uses your Windows domain login credentials (SSPI) to authenticate to the Secure Shell server. SSPI is supported for protocol version 2 connections only, and the server must support the GSSAPI-with-mic authentication method. The default is 'yes'.

GssServicePrincipal

Specifies a non-default service principal name to use when the client sends a request for a service ticket to the Kerberos Key Distribution Center (KDC). If you have selected SSPI for your GSSAPI provider, you can use this setting to specify a service principal in a realm that is different from the Windows domain. Use a fully qualified host name followed by @ then the realm name, for example myhost.myrealm.com@MYREALM.COM. (By default the hostname value is the name of the Secure Shell server to which you are connecting and the realm depends upon the value of GssapiUseSSPI. When GssapiUseSSPI is 'no' the realm name is specified in your default principal profile. When GssapiUseSSPI is 'yes', the realm is your Windows domain name.)
Host
Identifies the declarations that follow (up to the next Host key word) as belonging to the specified SSH configuration scheme (page 403). The characters ‘*’ and ‘?’ can be used as wildcards. A single ‘*’ as a pattern can be used to provide global defaults for all hosts. A Reflection connection will use the first occurrence of any matching Host string (including wildcard characters). Any subsequent matches will be ignored.

NOTE: When you close the Reflection Secure Shell Settings dialog box, values with default settings are not saved to the configuration file. If a default value has been manually added to the file, it is removed when you close the dialog box. This imposes design constraints if you use wildcard host stanzas in combination with stanzas that use specific host names. If you have manually configured a default value in a specific host stanza that is meant to override a value configured in a wildcard stanza, the default setting is removed when you open the Secure Shell settings dialog box to view settings for the host-specific SSH configuration scheme. You can successfully handle this situation by using the global configuration file, which is not updated when users open and close the Reflection Secure Shell Settings dialog box.

HostKeyAlgorithms
Specifies, in order of preference, the host key algorithms that the client uses. The default for this option is: "x509v3-rsa2048-sha256, x509v3-sign-rsa, x509v3-sign-dss, ssh-rsa-sha2-256@attachmate.com, ssh-rsa,ssh-dss". This setting is useful when the server is configured for both certificate and standard host key authentication. The default value presents x509 algorithms before regular SSH key algorithms. SSH protocol allows only one attempt to authenticate the host. (This is different from user authentication in which multiple authentication methods and attempts are supported.) If the host presents a certificate, and the client is not configured for host authentication using certificates, the connection will fail when x509 algorithms are preferred. In this situation you can configure the client to prefer SSH keys over certificates by changing the order of preference to "ssh-rsa-sha2-256@attachmate.com, ssh-rsa,ssh-dss, x509v3-rsa2048-sha256, x509v3-sign-rsa, x509v3-sign-dss".

HostKeyAlias
Specifies an alias to be used instead of the real host name for looking up or saving the host key in the host key database files. This option is useful for tunneling ssh connections or for multiple servers running on a single host.

IdentityFile
Specifies a private key to use for key authentication. Files are located in the user .ssh folder (page 891). IdentityFile items are added when you select keys or certificates from the list in the User Keys tab of the Secure Shell settings dialog box. It is possible to have multiple identity files specified in configuration files; all these identities will be tried in sequence.

NOTE: Enclose the full path name in quotation marks if it includes spaces.

KbdInteractiveAuthentication
Specifies whether to use keyboard interactive authentication. The allowed values are ‘yes’ and ‘no’. The default is ‘yes’. This authentication method is recommended if you are using SecurID, PAM authentication, or any other external authentication method that requires prompts from the server and responses from the user. It may also work better than the PasswordAuthentication method for password authentication on hosts where password expiration or first login password changing is enabled. It may also be required for password authentication when expired passwords need to be reset in order to successfully authenticate. This applies to SSH protocol 2 only. Use ChallengeResponseAuthentication for SSH protocol version 1.
KeepAlive

Specifies whether the system should send TCP keepalive messages to the other side. If they are sent, death of the connection or crash of one of the machines will be detected. The default is 'yes' (to send keepalives), so that the client will detect that the network goes down or the remote host dies. This is important in scripts and helpful to users. However, this means that connections will die if the route is down temporarily, which some users find annoying. To disable keepalives, set the value to 'no'. This keyword enables the Windows TCP keep alive setting, which sends keep alive messages every two hours by default. TCP/IP keep alive is configurable using two optional parameters that typically do not exist in the Windows registry: KeepAliveTime and KeepAliveInterval. These are configured in the HKEY_LOCAL_MACHINE registry subtree, in the following location:

SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

For information about setting these parameters, refer to Microsoft Knowledge Base Article 120642.

KerberosAuthentication

Specifies whether Kerberos authentication is used for protocol version 1 connections. (The equivalent setting for protocol version 2 is GssapiAuthentication.) The argument to this keyword must be 'yes' or 'no'.

KerberosTgtPassing

Specifies whether a Kerberos TGT is forwarded to the server. This will work only if the Kerberos server is actually an AFS kaserver. This setting applies to protocol version 1 only. (The equivalent setting for protocol version 2 is GssapiDelegateCredentials.) The argument to this keyword must be 'yes' or 'no'.

KexAlgorithms

Specifies which key exchange algorithms the client supports, and the order of preference. The supported values are 'diffie-hellman-group1-sha1', 'diffie-hellman-group-exchange-sha1' and 'diffie-hellman-group14-sha1'. The default is 'diffie-hellman-group1-sha1,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1'. In some cases, you may need to change the order of the key exchange algorithms to put 'diffie-hellman-group14-sha1' ahead of the other two. This is required if you want use the hmac-sha512 MAC, or if you see the following error during key exchange: "fatal: dh_gen_key: group too small: 1024 (2^need 1024)".

NOTE: If GSSAPI authentication using the Reflection Kerberos Client is enabled, then the following additional key exchange algorithms are automatically added to the list: gss-group1-sha1 and gss-gex-sha1.

LocalForward

Specifies that a TCP/IP port on the local machine be forwarded over the secure channel to the specified host and port on the remote machine. Multiple forwardings can be specified. Only users with administrator privileges can forward privileged ports. You can also configure optional arguments for forwarding FTP, configuring remote desktop, and automatically launching an executable file (*.exe) after the connection is made. The syntax for this keyword is:

LocalForward localport host:hostname [FTP=0|1] [RDP=0|1] ["ExecutableFile" [args]]
The options are:

- **localport**
  - A local port number.

- **host:hostport**
  - A remote host and a port on that host. (You can specify localhost to forward data to a different port on the same remote host to which you have already established a Secure Shell connection.) IPv6 addresses can be specified with an alternative syntax: host/port.

- **FTP**
  - Set to 1 if you are tunneling FTP file transfer.

- **RDP**
  - Set to 1 if you are tunneling a Remote Desktop session.

- **"ExecutableFile"**
  - Specify an executable file (including complete path information, if required) to have Reflection launch an application immediately after the Secure Shell connection is established. To forward data through the secure tunnel, this application should be configured to make a connection to localhost (or the loopback IP address, 127.0.0.1) using the specified localport.

### Logfile

Specifies a log file to use for debugging. All session input and output is written to this file. Use this keyword with the -o command-line utility option as shown here:

```
-o Logfile=\path\logfile_name
```

**NOTE:** Enclose the path filename in quotation marks if any part of the path or filename includes spaces.

### LogLevel

Specifies the verbosity level that is used when logging messages from the Reflection Secure Shell Client. The possible values are: QUIET, FATAL, ERROR, INFO, VERBOSE, DEBUG, DEBUG1, DEBUG2 and DEBUG3. The default is INFO. DEBUG and DEBUG1 are equivalent. DEBUG2 and DEBUG3 each specify higher levels of verbose output.

### Macs

Specifies the MAC (message authentication code) algorithms in order of preference. The MAC algorithm is used in protocol version 2 for data integrity protection. Multiple algorithms must be comma-separated. The default is: "hmac-sha256, hmac-sha2-256, hmac-sha1, hmac-md5, hmac-ripemd160, hmac-sha1-96, hmac-md5-96, hmac-sha512, hmac-sha2-512." If the connection is set to run in FIPS mode, the default is "hmac-sha256, hmac-sha2-256, hmac-sha1, hmac-sha512, hmac-sha2-512".

### MatchHostName

Specifies whether host name matching is required when validating host certificates. When this setting is 'yes' (the default), the host name you configure in Reflection must exactly match a host name entered in either the CommonName or the SubjectAltName fields of the certificate.

### MultiHop

Configures multi-hop (page 400) connections, which can be used to establish secure connections through a series of SSH servers. This is useful if your network configuration doesn't allow direct access to a remote server, but does allow access via intermediate servers.

The syntax for this keyword is:

```
MultiHop localport host:hostport ["SSH config scheme"]
```
Add a new Multihop line for each server in the series. Each connection on the list is sent through the tunnel established by the connection above it.

In the example below, SSH connections configured to ServerC will connect first to ServerA, then to ServerB, and finally to the ServerC.

Host ServerC
Multihop 2022 ServerA:22
Multihop 3022 ServerB:22

You can optionally specify an SSH configuration scheme (page 403) to configure Secure Shell settings for any host in the chain. For example:

Multihop 4022 joe@ServerA:22 "Multihop SchemeA"

NoShell
When NoShell is set to "Yes", the client creates a tunnel without opening a terminal session. This option can be used in combination with ConnectionReuse to create a tunnel that can be reused by other ssh connections. Note: This option affects connections made with the command line utility; it is not intended for use with the Reflection user interface.

NumberOfPasswordPrompts
Specifies the number of password prompts before giving up. The argument to this keyword must be an integer. The default is 3.

PasswordAuthentication
Specifies whether to use password authentication. The allowed values are 'yes' and 'no'. The default is 'yes'.

Port
Specifies the port number to connect on the remote host. The default is 22.

PreferredAuthentications
Specifies the order in which the client should try protocol 2 authentication methods. This corresponds to the order (top to bottom) in which the methods are displayed in the User Authentication list on the General tab of the Reflection Secure Shell Settings dialog box. This setting enables the client to prefer one method (such as keyboard-interactive) over another method (such as password). By default, Reflection attempts authentication in the following order: 'publickey,keyboard-interactive,password'. If GSSAPI authentication is enabled, the default changes to: 'gssapi-with-mic,external-keyex,gssapi,publickey,keyboard-interactive,password'.

NOTE

- If you include PreferredAuthentications in your config file, the list you specify must include every authentication method you want to try. If PreferredAuthentications is present, but does not specify a particular authentication method, Reflection will not use that authentication method, even if the keyword for enabling that authentication method is correctly configured.

- Including an authentication method in the PreferredAuthentications list does not enable authentication using that method. To enable an authentication method that is not used by default, the keyword for that authentication method must also be correctly configured (for example, to enable GSSAPI authentication, you must set GssapiAuthentication to yes.)
PreserveTimestamps
Specifies whether file attributes and timestamps are modified when files are transferred to and from the server. When this keyword is "no" (the default), timestamps and attributes are modified. When it is "yes", the files retain their original timestamps and attributes.

Protocol
Specifies the protocol versions the Reflection Secure Shell Client should support in order of preference. The possible values are '1' and '2'. Multiple values must be comma-separated. The default is '2,1', which means that Reflection tries version 2 and falls back to version 1 if version 2 is not available.

Proxy
Specifies a proxy type to use for Secure Shell connections. Supported values are "SOCKS" and "HTTP".

**NOTE:** Proxy use is enabled for each Host section in the configuration file using this setting. The proxy server address is stored in the Windows registry on a per-user basis.

PubkeyAuthentication
Specifies whether to try public key authentication. This option applies to protocol version 2 only. The allowed values are 'yes' and 'no'. The default is 'yes'.

RemoteCommand
Specifies one or more commands to run on the remote server. Use a semicolon (;) to separate multiple commands when connecting to a UNIX server. Use an ampersand (&) to separate commands when connecting to a Windows server. After a connection is established the server executes (or attempts to execute) the specified command(s), and then the session terminates. The server must be configured to allow commands received from the client to run.

The commands must be specified using the correct syntax for your server. For example, the following are equivalent:

On UNIX: `ls ; ls -l`
On Windows: `dir/w & dir`

RemoteForward
Specifies that a TCP/IP port on the remote machine be forwarded over the secure channel to the specified host and port from the local machine. The first argument must be a port number, and the second must be host:port. IPv6 addresses can be specified with an alternative syntax: host/ port. Multiple forwardings may be specified. Only the users with administrator privileges can forward privileged ports.

RSAAuthentication
Specifies whether to try RSA authentication. This option applies to protocol version 1 only. RSA authentication will only be attempted if the identity file exists. The allowed values are 'yes' and 'no'. The default is 'yes'.

SendEnv
Specifies an environment variable to set on the server before executing a shell or a command. The value should be of form: VAR val. The server must support the specified variable, and must be configured to accept these environment variables.
ServerAlive

Specifies whether to send server alive messages to the SSH server at the interval specified by ServerAliveInterval. The Secure Shell ServerAlive setting sends an SSH protocol message to the server at the specified interval to ensure that the server is still functioning. If this is setting is not enabled, the SSH connection will not terminate if the server dies or the network connection is lost. This setting can also be used to keep connections that only forward TCP sessions from being timed out by the server, as the server may timeout these connections because it detects no SSH traffic. The allowed values are 'yes' and 'no'. The default is 'no'.

NOTE: The Secure Shell ServerAlive setting is not related to the TCP keep alive setting (KeepAlive) that can be set in the Windows registry to keep all TCP/IP connections from being timed out by a firewall. To change the TCP/IP keep alive behavior, you need to edit the Windows registry.

ServerAliveInterval

Specifies the interval (in seconds) to use when ServerAlive = 'yes'. Use an integer value of one or greater. The default is 30.

SftpBufferLen

Specifies the number of bytes requested in each packet during SFTP transfers. The default is 32768. Adjusting this value can improve transfer speed. The optimum value depends on your network and server setup. Changing this value may also affect how quickly you can cancel a transfer.

SftpMaxRequests

Specifies the maximum number of outstanding data requests that the client will allow during SFTP transfers. The default is 10. Adjusting this value can improve transfer speed. The optimum value depends on your network and server setup. Changing this value may also affect how quickly you can cancel a transfer.

SftpVersion

Specifies which version the client uses for SFTP connections. Valid values are 3 and 4. When this setting is 4 (the default), the connection uses SFTP version 4 if the server supports it, and drops to version 3 if the server doesn't support version 4. If this setting is 3, the client always uses SFTP version 3. Note: If you require SFTP 4, check with Attachmate technical support to confirm that this setting is available with your version of the Reflection client. [Remove this note when mamba ships - Rita 12/28/10]

StrictHostKeyChecking

The argument must be 'yes', 'no' or 'ask'. The default is 'ask'. If this option is set to 'yes', the Reflection Secure Shell Client never automatically adds host keys to the known_hosts file (located in the user .ssh folder (page 891)), and refuses to connect to hosts whose host key has changed. This option forces the user to manually add all new hosts. If this flag is set to 'no', Reflection connects to the host without displaying a confirmation dialog box, and does not add the host key to the list of trusted keys. If this flag is set to 'ask', new host keys are added to the user known host files only after the user has confirmed that is what they want. The host keys of known hosts are verified automatically in all cases.

NOTE: This setting has no effect when the host has been configured to authenticate using x509 certificates. If a host presents a certificate for host authentication and you do not have the required CA certificate configured as a trust anchor, the connection will fail.
TryEmptyPassword

If this flag is set to 'yes', the client starts the password authentication by trying to enter an empty password. Note that this will count as a login attempt on most systems.

User

Specifies the user to log in as. This can be useful when a different user name is used on different machines.

UseOCSP

Specifies whether the client uses OCSP (Online Certificate Status Protocol) to validate host certificates. The allowed values are 'yes' and 'no'. The default is 'no'.

UserKeyCertLast

Specifies how the Reflection client handles the signature for certificates during public key authentication. When this setting is 'yes' (the default), the client sends the certificate using a standard ssh key signature first (ssh-rsa or ssh-dss). If that fails, the client tries again using a certificate signature (x509-sign-rsa or x509-sign-dss). In some cases this second attempt may not occur and authentication fails. When this setting is 'no', the client tries the certificate signature first followed by the ssh key signature.

UserKnownHostsFile

Specifies a file to use for the user host key database instead of the known_hosts file (located in the user .ssh folder (page 891)). Use quotation marks if the file or path includes spaces.

x509dsasigtype

Specifies the hash algorithm the client uses in the process of proving possession of DSA private keys. Possible values are 'sha1raw' (the default) and 'sha1asn1'.

x509rsasigtype

Specifies the hash algorithm the client uses in the process of proving possession of RSA private keys. Possible values are 'md5', 'sha1' (the default), and 'sha256'.

X11Display

Determines the port on the PC's local loopback interface to which X11 protocol communications are forwarded when X11 forwarding is enabled.

NOTE: If you are using Reflection X (version 12.x, 13.x, or 14.x), you don’t need to configure this keyword. The Reflection X server and Reflection Secure Shell client automatically synchronize to use the correct port based on your X server display setting (Settings > Display > X display number); in this case the X11Display keyword is ignored. If you use a different PC X server, use this keyword to specify the correct listening port as defined for your PC X server.

The default value is 0. This configures forwarding to port 6000, which is the default listening port defined by X11 protocol convention. The display value you specify is added to 6000 to determine the actual listening port. For example, setting X11Display to 20 indicates to the Secure Shell client that the PC-X server is listening on port 6020.

Related Topics

* “Configuration File Keyword Reference - Terminal Emulation Settings” on page 416
Configuration File Keyword Reference - Terminal Emulation Settings

Items in this list configure terminal emulation settings for Reflection ssh (page 423) and A2D unwrapped a broken link to: t_7879 in an excluded topic.ssh2 command line sessions. These settings can be implemented by adding them manually to the Secure Shell A2D removed a broken link to: t_13406 in an excluded topic.configuration file (page 402), or by using the -o switch on the command line.

NOTE: These settings affect command line terminal sessions only; they have no affect on terminal sessions running in the Reflection user interface.

The configuration file is organized into sections, each identified by a Host keyword. Each section specifies settings to be used for all connections made using the specified host or SSH configuration scheme (page 403).

The configuration file consists of keywords followed by values. Configuration options may be separated by white space or by optional white space and exactly one equal sign (=). Keywords are case-insensitive and arguments are case-sensitive.

Any line starting with a number sign (#) is a comment. Any empty line is ignored.

Quotation marks are required around string arguments that include spaces. Terminal emulation keywords and arguments are not case-sensitive.

NOTE: Keywords for configuring Secure Shell connections are available in a separate list. See “Configuration File Keyword Reference - Secure Shell Settings” on page 405.

AnswerBackMessage

When AutoAnswerback is set to ‘yes’, AnswerBackMessage specifies the string that is sent to the host in response to an answerback request (the ENQ character-ASCII 5).

Possible String Values: A string value of up to 30 characters.
Default: "" (null string)
Sample syntax:

AutoAnswerback yes
AnswerbackMessage "My answer back string"

AutoAnswerback

When AutoAnswerback is set to yes, the message string specified using the AnswerBackMessage keyword is automatically sent to the host after a connection is made.

Possible Values: yes or no
Default: no
Sample syntax:

AutoAnswerback yes
AnswerbackMessage "My answer back string"

AutoWrap

Determines what happens when the cursor reaches the right margin. When set to yes, characters will wrap to the next line automatically when the cursor reaches the right margin of the terminal window. When set to no, the cursor is not automatically advanced when it reaches the right margin—as you type additional characters, each character overwrites the previous character until you move the cursor.

Possible Values: yes or no
AutoWrap yes

**BackspaceKeyIsDel**
Specifies the behavior of the backspace key. When set to no, the backspace key transmits a backspace (ASCII 8) character. When set to yes, the backspace key transmits the delete (ASCII 127) character.

Possible Values: yes or no
Default: no
Sample syntax:
BackspaceKeyIsDel yes

**CursorKeyMode**
Specifies how the client handles keys on the cursor keypad. When set to no, the cursor keypad is set to normal mode-the cursor keypad keys transmit cursor escape sequences. When set to yes, the cursor keypad is set to application mode-cursor keypad keys will transmit application escape sequences.

Possible Values: yes or no
Default: no
Sample syntax:
CursorKeyMode yes

**CursorStyle**
Specifies the cursor style.

Possible String Values: Block, Blockblink, Line, Lineblink
Default: Lineblink
Sample syntax:
CursorStyle Block

**CursorVisible**
Specifies whether the cursor is visible. When set to no, the cursor is not visible in the terminal window.

Possible Values: yes or no
Default: yes
Sample syntax:
CursorVisible no

**DisplayCols**
Sets the number of columns in the terminal window.

Possible Values: The minimum is 80. The maximum usable value depends on your monitor size and display settings.
Default: Determined by the current command window size.
Sample syntax:
DisplayCols 120

**DisplayRows**
Sets the number of rows in the terminal window.
**Possible Values:** The minimum is 24. The maximum usable value depends on your monitor size and display settings.
**Default:** Determined by the current command window size.
**Sample syntax:**
```plaintext
DisplayRows 30
```

**HostCharacterSet**

Specifies a non-default host character set.

**Possible String Values:**

- **PC437_English**
- **PC737_Greek**
- **PC775_Baltic**
- **PC850 Multilingual**
- **PC852_Slavic**
- **PC855_Cyrillic**
- **PC857_Turkish**
- **PC858 Multilingual_Euro**
- **PC860_Portuguese**
- **PC861_Icelandic**
- **PC862_Hebrew**
- **PC863_CanadianFrench**
- **PC864_Arabic**
- **PC865_Nordic**
- **PC866_Cyrillic**
- **PC869_ModernGreek**
- **PC932_Shift_JIS**
- **PC936_SimplifiedChinese**
- **PC949_Korean**
- **PC950_TraditionalChinese**
- **DECMultinational**
- **UCS2**
- **Windows1250**
- **Windows1251**
- **Windows1252**
- **Windows1253**
- **Windows1254**
- **Windows1255**

**Default:** PC437_English

**Sample syntax:**
```plaintext
HostCharacterSet EUC_Japanese
```

**InsertMode**

Specifies whether typing is in insert or replace mode. When set to no, typing replaces existing characters at the cursor location. When set to yes, new characters are inserted at the cursor location, and existing characters are moved to the right.

**Possible Values:** yes or no

**Default:** no
Sample syntax:
InsertMode yes

**InverseVideo**
Specifies whether the terminal window uses inverse video. When set to yes, foreground and background colors for all screen attributes are reversed.

Possible Values: yes or no
Default: no
Sample syntax:
InverseVideo yes

**KeyBoardActionMode**
Specifies whether the keyboard is available. When set to yes, the keyboard is locked and cannot be used.

Possible Values: yes or no
Default: no
Sample syntax:
KeyBoardActionMode yes

**MarginBell**
Determines whether a margin bell sounds. When set to yes, the bell sounds when the cursor is eight characters from the right margin. Set this setting to no to prevent sounding the margin bell.

Possible Values: yes or no
Default: yes
Sample syntax:
MarginBell no

**NewLine**
Specifies whether the client is in linefeed or newline mode. When set to no (linefeed mode), pressing the Enter key sends only a carriage return. Received linefeeds, formfeeds, and vertical tabs move the cursor down one line in the current column. When set to yes (newline mode), pressing the Enter key sends both a carriage return and a linefeed. Received formfeeds, and vertical tabs move the cursor to the first column of the next line.

Possible Values: yes or no
Default: no
Sample syntax:
NewLine yes

**NRCSet**
Use one of the supported string values to specify a different National Replacement Character set. You must also set the UseNRC keyword to yes to enable this.
Possible String Values:

<table>
<thead>
<tr>
<th>British</th>
<th>Norwegian</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finnish</td>
<td>Portuguese</td>
</tr>
<tr>
<td>French</td>
<td>EuropeanSpanish</td>
</tr>
<tr>
<td>CanadianFrench</td>
<td>Swedish</td>
</tr>
<tr>
<td>German</td>
<td>SwissGerman</td>
</tr>
<tr>
<td>Italian</td>
<td></td>
</tr>
</tbody>
</table>

Default: ASCII
Sample syntax:

```plaintext
UseNRC yes
NRCSets British
```

**NumericKeypadMode**

Specifies how the client handles the keys on the numeric key pad. When set to yes, the keypad is set to numeric mode — the keypad keys transmit numeric values when pressed. When set to no, the keypad is set to application mode — the keypad keys transmit application escape sequences such as home, up, and right.

Possible Values: yes or no
Default: no
Sample syntax:

```plaintext
NumericKeypadMode no
```

**OriginMode**

Specifies the cursor’s home position. When set to no, the cursor’s home position is at the upper-left hand corner of the terminal window. When set to yes the cursor’s home position is relative to the terminal windows margin settings.

Possible Values: yes or no
Default: no
Sample syntax:

```plaintext
OriginMode yes
```

**SevenBitControls**

Specifies how 8-bit C1 control codes are transmitted. When set to yes, 7-bit equivalents are transmitted for the 8-bit C1 control codes. When set to no, 8-bit C1 control codes are transmitted.

**NOTE:** The default value for HostCharacterSet for the ssh command line client is PC437_English. If you want to send C1 controls, you need to set HostCharacterSet to DECMultinational or one of the ISOLatin character sets.

Possible Values: yes or no
Default: yes
Sample syntax:

```plaintext
SevenBitControls no
```

**TerminalModel**

Specifies which terminal type the client emulates.

Possible String Values: vt52, vt102, vt220
Default: vt220
Sample syntax:

TerminalModel vt102

UseNRC
When this is set to yes, you can specify a National Replacement Character set using the NRCSet keyword.

Possible Values: yes or no
Default: no
Sample syntax:

UseNRC yes
NRCSet British

UseANSIColor
When set to yes, ANSI color escape sequences are supported.

Possible Values: yes or no
Default: yes
Sample syntax:

UseANSIColor no

WarningBell
Specifies whether a warning bell sounds. When set to yes, the bell sounds when a bell character (ASCII 7) is received from the host or entered from the keyboard. Set this setting to no to prevent sounding the warning bell.

Possible Values: yes or no
Default: yes
Sample syntax:

WarningBell no

Related Topics
• “Configuration File Keyword Reference - Secure Shell Settings” on page 405

Deploy Secure Shell Settings with a Companion Installer

Index Term
Primary: administrative installation
Secondary: deploy Secure Shell settings

System administrators can use the Attachmate Customization Tool to deploy Secure Shell settings to end users. You can specify both user-specific and global locations for installing files.

NOTE: For names and locations of configuration files used by Secure Shell sessions, see the lists that follow the procedure

To create a companion package to install Secure Shell settings

1 Configure the Secure Shell settings you want to deploy.
2 Create an administrative installation of InfoConnect (or use an existing one).
3 From your administrative installation point, open the Attachmate Customization Tool from an A2D unwrapped a broken link to: act_setup_shortcut in an excluded topic shortcut or by typing the following command line:

<path_to_setup>\setup.exe /admin

4 From the Select Customization dialog box, select Create a new Companion installer (or open an existing MSI), and then click OK.

5 From the navigation pane, select Specify install locations.

6 Under Installation type, specify either Installs to all users of a machine or Installs only for the user who installs it.

7 From the navigation pane, select Add files.

8 Under Add files to, specify a destination location. Refer to the lists that follow this procedure.

9 Click Add, browse to locate the file you want to add to the installation, then click Open.

10 Click File > Save As and enter a name for your installer file (for example SecureShellSettings.msi).

User-specific files and locations

<table>
<thead>
<tr>
<th>File Name</th>
<th>Add File To</th>
</tr>
</thead>
<tbody>
<tr>
<td>config</td>
<td>[PersonalFolder]\Attachmate\Reflection.ssh</td>
</tr>
<tr>
<td>known_hosts</td>
<td>[PersonalFolder]\Attachmate\Reflection.ssh</td>
</tr>
<tr>
<td>NOTE:</td>
<td>For information about this file, see A2D removed a broken link to: t_13406 in an excluded topic. “Secure Shell Configuration Files” on page 402.</td>
</tr>
<tr>
<td>pki_config</td>
<td>[PersonalFolder]\Attachmate\Reflection.pki</td>
</tr>
<tr>
<td>NOTE:</td>
<td>This file configures Reflection Certificate Manager settings.</td>
</tr>
<tr>
<td>trust_store.p12</td>
<td>[PersonalFolder]\Attachmate\Reflection.pki</td>
</tr>
<tr>
<td>NOTE:</td>
<td>This file configures Reflection Trusted Certificate Authorities</td>
</tr>
</tbody>
</table>

Global files and locations

<table>
<thead>
<tr>
<th>File Name</th>
<th>Add File To</th>
</tr>
</thead>
<tbody>
<tr>
<td>ssh_config</td>
<td>[CommonAppDataFolder]\Attachmate\Reflection</td>
</tr>
<tr>
<td>NOTE:</td>
<td>This is the global Secure Shell client configuration file.</td>
</tr>
<tr>
<td>ssh_known_hosts</td>
<td>[CommonAppDataFolder]\Attachmate\Reflection</td>
</tr>
<tr>
<td>NOTE:</td>
<td>This is the global known hosts file.</td>
</tr>
<tr>
<td>pki_config</td>
<td>[CommonAppDataFolder]\Attachmate\Reflection.pki</td>
</tr>
<tr>
<td>trust_store.p12</td>
<td>[CommonAppDataFolder]\Attachmate\Reflection.pki</td>
</tr>
</tbody>
</table>
Command Line Utilities

Reflection Secure Shell support includes DOS command-line utilities. The executable files that support these utilities are installed to your PC in the same location as your Reflection program files.

In this Section

- "ssh Command Line Utility" on page 423
- "sftp Command Line Utility" on page 426
- "ssh-keygen Command Line Utility" on page 430
- "scp Command Line Utility" on page 432

ssh Command Line Utility

Index Term
Primary: ssh command line utility

Syntax: ssh [options] [user@]hostname [host command]

You can use the ssh command line utility to make Secure Shell connections from the Windows command line.

NOTE

- Reflection also provides an A2D unwrapped a broken link to: t_7879 in an excluded topic. ssh2 utility. Both ssh and ssh2 can be used to establish Secure Shell connections, but some of the options supported by these two utilities are different. The ssh options are based on the OpenSSH Secure Shell implementation with some additional options supported only by the Reflection client. The ssh2 options are compatible with the Reflection for Secure IT UNIX client and the F-Secure client.
- You can reuse an existing Secure Shell connection. However, to do so you must explicitly enable this on each command line, or set the SSHConnectionReUse environment variable to Yes. For details, see “Connection Reuse in Secure Shell Sessions” on page 360.

Options

-A

Enables authentication agent forwarding. This can also be specified on a per-host basis in a A2D removed a broken link to: t_13406 in an excluded topic.configuration file (page 402). Agent forwarding should be enabled with caution. Users with the ability to bypass file permissions on the remote host can access the local agent through the forwarded connection. Attackers cannot obtain key material from the agent, however they can perform operations on the keys that enable them to authenticate using the identities loaded into the agent.

-a

Disables authentication agent forwarding. (This is the default.)

-b bind_address

Specify the interface to transmit from on machines with multiple interfaces or aliased addresses.
-c cipher_spec
   A comma-separated list of ciphers specified in order of preference. The default is "aes128-ctr,aes128-cbc,aes192-ctr,aes192-cbc,aes256-ctr,aes256-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour128,arcfour256,arcfour". If the connection is set to run in FIPS mode, the default is "aes128-ctr,aes128-cbc,aes192-ctr,aes192-cbc,aes256-ctr,aes256-cbc,3des-cbc".

Protocol version 1 (which is deprecated and not recommended) allows specification of a single cipher. The supported values are "3des", "blowfish", and "des".

-C
   Enables compression of all transmitted data. Compression is desirable on modem lines and other slow connections, but will only slow down response rate on fast networks.

-e escape_character
   Sets the escape character for the terminal session. The default character is a tilde (~). Setting the escape character to 'none' means that no escape character is available and the tilde acts like any other character. The following escape sequences are available. (Replace the tilde with your designated escape_character.)
   - . Terminate the connection.
   -R Request rekey (SSH protocol 2 only).
   -# List forwarded connections.
   -? Display available escape sequences.
   -- Type the escape character twice to send it to the host.

-E provider
   Uses the specified provider as the external key provider.

-f
   Places the client in the background just before command execution.

-F config_file
   Specifies an alternate configuration file to use for this connection. If a configuration file is given on the command line, other configuration files (page 402) are ignored.

-g
   Enables gateway ports. Remote hosts are allowed to connect to local forwarded ports.

-h
   Displays a summary of command line options.

-H scheme
   Specifies which SSH configuration scheme (page 403) to use for this connection.

-i key_file
   Specifies a private key to use for key authentication. Key files can also be specified on a per-host basis in the configuration file (page 402). It is possible to have multiple -i options (and multiple keys specified in a configuration file). Use quotation marks if the file or path includes spaces.
-k directory
  Specifies an alternate location for the config, host key, and user key files. Note: When -k is used, host keys are read and written from the specified location only if a known-hosts file already exists in that location. If no known-hosts file is found, host keys are read and written to the known-hosts file in the default location.

-l login_name
  Specifies a name to use for login on the remote computer. This can also be specified in the configuration file (page 402).

-L localport:remotehost:hostport
  Redirects data from the specified local port, through the secure tunnel to the specified destination host and port. For more information, see Local Port Forwarding. Port forwardings can also be specified in the configuration file. You cannot forward privileged ports (port numbers below 1024) unless you are logged in as an administrator. IPv6 addresses can be specified with an alternative syntax: port/host/hostport.

-m mac_spec
  Specifies one or more comma-separated MAC (message authentication code) algorithms to use for this connection. Specify algorithms in order of preference. The default is "hmac-sha1,hmac-sha256,hmac-sha512,hmac-md5,hmac-ripemd160,hmac-sha1-96,hmac-md5-96". If the connection is set to run in FIPS mode, the default is "hmac-sha1,hmac-sha256,hmac-sha512".

-N
  Do not execute a remote command. This is useful for configuring just port forwarding. (protocol version 2 only).

-o option
  Sets any option that is supported in the configuration file (page 405). For example:

  ssh "-o FIPSMode=yes" myuser@myhost

-p port
  Specifies the port to connect to on the server. The default is 22, which is the standard port for Secure Shell connections. This can be specified on a per-host basis in the configuration file (page 402).

-q
  Enables quiet mode, which causes all warning and diagnostic messages, including banners, to be suppressed.

-R localport:remotehost:hostport
  Redirects data from the specified remote port (on the computer running the Secure Shell server), through the secure tunnel to the specified destination host and port. For more information, see Remote Port Forwarding. Port forwardings can also be specified in the configuration file. You cannot forward privileged ports (port numbers below 1024) unless you are logged in as an administrator. IPv6 addresses can be specified with an alternative syntax: port/host/hostport.

-S
  Do not execute a shell.
-t
  Forces a tty allocation even if a command is specified.

-T
  Disable pseudo-tty allocation.

-v
  Sets the debug level to verbose mode, which is equivalent to setting the debug level to 2.

-V
  Displays product name and version information and exits. If other options are specified on the command line, they are ignored.

-x
  Disables X11 connection forwarding.

-X
  Enables X11 connection forwarding and treats X11 clients as untrusted. Untrusted remote X11 clients are prevented from tampering with data belonging to trusted X11 clients.
  X11 forwarding should be enabled with caution. Users with the ability to bypass file permissions on the remote host (for the user's X authorization database) can access the local X11 display through the forwarded connection. An attacker may then be able to perform activities such as keystroke monitoring.

-Y
  Enables X11 connection forwarding and treats X11 clients as trusted.
  X11 forwarding should be enabled with caution. Users with the ability to bypass file permissions on the remote host (for the user's X authorization database) can access the local X11 display through the forwarded connection. An attacker may then be able to perform activities such as keystroke monitoring.

-1
  Forces ssh to try protocol version 1 only. Protocol version 1 is deprecated and not recommended.

-2
  Forces ssh to try protocol version 2 only.

-4
  Forces connections using IPv4 addresses only.

-6
  Forces connections using IPV6 addresses only.

sftp Command Line Utility

Index Term
  Primary: sftp command line utility

Index Term
  Primary: file transfer
  Secondary: sftp command line utility
Syntax:
sftp [options] [user@]host[#port]:source_file
[user@]host[#port][:destination_file]

NOTE: You can reuse an existing Secure Shell connection. However, to do so you must explicitly enable this on each command line, or set the SSHConnectionReUse environment variable to Yes. For details, see "Connection Reuse in Secure Shell Sessions" on page 360.

Command Line Options

-a
   Transfer files in ASCII mode.

-b buffersize
   Sets the maximum buffer size for one request. Valid values are 1024 - 32768.

-B batchfile
   After a successful login, executes each command in the specified batch file and then terminates the connection. For example, the following command connects to myhost using myname and executes the commands in myfile. After all commands in the file are executed, the connection is terminated.

   sftp -B c:\mypath\myfile myhost.com myname

   The batch file can use any of the interactive commands documented below.

   NOTE: Semicolons are not supported for comments in scripts supplied to the sftp command line using the -B option. Use the number sign (#) to mark comments in these batch files.

-c cipher
   A comma-separated list of ciphers specified in order of preference. The default is "aes128-ctr,aes128-cbc,aes192-ctr,aes192-cbc,aes256-ctr,aes256-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour128,arcfour256,arcfour". If the connection is set to run in A2D unwrapped a broken link to: t_5746 in an excluded topic. FIPS mode, the default is "aes128-ctr,aes128-cbc,aes192-ctr,aes192-cbc,aes256-ctr,aes256-cbc,3des-cbc".

   Protocol version 1 (which is deprecated and not recommended) allows specification of a single cipher. The supported values are "3des", "blowfish", and "des".

-C
   Enables compression of all transmitted data. Compression is desirable on modem lines and other slow connections, but will only slow down response rate on fast networks.

-d
   Force target to be a directory.

-F config_file
   Specifies an alternate configuration file to use for this connection. If a configuration file is given on the command line, other configuration files (page 402) are ignored.

-h
   Displays a summary of command line options.

-H scheme
   Specifies which SSH configuration scheme (page 403) to use for this connection.
-i key_file
   Specifies a private key to use for key authentication. Key files can also be specified on a per-host basis in the configuration file (page 402). It is possible to have multiple -i options (and multiple keys specified in a configuration file). Use quotation marks if the file or path includes spaces.

-k directory
   Specifies an alternate location for the config, host key, and user key files. Note: When -k is used, host keys are read and written from the specified location only if a known-hosts file already exists in that location. If no known-hosts file is found, host keys are read and written to the known-hosts file in the default location.

-m mac_spec
   Specifies one or more comma-separated MAC (message authentication code) algorithms to use for this connection. Specify algorithms in order of preference. The default is "hmac-sha1,hmac-sha256,hmac-sha512,hmac-md5,hmac-ripemd160,hmac-sha1-96,hmac-md5-96". If the connection is set to run in FIPS mode, the default is "hmac-sha1,hmac-sha256,hmac-sha512".

-o option
   Sets any option that is supported in the configuration file (page 405). For example:
   ssh "-o FIPSMode=yes" myuser@myhost

-P
   Preserve time stamps and file attributes.

-P port
   Port to connect to on the remote host.

-q
   Enables quiet mode, which causes all warning and diagnostic messages, including banners, to be suppressed.

-Q
   Turns off display of the progress indicator.

-R maximum_requests
   Specifies the maximum number of concurrent requests. Increasing this may slightly improve file transfer speed but will increase memory usage. The default is 16 outstanding requests.

-s subsystem
   Specifies the ssh subsystem.

-S program
   Program to use for encrypted connections.

-u
   Remove the source file after copying.

-v
   Sets the debug level to verbose mode, which is equivalent to setting the debug level to 2.
-V
Displays product name and version information and exits. If other options are specified on the command line, they are ignored.

-4
Forces connections using IPv4 addresses only.

-6
Forces connections using IPV6 addresses only.

Interactive Mode

ascii
Set transfer type to ASCII.

binary
Set transfer type to binary.

bye
Quit sftp.

cd path
Change remote directory to path.

chmod path
Changes the permissions associated with path. Use mode to specify a three digit numeric permissions.

lcd path
Change local directory to path.

exit
Quit sftp.

get remote-path [local-path]
Retrieve the remote-path and store it on the local machine. If the local path name is not specified, it is given the same name it has on the remote machine.

getext [extension,extension...]
Displays the file extensions that will use ascii transfer. Use setext to modify this list.

help
Display help text.

lls [ls-options [path]]
Display local directory listing of either path or current directory if path is not specified.

lmkdir path
Create local directory specified by path.

lpwd
Print local working directory.
ls [path]
Display remote directory listing of either path or current directory if path is not specified.

mkdir path
Create remote directory specified by path.

put local-path [local-path]
Put command ![A2D - this term is missing a definition]

pwd
Display remote working directory.

quit
Quit sftp.

reget remote-file [local-file]
Resume the specified transfer. This works like the get command, but checks for the presence of a partially written local file and, if it is found, starts the transfer where the last attempt left off.

rename oldpath newpath
Rename remote file from oldpath to newpath.

rmdir path
Remove remote directory specified by path.

rm paths
Delete remote file specified by path.

setext [extension,extension...]
Sets the file extensions that will use ascii transfer. Wildcard characters are supported. When no argument is given, no file extensions use ascii transfer.

version
Display sftp version.

? Synonym for help.

**ssh-keygen Command Line Utility**

*Index Term*
Primary: ssh-keygen command line utility

**ssh-keygen** - Creation, management, and conversion of keys used for client and server authentication.

**Synopsis**

```
ssh-keygen [-b bits] -t type [-N [passphrase]] [-C comment] [-f output_keyfile]
ssh-keygen -B [-f input_keyfile]
ssh-keygen -c [-P passphrase] [-C comment] [-f keyfile]
ssh-keygen -e [-f input_keyfile]
ssh-keygen -i [-f input_keyfile]
ssh-keygen -y [-f input_keyfile]
ssh-keygen -l [-f input_keyfile]
```
Description

You can use the `ssh-keygen` command line utility to create RSA and DSA keys for public key authentication, to edit properties of existing keys, and to convert file formats. When no options are specified, `ssh-keygen` generates a 2048-bit RSA key pair and queries you for a key name and a passphrase to protect the private key. Public keys are created using the same base name as the private key, with an added `.pub` extension. The key location is displayed when key generation is complete.

Options

- **-b bits**
  
  Specifies the key size. Up to a point, a larger key size improves security. Increasing key size slows down the initial connection, but has no effect on the speed of encryption or decryption of the data stream after a successful connection has been made. The length of key you should use depends on many factors, including: the key type, the lifetime of the key, the value of the data being protected, the resources available to a potential attacker, and the size of the symmetric key you use in conjunction with this asymmetric key. To ensure the best choice for your needs, we recommend that you contact your security officer. Key sizes are rounded up to the next value evenly divisible by 64 bits. The default for DSA keys is 1024 bits; for RSA it is 2048 bits.

- **-B**
  
  Shows the fingerprint of the specified key in SHA-1 Bubble Babble format. You can specify the key file using `-f`. If you don't specify a file, you are queried for a filename. You can specify the private or public key name, but in either case, the public key must be available.

- **-c**
  
  Requests a change of the comment in the private and public key files. This operation is only supported for RSA1 keys. The program will prompt for the file containing the private keys, for the passphrase if the key has one, and for the new comment.

- **-C comment**
  
  Specifies information for the comment field within the key file. Use quotation marks if the string includes spaces. If you do not specify a comment when you create a key, a default comment is created that includes the key type, creator, date, and time.

- **-e**
  
  Uses the specified OpenSSH public or private key to generate a public key in Reflection format. You can specify the key file using `-f`. If you don't specify a file, you are queried for a filename.

- **-f filename**
  
  Specifies the filename for the generated private key. (A public key is also created and is always given the same name as the private key plus a `.pub` file extension.) This option can also be used in combination with `-e`, `-i`, `-l`, `-p`, `-y`, and `-B` to specify the input filename.

- **-i**
  
  Converts the specified Reflection public key to OpenSSH format. You can specify the key file using `-f`. If you don't specify a file, you are queried for a filename.

- **-h**
  
  Displays a summary of command line options.
Show fingerprint of specified public key file using the MD5 hash. You can specify the key file using \texttt{-f}. If you don't specify a file, you are queried for a filename. If you specify a private key, \texttt{ssh-keygen} tries to find the matching public key file and prints its fingerprint.

\textbf{-N passphrase}

Sets the passphrase. For example, to specify the passphrase for a new key:

\begin{verbatim}
ssh-keygen -N mypassphrase -f keyfile
\end{verbatim}

To create a new key that is not passphrase protected:

\begin{verbatim}
ssh-keygen -N -f keyfile
\end{verbatim}

You can also use \texttt{-N} in combination with \texttt{-p} and \texttt{-P} to change the passphrase of an existing key.

\textbf{-p}

Use this option to change the passphrase of an existing private key. If you use this option alone, the program prompts for the file containing the private key, for the old passphrase, and twice for the new passphrase. You can use it in combination with \texttt{-f}, \texttt{-P}, and \texttt{-N} to change the passphrase non-interactively. For example:

\begin{verbatim}
ssh-keygen -p -f keyfile -P oldpassphrase -N newpassphrase
\end{verbatim}

\textbf{-P passphrase}

Provides the (old) passphrase.

\textbf{-q}

Silence \texttt{ssh-keygen}.

\textbf{-t type}

Specifies the algorithm used for key generation. The possible values are "rsa" or "dsa" for protocol version 2.

\textbf{-y}

Uses the specified private key to derive a new copy of the public key. You can specify the key file using \texttt{-f}. If you don't specify a file, you are queried for a filename.

\textbf{Return values}

\texttt{ssh-keygen} returns 0 (zero) if the command completes successfully. Any non-zero value indicates a failure.

\textbf{scp Command Line Utility}

\textbf{Index Term}

Primary: scp command line utility

\textbf{Index Term}

Primary: file transfer

Secondary: scp command line utility

\textbf{Syntax}: scp [options] [user@host:]file1 [user@host:]file2
The `scp` command line utility copies files securely between hosts on a network. It uses Secure Shell `sftp` subsystem for data transfer, and uses the same authentication and provides the same security as Secure Shell. `Scp` will ask for passwords or passphrases if they are needed for authentication. Any file name may contain a host and user specification to indicate that the file is to be copied to/from that host.

**Examples**

This command line copies the file `f1` from the host to the local machine and gives it the name `f2`:

```bash
scp user@host:f1 f2
```

This command copies the local file `f1` to `f2` on the remote host.

```bash
scp f1 user@host:f2
```

**NOTE:** You can reuse an existing Secure Shell connection. However, to do so you must explicitly enable this on each command line, or set the SSHConnectionReUse environment variable to Yes. For details, see “Connection Reuse in Secure Shell Sessions” on page 360.

**Options**

The following options are available:

- `-a`
  Transfer files in ASCII mode.

- `-b buffersize`
  Sets the maximum buffer size for one request.

- `-B`
  Sets batch mode on, which prevents asking for passwords or passphrases. Use passphraseless user keys to authenticate.

- `-c cipher`
  A comma-separated list of ciphers specified in order of preference. The default is "aes128-ctr,aes128-cbc,aes192-ctr,aes192-cbc,aes256-ctr,aes256-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour128,arcfour256,arcfour". If the connection is set to run in A2D unwrapped a broken link to: t_5746 in an excluded topic FIPS mode, the default is "aes128-ctr,aes128-cbc,aes192-ctr,aes192-cbc,aes256-ctr,aes256-cbc,3des-cbc".

  Protocol version 1 (which is deprecated and not recommended) allows specification of a single cipher. The supported values are "3des", "blowfish", and "des".

- `-C`
  Enable compression.

- `-d`
  Force target to be a directory.

- `-D level`
  Sets the debug level. Allowed values are 1, 2, and 3.

- `-F configfile`
  Specifies an alternative per-user configuration file (page 402). If a configuration file is given on the command line, the system-wide configuration file will be ignored.
-h
   Displays a summary of command line options.

-H scheme
   Specifies which SSH configuration scheme (page 403) to use for this connection.

-i keyfile
   Selects a file from which the identity (private key) for RSA or DSA authentication is read. Identity
   files may also be specified on a per-host basis in the configuration file. It is possible to have
   multiple -i options (and multiple identities specified in a configuration file (page 402)). Path names containing spaces must be
   embedded inside double quotation marks.

-k directory
   Specifies an alternate location for the config, host key, and user key files. Note: When -k is used,
   host keys are read and written from the specified location only if a known-hosts file already exists
   in that location. If no known-hosts file is found, host keys are read and written to the known-hosts
   file in the default location.

-o option
   Can be used to give options in the format used in the configuration file (page 402). This is useful for specifying options for which
   there is no separate command-line flag. For a list of supported options, see the Configuration
   Keyword Reference (page 405).

--overwrite
   Specifies whether or not to overwrite existing destination files. The allowed values are 'yes' and
   'no'. The default is 'yes'.

-p
   Preserve timestamps and file attributes.

-P port
   Port to connect to on the remote host.

-q
   Quiet mode. Causes all warning and diagnostic messages, including banners, to be suppressed.

-Q
   Turns off display of the progress indicator.

-r
   Copy directories recursively, including all subdirectories.

-u
   Remove the source file after copying.

-v
   Verbose mode. Causes ssh to display debugging messages about its progress. This is helpful in
debugging connection, authentication, and configuration problems. Multiple -v options increases
the verbosity. Maximum is 3 (-vvv).

-V
   Display the version number and application information.
Secure Connections

Troubleshooting Secure Shell

Troubleshooting Secure Shell Connections

Index Term
Primary: troubleshooting (Secure Shell)
Secondary: troubleshooting connections

Index Term
Primary: SSH
Secondary: troubleshooting connections

Index Term
Primary: Secure Shell
Secondary: troubleshooting connections

If you are having trouble making a Secure Shell connection the trouble may come because Reflection cannot locate your host, or because of a problem with either host authentication or user authentication.

Using log files

If your connection problem is with host authentication (page 360), you may find useful information in the Reflection client A2D removed a broken link to: rsit_client_secure_shell_log_rf in an excluded topic.log file (page 436).

If your problem is with user authentication (page 362), you may need to contact the administrator of the Secure Shell server. User authentication problems are common, and complete information about failed user authentication is available only in the server debug log—not in the client log. By design, the Secure Shell protocol does not provide specific information to clients about failed authentication attempts. This is done so that an attacker cannot use error messages to determine why an authentication failed and thus narrow in on a successful attack.
Troubleshooting suggestions

Password authentication

- Incorrect password. Check that Caps lock is not enabled.
- Expired password. You may need to use Keyboard Interactive authentication instead of Password authentication to enable password updates.
- If no password prompt is displayed, password authentication may be disabled.

Public Key authentication

- User's public key has not been uploaded to the correct location on the host.
- User's public key has been uploaded to the correct location but has incorrect ownership or file permissions.
- Key is passphrase protected and you have entered an incorrect passphrase.
- The wrong key is selected for authentication on the User Keys (page 367) tab of the Secure Shell Settings dialog box.
- Too many public keys are selected, especially if you are attempting connections to servers running older versions of OpenSSH.

Certificate authentication

- The certificate used to authenticate the host is not available. Check the Reflection trusted root store and the Microsoft trusted root and intermediate stores. (If use of the Microsoft store has been disabled, certificates must be in the Reflection store.)
- The certificate used to authenticate the user is not available. Check the Reflection personal store and the Microsoft personal store.
- The certificate used to authenticate either the host or user has expired.
- Certificate host name must match host being contacted (page 386) is enabled and the host name you have specified for this connection doesn't exactly match host name in certificate.
- Certificate revocation checking is enabled (page 386) and the Certificate Revocation List is not available.
- Certificate revocation checking is enabled (page 386) and the host certificate has been revoked.

Key exchange

- The following error occurs during key exchange: "fatal: dh_gen_key: group too small: 1024 (2*need 1024)". Modify the key exchange algorithms to put diffie-hellman-group14-sha1 ahead of the other algorithms.

Related Topics

- “Enabling and Disabling Use of the Windows Certificate Store” on page 439

Use the Secure Shell Log File

The log file contains information you can use to troubleshoot Secure Shell connections.

NOTE: You can use the A2D unwrapped a link with an empty targetLogging Level setting to determine the amount of information written to the Secure Shell log. This setting is available from the Reflection Secure Shell Settings dialog box -- General tab (page 355).
To use the log file from the InfoConnect workspace

1 Capture a trace.
   The steps depend on your user interface mode (page 120).

   **User Interface Mode** | **Steps**
   --- | ---
   Ribbon | On the Tools tab, in the Tracing group, click Start Trace. Then perform the actions to trace. In the Tracing group, choose Stop Trace, and then choose Process Trace.
   InfoConnect Browser | On the InfoConnect menu choose Tools, Trace, and then Start Trace. Then perform the actions to trace. On the InfoConnect menu choose Tools, Trace, and then Stop Trace. In the search box, enter P and then, under Actions, select Process Trace.
   TouchUx | On the menu, select the Wrench icon and then, under Trace, select Start Trace. After you have performed the actions to trace, select the Wrench icon and choose Stop Trace. Then select the Wrench icon again and choose Process Trace.

2 Select Network protocol details, and then click OK.
3 Locate the event file (*.rev) and then click Open.
4 Select a filename and format for your log output, and then click Save.

To use the log file from the FTP Client

- Do one of the following:

   **To** | **Choose**
   --- | ---
   Send log information to a file | Tools > Start Logging, and then change Files of Type to "Diagnostic File (*.txt)".
   View the log information in the FTP command window | View > Command Window.

Certificate Authentication (PKI)

In this Section

- “PKI Overview” on page 438
- “Enabling and Disabling Use of the Windows Certificate Store” on page 439
- “Configuring Certificate Revocation Checking” on page 440
- “Distributing Intermediate Certificates using an LDAP Directory” on page 441
- “DOD PKI Information” on page 442
- “Reflection Certificate Manager” on page 446
PKI Overview

Index Term
Primary: PKI
Secondary: overview

A Public Key Infrastructure (PKI) is a system that helps facilitate secure communications through the use of digital certificates. Reflection supports the use of a PKI for host and user authentication during Secure Shell and SSL/TLS sessions.

Authentication

Authentication is the process of reliably determining the identity of a communicating party. Identity can be proven by something you know (such as a password), something you have (such as a private key or token), or something intrinsic about you (such as a fingerprint). In a typical Telnet session to a remote host, the user authenticates with a password, but the host is not authenticated. More secure protocols, including Secure Shell and SSL/TLS, require host authentication. In both Secure Shell and SSL/TLS sessions, host authentication is accomplished using public key cryptography. In addition, both session types can also be configured to use public key cryptography for user authentication.

Public Key Cryptography

Public key cryptography uses a mathematical algorithm with a public/private key pair to encrypt and decrypt data. One of the keys is a public key, which can be freely distributed to communicating parties, and the other is a private key, which should be kept secure by the owner of the key. Data encrypted with the private key can be decrypted only with the public key; and data encrypted with the public key can be decrypted only with the private key.

When keys are used for authentication, the party being authenticated creates a digital signature using the private key of a public/private key pair. The recipient must use the corresponding public key to verify the authenticity of the digital signature. This means that the recipient must have a copy of the other party's public key and trust in the authenticity of that key.

Digital certificates

Digital certificates are an integral part of a PKI (Public Key Infrastructure). Certificates are issued by a certification authority (CA), which ensures the validity of the information in the certificate. Each certificate contains identifying information about the certificate owner, a copy of the certificate owner's public key (used for encrypting and decrypting messages and digital signatures), and a digital signature (generated by the CA based on the certificate contents). The digital signature is used by a recipient to verify that the certificate has not been tampered with and can be trusted.

Digital certificate stores

Digital certificates are maintained on your computer in certificate stores. A certificate store contains the certificates you use to confirm the identity of remote parties, and may also contain personal certificates, which you use to identify yourself to remote parties. Personal certificates are associated with a private key on your computer.

Reflection can be configured to use digital certificates located in either or both of the following stores:

- The Windows Certificate Store

  This store can be used by a number of applications, including Reflection, web browsers, and mail clients. Some certificates in this store are included when you install the Windows operating system. Others may be added when you connect to internet sites and establish trust, when you install software, or when you receive an encrypted or digitally signed e-mail. You can also import certificates manually into your Windows store. Manage the certificates in this store using the Windows Certificate Manager.
The Reflection Certificate Store

This store is used only by Reflection applications. To add certificates to this store, you must import them manually. You can import certificates from files and also use certificates on hardware tokens such as smart cards. Manage the certificates in this store using the “Reflection Certificate Manager” on page 446.

Reflection applications can be configured to authenticate using only those certificates located in Reflection store, or using both the Windows and the Reflection store. Enabling host authentication using the Windows certificate store means that you may not need to import certificates, because authentication may be accomplished using certificates that are already available. Disabling authentication using the Windows certificate store enables you to have greater control over which certificates are used for authentication. For more information, see Enabling or Disabling authentication using the Windows certificate store (page 439).

PKI in Reflection sessions

Reflection sessions support PKI authentication for both Secure Shell and SSL/TLS sessions.

- All SSL/TLS sessions require certificates for host authentication; without the necessary certificate, you cannot make a host connection. Depending on the host configuration, you may also need to install certificates for user authentication. For more information, see “Digital Certificates in SSL/TLS Sessions” on page 341.

- Secure Shell sessions typically require both host and user authentication. Certificates can be used for either host and/or user authentication, but are not required by default. For more information, see Digital Certificates in Secure Shell Sessions (page 385).

Enabling and Disabling Use of the Windows Certificate Store

Reflection Secure Shell and SSL/TLS sessions support the use of digital certificates (page 887) for both host and user authentication. Reflection applications can be configured to authenticate using only those certificates located in Reflection store, or using both the Windows and the Reflection store.

Host authentication

Enabling use of the Windows certificate store means that you may not need to import the certificates used for host authentication. If your host certificates were acquired from a well-known Certification Authority (page 887) (CA), such as VeriSign or Thawte, a certificate identifying the issuer as a trusted CA should already be included in the Trusted Root Certification Authorities list on your system. When use of the system store is enabled, Reflection clients look for certificates in both the Reflection and the system store.
Disabling use of the Windows certificate store enables you to have greater control over which certificates are used for authentication. Certificates can be added to the Windows store in a variety of ways, and you may not want to allow use of all of these certificates for authenticating Reflection sessions. When use of the Windows store is disabled, only those certificates you have imported into the Reflection store are used for host authentication.

To enable (or disable) host authentication using certificates in the Windows store:

1. Open the "Reflection Certificate Manager" on page 446.
2. Click the Trusted Certificate Authorities (page 449) tab.
3. Select (or clear) Use System Certificate Store for SSH connections and/or Use System Certificate Store for SSL/TLS connections.

User authentication

Reflection uses personal certificates in the Windows store and the Reflection store in the same way. Available personal certificates include those in the Windows personal store, the Reflection personal store (page 448), and certificates on configured hardware tokens (page 453) (for example smart cards).

- If you have configured a Reflection Secure Shell session, you must specify which certificates to use for user authentication from the User Keys tab in the Secure Shell settings dialog box.
- If you have configured a Reflection SSL/TLS session, all certificates located in either store are automatically available for user authentication.

Configuring Certificate Revocation Checking

Reflection SSL/TLS and Secure Shell connections can be configured to authenticate hosts using digital certificates (page 887). To ensure that certificates have not been revoked, you can configure Reflection to check for certificate revocation using CRLs (page 887) or using an OCSP (page 888) responder.

When CRL checking is enabled, Reflection always checks for CRLs in any location specified in the CRL Distribution Point (CDP) field of the certificate. In addition, Reflection can also be configured to check for CRLs located in an LDAP (page 888) directory or using an OCSP (page 888) responder.

Reflection’s default value for certificate revocation checking is based on your current system setting. If your system is configured to do CRL checking, all Reflection sessions will check for certificate revocation using CRLs by default.
NOTE: When Reflection is running in DOD PKI mode (page 442), certificate revocation is always enabled and cannot be disabled.

To enable CRL checking for all SSH sessions

1. In Internet Explorer, choose Tools > Internet Options > Advanced.

Using Reflection, you can enable certificate revocation checking using either a CRL or an OCSP responder.

To enable CRL checking for a Secure Shell session

1. Open the Reflection Secure Shell Settings dialog box.
2. Click the PKI tab.
3. Select either Use OCSP or Use CRL.

To enable CRL checking for SSL/TLS sessions

1. Open the Security Properties (page 511) dialog box.
2. On the SSL/TLS tab, click Configure PKI. (Use SSL/TLS security must be selected.)
3. Select either Use OCSP or Use CRL.

NOTE: CRLs and/or OCSP responders required by a certificate are identified in the AIA and/or CDP extension of the certificate. If this information is not provided in the certificate, you can use the OCSP (page 453) and LDAP (page 451) tabs of the Reflection Certificate Manager to configure it.

Distributing Intermediate Certificates using an LDAP Directory

Index Term
Primary: LDAP
Secondary: distributing intermediate certificates

Index Term
Primary: certificate authentication
Secondary: distribute using LDAP

Reflection SSL/TLS and Secure Shell connections can be configured to authenticate hosts using digital certificates (page 887). Depending on how you have configured the Reflection Certificate Manager (page 439), Reflection may use certificates in just the Reflection store or in both the Windows and Reflection stores. The Windows store holds intermediate as well as trusted root certificates. The Reflection store holds trusted root certificates only. Reflection can also be configured to locate intermediate certificates from an LDAP server.

To configure Reflection to locate intermediate certificates stored in an LDAP directory, use the LDAP (page 451) tab of the Reflection Certificate Manager to identify the LDAP server (or servers).
Configuring the LDAP server

Reflection can locate a certificate in the LDAP directory only if the LDAP distinguished name (DN) exactly matches the contents of the Subject field in the certificate. For example, if the Subject field of the certificate displays the following objects:

- CN = Some CA
- O = Acme
- C = US

The DN of the entry in the LDAP directory must be exactly: "CN = Some CA, O=Acme, C = US".

The attributes of the LDAP entry identified by this DN must include one of the following. (Reflection looks for these attributes in order from top to bottom.)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>OID (Object Identifier)</th>
</tr>
</thead>
<tbody>
<tr>
<td>userCertificate;binary</td>
<td>2.5.4.36</td>
</tr>
<tr>
<td>cACertificate;binary</td>
<td>2.5.4.37</td>
</tr>
<tr>
<td>userCertificate</td>
<td>2.5.4.36</td>
</tr>
<tr>
<td>cACertificate</td>
<td>2.5.4.37</td>
</tr>
<tr>
<td>mosaicKMandSigCertificate</td>
<td>2.16.840.1.101.2.1.5.5</td>
</tr>
<tr>
<td>sdnsKMandSigCertificate</td>
<td>2.16.840.1.101.2.1.5.3</td>
</tr>
<tr>
<td>fortezzaKMandSigCertificate</td>
<td>2.16.840.1.101.2.1.5.5</td>
</tr>
<tr>
<td>crossCertificatePair;binary</td>
<td>2.5.4.40</td>
</tr>
<tr>
<td>crossCertificatePair</td>
<td>2.5.4.40</td>
</tr>
</tbody>
</table>

DOD PKI Information

Index Term
Primary: PKI
Secondary: DOD PKI information

Index Term
Primary: DOD PKI information

This section describes how to install, configure, and use Reflection to operate within the Department of Defense (DOD) or other Public Key Infrastructure (PKI) (page 438) environment. PKI configuration affects both Secure Shell and SSL/TLS connections.

Running Reflection in DOD PKI mode

By default, Reflection applications allow some configurations that do not meet DOD PKI requirements. Administrators can use Reflection Group Policies to configure all Reflection sessions to meet DOD PKI requirements.
To configure DOD PKI mode

1 Run the Group Policy Editor using one of the following techniques:
   • On the command line, enter `Gpedit.msc`
   • In the Active Directory Users and Computers console, open the properties for an Organizational Unit, click the Group Policy tab, and edit or create a new policy object.

2 A2D unwrapped a broken link to: t_24306 in an excluded topic. Install the Reflection template (ReflectionPolicy.adm) if you have not already done so.

   **NOTE:** For information about how to download and install the Reflection policy template, see Technical Note 2216 (http://support.attachmate.com/techdocs/2216.html)

3 Under Local Computer Policy > User Configuration > Administrative Templates > Reflection Settings, disable the setting Allow non-DoDPKI mode.

Configuring DOD PKI mode has the following effects.

• You must configure Reflection to use either CRL (page 887) checking or an OCSP (page 888) responder. In DOD PKI mode, the option to use neither form of checking is disabled. (For SSH connections, certificate revocation is configured using the PKI tab of the Secure Shell settings dialog box. For SSL/TLS connections it is configured using the PKI Configuration dialog box.)

• Reflection enforces FIPS-approved encryption algorithms. For SSH connections, this means that only FIPS-approved options are available on the Encryption tab of the Secure Shell settings dialog box. For SSL/TLS connections this means that you cannot set Encryption strength to 40 Bits or 56 Bits.

• For a connection to succeed, the certificate host name must exactly match the host name specified for your Reflection connection. This means that the setting Certificate must match host name being contacted is automatically selected and cannot be modified. (For SSH connections, this setting is configured using the PKI tab of the Reflection Secure Shell Settings dialog box. For SSL/TLS connections it is configured using the PKI Configuration (page 523) dialog box.)

• Intermediate CA certificates signed using the MD2 or MD5 hash are not supported for certificate validation.

**Installing and Removing Trust Points**

A trust point is any CA (page 887) certificate in a chain of trust.

To add a trust point to the Reflection certificate store:

1 “Open the Reflection Certificate Manager” on page 447 A2D removed a broken link to: t_13510 in an excluded topic..

2 Click the Trusted Certificate Authorities tab.

3 Click Import, then browse to locate a certificate (typically *.cer or *.crt).

To remove a trust point from the Reflection certificate store,

1 “Open the Reflection Certificate Manager” on page 447 A2D removed a broken link to: t_13510 in an excluded topic..

2 Click the Trusted Certificate Authorities tab.

3 Select the certificate and click Remove.
NOTE

- Intermediate CA trust points can be retrieved from an LDAP (page 888) or HTTP server which may be identified by explicit URIs defined in the Authority Information Access (AIA) extension of a certificate, or using LDAP server information configured on the LDAP tab of the Reflection Certificate Manager. These certificates are stored in the cert_cache file located in either <My Documents>\Attachmate\Reflection\pki or \All users\Application data\Attachmate\Reflection.
- When Reflection is running in DOD PKI mode, only those root certificates you have added to the Reflection Certificate manager are used. There is no need to remove any non-DOD PKI certificates that may be present in the Windows Certificate Store.

Configuring Certificate Revocation Checking

Reflection's default value for certificate revocation checking is based on your current system setting. If your system is configured to do CRL checking, Reflection sessions will check for certificate revocation using CRLs (page 887) by default. You can also configure Reflection to use an OCSP (page 888) responder.

Reflection also supports a setting to disable CRL checking. You may want to use this setting for testing purposes, however this option is not available if Reflection is running in DOD PKI mode.

CAUTION: Disabling CRL checking compromises your security. Use this option only for testing purposes.

You can define one or more LDAP (page 888) servers from which to retrieve intermediate certificates or CRLs.

To define an LDAP server

1. **Open the Reflection Certificate Manager** on page 447A2D removed a broken link to: t_13510 in an excluded topic.
2. Click the LDAP tab.
3. Click Add, then specify the server using the following URL format:
   
   ldap://hostname:portnumber
   
   For example:
   
   ldap://ldapserver.myhost.com:389

To configure OCSP

1. You can define one or more OCSP servers from which to request certificate revocation information.
2. Set Certificate Revocation to Use OCSP. (For SSH connections use the PKI tab of the Secure Shell settings dialog box. For SSL/TLS connections use the PKI Configuration dialog box.)

NOTE: OCSP responder URLs required by a certificate are identified in the AIA extension of the certificate. If this information is not provided in the certificate, you can use the following steps to configure OCSP responder information.

3. **Open the Reflection Certificate Manager** on page 447A2D removed a broken link to: t_13510 in an excluded topic..
4. Click the OCSP tab.
5. Click Add, then specify the server using the following URL format:
Using Uniform Resource Identifiers for DOD PKI Services

Reflection supports the use of URIs (page 890) for automatic CRL (page 887) updating and retrieval. As defined in section 4.2.1.14 of RFC3280.

If CRL checking is enabled, Reflection checks for certificate revocation as follows:

1. Check the crl_cache file for valid revocation information. If none is found, continue on to step 2.
2. Check the CDP extension in the certificate for HTTP or LDAP URIs and query these in the order specified (first HTTP, then LDAP). If the certificate is found to be revoked, close the connection. If the certificate is not found continue on to step 3.
3. If one or more LDAP servers is specified in the Reflection Certificate Manager LDAP tab, assemble the Distinguished Name for the CA listed in the Issuer extension of the certificate and query for the CRL file. If the certificate is not found to be revoked in any CRL, continue to the next validation step.

Updates for expired CRLs are handled automatically, and do not require administrator intervention or configuration.

If OCSP checking is enabled, Reflection always checks all available OCSP responders to ensure that the connection will fail if any of these responders knows that the certificate has been revoked. For the connection to succeed at least one OCSP responder must be available and return a value of 'good' for the certificate status. Reflection performs these checks as follows.

1. Check the AIA extension in the certificate for one or more OCSP responders and query each of those responders. If the status of the certificate comes back as 'revoked' from any responder, close the connection.
2. Check for one or more user configured OCSP responders specified using the Reflection Certificate Manager OCSP tab and query each of those responders. If the status of the certificate comes back as 'revoked' from any responder, close the connection.
3. If all responders returned 'unknown' close the connection. If a 'good' response was returned from at least one of the queried OCSP responders continue on to the next validation step.

Using URIs to Retrieve Intermediate Certificates

As defined in section 4.2.2.1 of RFC3280, Reflection can use URIs (page 890) to retrieve intermediate CA (page 887) certificates as follows:

1. Check the cert_cache file for the required intermediate certificate. If it is not found, continue on to step 2.
2. If either HTTP or LDAP URIs are defined in the Authority Information Access (AIA) extension of a certificate, attempt to use these (first HTTP, then LDAP) to retrieve intermediate CA certificates.
3. If the preceding attempts fail, assemble a Distinguished Name from the issuing certificate's Subject Name, and queries the defined LDAP server for the contents of the CACertificate attribute.

Because Reflection does not enforce the security policy extension of a certificate, security policy configuration is not necessary.
Configuring and Protecting Certificates and Private Keys

To configure client authentication using certificates:

1. "Open the Reflection Certificate Manager" on page 447A2D removed a broken link to: t_13510 in an excluded topic.

2. On the Personal tab, click Import, then browse to locate a certificate (typically *.pfx or *.p12). You will be prompted to create a passphrase that will be required any time this key is used. Entering a passphrase is advisable to help protect this key on your system.

3. For Secure Shell connections, open the Reflection Secure Shell Settings dialog box, click the User Keys tab and select the certificate(s) you want to use for client authentication to the currently specified host. (This step is not required for SSL/TLS connections.)

Private Key Safeguards

If a client private key is stolen, a malicious user can gain access to files on any servers accessible to that user. To minimize this risk, each client user should always protect his or her private key with a passphrase. This ensures that only someone who knows the passphrase can authenticate with that key. Users should create and protect passphrases following the password specifications in your organization’s Security Policy.

Actions to Take if a Key is Compromised

Consider a private key compromised if it has become available to any unauthorized entity, or if you have reason to distrust the actions of any person who has access to the key.

If the client key is compromised, revoke the client certificate.

To replace a compromised key:

1. Generate a new private key and certificate and import the key into the Reflection Certificate Manager.

2. On the server, update the map file line for this client if the identifying information has changed.

To remove the compromised key from the client computer:

1. Remove the key from the Personal (page 448) tab of the Reflection Certificate manager. This removes this key from the identity_store.p12 file.

2. If the original file containing the old key and certificate (*.pfx or *.p12) is still on the client computer, use a DOD-approved file erasure utility to delete this file.

Related Topics

- “PKI Overview” on page 438
- “Configuring Certificate Revocation Checking” on page 440
- “Configuring the LDAP Server for CRL Checking” on page 452
- “PKI Configuration Dialog Box” on page 523
- “PKI Tab (Secure Shell Settings)” on page 386

Reflection Certificate Manager

Index Term
Primary: Reflection Certificate Manager
Secondary: overview
Reflection applications can authenticate using digital certificates (page 887) located in either the Windows certificate store or the Reflection certificate store (or both). The Reflection certificate store can be used for authentication during Secure Shell and/or SSL/TLS sessions.

Use the Reflection Certificate manager to manage the digital certificates in the Reflection certificate store and to configure other aspects of Reflection PKI support.

**Open the Reflection Certificate Manager**

Use one of the following procedures to launch the Reflection Certificate Manager, depending on the application and security protocol you are using.

**From the Secure Shell Settings dialog box**

1. A2D removed a broken link to: reflection_secure_shell_settings_topic_gta in an excluded topic.
2. On the PKI tab, click Reflection Certificate Manager.

**From the Security Properties dialog box**

1. Open the Security Properties (page 511) dialog box.
2. On the SSL/TLS tab, select Use SSL/TLS Security.
3. Click Configure PKI.
4. Click Reflection Certificate Manager.

**Opening the Windows Certificate Manager from Internet Explorer**

1. Open Microsoft Internet Explorer.
2. On the Tools menu, click Internet Options.
3. On the Content tab, click Certificates.

**Opening the Windows Certificate Manager from the Control Panel**

1. Use the Windows Start menu to open the Control Panel.
2. Double-click Internet Options.
3. On the Content tab, click Certificates.
Opening the Windows Certificate Manager from Reflection

While you are configuring your Reflection sessions, you can get quick access to the Windows Certificate Manager from either the Secure Shell Settings dialog box or the Security Properties dialog box. Availability of these dialog boxes depends on the application and security protocol you are using.

From the Secure Shell Settings dialog box

1. Open the Reflection Secure Shell Settings (page 353) dialog box.
2. On the PKI tab, click View System Certificates.

From the Security Properties dialog box

1. Open the Security Properties (page 511) dialog box.
2. On the SSL/TLS tab, select Use SSL/TLS Security.
3. Click Configure PKI.
4. Click View System Certificates.

Server Certificate not Found

The host is presenting a self-signed server certificate that is not in the Trusted Root Certification Authorities list of your Window's certificate store.

The options are:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Always | Accept the certificate and add it to your trusted root list. The host will be authenticated with this certificate in subsequent connections and this dialog box will not appear again unless the certificate is removed from the list.  
**NOTE:** The accepted certificate is saved to your user-specific certificate store. If your system administrator has configured a global certificate store, certificates in your personal store are not used and you will continue to see this prompt. |
| Once   | Accept the certificate for this connection only, but don't load it into the certificate store. |
| No     | Decline the certificate and close the connection. |

**CAUTION:** Accepting a self-signed certificate can create a security risk. The appearance of this dialog box might be the result of a "man-in-the-middle attack," in which another server poses as your host. If you are not sure how to respond, click No and contact a system administrator.

Personal Tab (Reflection Certificate Manager)

Index Term
Primary: Reflection Certificate Manager  
Secondary: Personal tab

Getting there (page 447)

Use this tab to manage the personal certificates (page 887) in the Reflection certificate store. Personal certificates are used for user (client) authentication.
The options are:

| Import | Add a certificate to the Reflection store. The imported file (typically a *.pfx or *.p12) must include a private key. Depending on how the file was created, you may be prompted for a password before you can import the file. You will be prompted to enter a "passphrase" on page 888 for to protect the private key in the Reflection store. If you specify a passphrase, you'll be prompted for this passphrase when this certificate is used to authenticate to a host. |
| Remove | Remove the selected certificate from the Reflection store. |
| View | View the selected certificate. |
| Change Passphrase | Change the "passphrase" on page 888 for the selected certificate. |

**Trusted Certification Authorities Tab (Reflection Certificate Manager)**

**Index Term**

Primary: Reflection Certificate Manager  
Secondary: Trusted Certification Authorities tab

**Getting there (page 447)** A2D removed a broken link to: t_13510 in an excluded topic.

Use this tab to manage certificates from trusted certification authorities (CAs) in the Reflection certificate store. Reflection automatically uses any certificates in the Trusted Certification Authorities store for host (server) authentication.

| Import | Add a certificate (typically *.cer or *.crt) to the Reflection store. |
| Remove | Remove the selected certificate from the Reflection store. |
| View | View the selected certificate. |
Store trusted certificates in the common application data folder

By default, trusted roots that you add using the Import button are saved to the following Reflection store, which makes them available only to your current user account:

```
personal_documents_folder\Attachmate\Reflection\.pki\trust_store.p12
```

Select **Store trusted certificates in the common application data folder** to import a certificate to the following location, which makes it available to all users of the computer:

```
common_application_data_folder\Attachmate\Reflection\.pki\trust_store.p12
```

**NOTE**

- The value of this setting is not saved. Selecting or clearing it only affects which certificate store you are viewing and editing while the dialog box remains open. If a shared store is present, this setting is selected by default when you open the dialog box. If no shared store is present, the setting is not selected by default.

- If a shared store exists, trusted roots are read exclusively from the shared store. Trusted roots you have configured for individual user accounts no longer have any effect.

- To revert to user-specific trusted root stores after creating a shared store, you must delete or rename the shared `trust_store.p12` file. If you simply clear this setting, subsequent changes will modify your personal store, but the personal store continues to have no effect on Reflection’s behavior as long as `trust_store.p12` is still present in the common application data folder.

- If the operating system has been configured by the administrator to deny users write access to `common_application_data_folder\Attachmate\Reflection`, this setting is not available to those users and they will not be able to modify items in the shared trusted root store.

Use System Certificate Store for SSH connections

When this item is selected, Reflection uses certificates in your Windows certificate store (in addition to any certificates you have imported into the Reflection store) to authenticate hosts when establishing a Secure Shell connection.

Clear this setting to ensure that Reflection applications authenticate hosts using only the certificates in the Reflection store.

Use System Certificate Store for SSL/TLS connections

When this item is selected, Reflection uses certificates in your Windows certificate store (in addition to any certificates you have imported into the Reflection store) to authenticate hosts when establishing an SSL/TLS connection.

Clear this setting to ensure that Reflection applications authenticate hosts using only the certificates in the Reflection store.
The Lightweight Directory Access Protocol (LDAP) is a standard protocol that can be used to store information in a central location and distribute that information to users. Administrators can configure an LDAP server to distribute information needed by users who are authenticating with certificates. This information can include:

- Certificate Revocation Lists (CRLs), which are used to ensure that certificates being used have not been revoked by the certification authority.
- Intermediate certificates needed to establish a valid certification path from the server certificate to a trusted root certification authority.

Use the LDAP tab of the Reflection Certificate Manager to list LDAP servers that distribute this information. The options are:

**Add**
Add an LDAP server to the list. Specify the server using the following URL format:

ldap://hostname[:portnumber]

For example:

ldap://ldapserver.myhost.com:389

**Modify**
Edit the server URL.

**Remove**
Remove the selected server from the list.
LDAP Directory Configuration

Use the following links for more information about how Reflection handles information stored in the LDAP directory.

- CRLs (page 452)
- Intermediate certificates (page 441)

NOTE

- It is not necessary to configure an LDAP server to use CRL checking. When CRL checking is enabled, Reflection always checks for CRLs in any location specified in the CRL Distribution Point (CDP) field of the certificate. Configuring an LDAP server provides an additional mechanism for retrieving CRL lists.
- Reflection does not support server URLs that use the LDAPS scheme (for example, ldaps://hostname:port) to transfer LDAP data using SSL.

Related Topics

- “Configuring Certificate Revocation Checking” on page 440
- “Distributing Intermediate Certificates using an LDAP Directory” on page 441

Configuring the LDAP Server for CRL Checking

Reflection can locate a CRL in the LDAP directory only if the LDAP distinguished name (DN) exactly matches the contents of the Issuer field in the CRL. For example, if the Issuer field of the CRL displays the following objects:

- CN = Some CA
- O = Acme
- C = US

The DN of the entry in the LDAP directory must be exactly: "CN = Some CA, O=Acme, C = US".

The attributes of the LDAP entry identified by this DN must include one of the following. (Reflection looks for these attributes in order from top to bottom.)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>OID (Obect Identifier)</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificateRevocationList;binary</td>
<td>2.5.4.39</td>
</tr>
<tr>
<td>authorityRevocationList;binary</td>
<td>2.5.4.38</td>
</tr>
<tr>
<td>certificateRevocationList</td>
<td>2.5.4.39</td>
</tr>
<tr>
<td>authorityRevocationList</td>
<td>2.5.4.38</td>
</tr>
<tr>
<td>deltaRevocationList;binary</td>
<td>2.5.4.53</td>
</tr>
<tr>
<td>deltaRevocationList</td>
<td>2.5.4.53</td>
</tr>
<tr>
<td>mosaicCertificateRevocationList</td>
<td>2.16.840.1.101.2.1.5.45</td>
</tr>
<tr>
<td>sdnsCertificateRevocationList</td>
<td>2.16.840.1.101.2.1.5.44</td>
</tr>
<tr>
<td>fortezzaCertificateRevocationList</td>
<td>2.16.840.1.101.2.1.5.45</td>
</tr>
</tbody>
</table>
OCSP Tab (Reflection Certificate Manager)

Index Term
Primary: Reflection Certificate Manager
Secondary: OCSP tab

Index Term
Primary: OCSP
Secondary: configuring OCSP responders

Getting there (page 447) A2D removed a broken link to: t_13510 in an excluded topic.

Configure one or more OCSP (page 888) responders for certificate revocation checking. Click Add to add a server to the list. By default, every server you add is queried for certificate validity, starting with the first server on the list. Clear the check box next to a server to disable certificate checking for that server without removing the server from the list.

Add  Add an OCSP server to the list. Specify the server using the following URL format:

URL:portnumber
For example:
www.ocspresponder.com:80

Modify  Edit the server URL.

Remove  Remove the selected server from the list.

Related Topics
- “Configuring Certificate Revocation Checking” on page 440
- “Distributing Intermediate Certificates using an LDAP Directory” on page 441

PKCS#11 Tab (Reflection Certificate Manager)

Index Term
Primary: smart cards, configuring

Index Term
Primary: Reflection Certificate Manager
Secondary: PKCS #11 tab

Getting there (page 447) A2D removed a broken link to: t_13510 in an excluded topic.

Use the PKCS#11 tab to configure authentication using hardware devices, such as smart cards or USB tokens. Your hardware device must conform to PKCS#11 (page 888) specifications.

This tab displays all currently available devices, and any certificates or public keys located on those devices. When use of a device is enabled using the check box provided, Reflection automatically uses any certificates or keys on the device for user authentication.

You must install the software supplied by your token provider before you can configure Reflection to authenticate using a hardware token. To configure authentication using the token, you will also need to know the name and location of the library file (*.dll) used by that provider to provide access to your hardware device.
The options are:

<table>
<thead>
<tr>
<th>Providers list</th>
<th>Displays devices currently available. Clear the check box(es) to disable authentication with a listed device.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Contents</td>
<td>Displays keys and certificates available on the selected device.</td>
</tr>
<tr>
<td>View Certificate</td>
<td>Displays the selected certificate.</td>
</tr>
<tr>
<td>Disconnect automatically when token is removed</td>
<td>When selected, the connection is active only while the token is present.</td>
</tr>
<tr>
<td>Seconds to wait before disconnecting</td>
<td>Specifies the number of seconds to wait to disconnect after a token is removed.</td>
</tr>
</tbody>
</table>

Related Topics

- “PKCS#11 Provider Dialog Box” on page 454

PKCS#11 Provider Dialog Box

Getting there (page 447) A2D removed a broken link to: t_13510 in an excluded topic.

The options are:

<table>
<thead>
<tr>
<th>Provider DLL</th>
<th>Specify the file name and location of the library used to access the hardware device. This is typically installed to the Windows system folder. You may need to contact the device manufacturer to determine the correct file.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slots</td>
<td>Identify the card slot that holds the card being used for authentication.</td>
</tr>
<tr>
<td>Additional parameters</td>
<td>Specify any additional parameters needed to access the information on the hardware device.</td>
</tr>
</tbody>
</table>

Related Topics

- “PKCS#11 Tab (Reflection Certificate Manager)” on page 453

SOCKS or HTTP

Index Term
- Primary: SOCKS
- Secondary: host connection (SOCKS)

You can configure sessions to connect through a SOCKS proxy server or an HTTP server.

NOTE

- SOCKS is supported for VT, 3270, and 5250 terminals.
- HTTP is supported only for VT terminals.

Related Topics

- “Security Properties Dialog Box” on page 511
**SOCKS Overview**

SOCKS is a software protocol used in conjunction with a firewall host system to provide secure, controlled access to internal and external networks. When you request a network connection from a SOCKS-enabled application, the SOCKS Client software communicates with the SOCKS server software to determine if the connection is allowed. If it is, the connection is established. If it is not, the SOCKS server rejects the connection request.

To enable SOCKS support, use the **SOCKS** tab of the Security Properties dialog box (or, if you are also configuring a Secure Shell connection, use the Reflection Secure Shell Settings dialog box). After enabling SOCKS support, you must configure the SOCKS client. You can configure the software in one of two ways: designate a single SOCKS proxy server through which all requested connections must pass; or designate specific SOCKS proxy servers (or request that the SOCKS proxy server be bypassed) for specific destination addresses.

When the SOCKS protocol is enabled and you use a Reflection application to request a connection to a remote host, Reflection determines if the connection request must go through the firewall system. If the firewall system must be used, the application uses the SOCKS protocol to communicate with the SOCKS server software, which determines if the connection is allowed.

The Reflection SOCKS Client is compliant with SOCKS version 4 and works with SOCKS version 4 or version 5 servers.

**NOTE:** If your SOCKS server requires authentication before it will grant a connection request, you must run the Identification Daemon. The Identification Daemon (IdentD) authenticates TCP connections between two hosts. Some SOCKS servers require authentication before they will grant a connection request through the firewall. The Identification Daemon must be running to perform this authentication.

Check with your system administrator to determine whether your SOCKS proxy server requires identification (that is, whether the SOCKS daemon was started using the -i or -I option). If the server does not require authentication, the Identification Daemon has no effect on SOCKS. The Identification Daemon has no configurable options.

**Related Topics**

- “Security Properties Dialog Box” on page 511

**Socks Configuration Dialog Box**

**Getting there**

The way you access the **SOCKS Configuration** dialog box depends on the session type you are in.

**Terminal session**

1. Open the Document Settings dialog box.
   
   The steps depend on your user interface mode (page 120).
2 Under **Host Connection**, click **Setup Connection Security**.
3 (3270 and 5250 terminal sessions only) Under **Security**, click **Security Settings**.
4 In the Security Properties dialog box, on the **Proxy** tab, click **Use proxy server**.
5 Under **Proxy type**, select **SOCKS** and then click **Configure**.

**Printer session**
1 Open a printer session.
2 On the **Connection** menu, click **Session Setup**.
3 Click **Security**.
4 In the Security Properties dialog box, on the **Proxy** tab, click **Use proxy server**.
5 Under **Proxy type**, select **SOCKS** and then click **Configure**.

**FTP Client**
1 In the **Connect to FTP Site** dialog box, select a site.
2 Click **Security**.
3 In the Security Properties dialog box, on the **Proxy** tab, click **Use proxy server**.
4 Under **Proxy type**, select **SOCKS** and then click **Configure**.

Use this dialog box to designate SOCKs proxy servers. You can designate a single SOCKs proxy server through which all requested connections must pass or use Advanced options to designate multiple SOCKs proxy servers.

**SOCKS proxy**
Enter information to designate a single SOCKS proxy server. If you want to configure more than one proxy server or configure specific destination routes, leave the the fields in the SOCKS proxy group blank and click Advanced.

**Server address**
Type the SOCKS proxy server address in this box.

**Protocol version**
Choose the protocol version your server uses from the menu.

**Advanced**
Click to configure multiple SOCKS proxy servers and destination routing filters for connection requests (see the following Advanced options).

**Advanced options**
Configure multiple proxy servers in order of preference. When a connection is requested, the client attempts to match the request with these addresses, beginning at the top of the list and moving down. The final line in the list, "Any address on any port", serves as a match for any request and prevents a connection request from being ignored.
To bypass a proxy server, select it from the list of destinations, click **Change**, and select the **Do not use...** check box.

**Destination**
- Specifies the name or IP address as well as the port number of one or more destination hosts. (Asterisks in an IP address represent wildcard characters.)

**Proxy**
- Specifies the name or IP address of the proxy server associated with the corresponding destination address. When a connection request is made to this destination address, the request must go through the proxy server indicated. "(Do not use proxy)" means that a proxy server will not be used when connection requests are made to the corresponding destination address.

**Proxy User ID**
- Specifies the user ID associated with a destination address and proxy server. User IDs can serve a variety of purposes: identification, definition of special privileges, etc. A user ID may or may not be required by the associated proxy server. Check with your system administrator to determine if a user ID is required.

**New**
- Opens the **New Routing Filter** dialog box in which you can add new entries to the destination routing list.

**Delete**
- Deletes the selected entry on the destination routing list. You cannot delete the final entry in this list.

**Change**
- Opens the **Change Routing Filter** dialog box in which you can edit the selected entry on the destination routing list. You cannot edit the destination in the final entry "Any address on any port".

To bypass click the destination route for which you want to bypass the proxy server.

**Up and Down arrows**
- Moves the selected entry up or down one line in the list.

---

**Set up a SOCKS or HTTP Proxy Server Session**

You can configure sessions to connect through a SOCKS proxy server or an HTTP server.

**NOTE**
- SOCKS is supported for VT, 3270, and 5250 terminals.
- HTTP is supported only for VT terminals.

**Before you start**

Make sure your system has a proxy server or servers and that you know the following information:

- If you are setting up a connection to a SOCKS server, know the proxy server address and protocol version.
- If you are setting up a connection to an HTTP server, know the proxy server address and port.

**To set up a session to connect through a SOCKS proxy server or an SSL/TLS server**

1. Open the Create New Document dialog box.
   - The steps depend on your **user interface mode** (page 120).
2 From the Create New Document dialog box, select a document template and click Create.

3 In the Create New Terminal Document dialog box, under Connection, enter the Host name/IP address.

4 Click Configure additional settings and then click OK.

5 In the Settings dialog box, under Host Connection, click Setup Connection Security.

6 If you are configuring a 3270 or 5250 terminal session, in the Configure Advanced Connection Settings dialog box, Under Security, click Security Settings.

7 On the Security Properties dialog box Proxy tab, select Use proxy server and then select the proxy type:
   - SOCKS (supported for VT, 3270, and 5250 terminals).
   - HTTP (supported only for VT).

8 Click Configure.

9 If you want to designate only one HTTP proxy server, configure the session for the proxy server as follows:

   To configure... Do this
   SOCKS Enter the Server address and the Protocol version.
   HTTP Enter the server Address and Port.
               If you want to use authentication that requires a user name and password, select Basic authentication and enter the user name for the proxy server. (If this is not selected, no authentication is used.)

10 If you want to configure more than one proxy server or configure specific destination routes, leave the fields in the HTTP (or SOCKS) proxy group blank and click Advanced.

HTTP Configuration Dialog Box

Getting there

The way you access the HTTP Configuration dialog box depends on the session type you are in.

Terminal session

1 Open the Document Settings dialog box.
   The steps depend on your user interface mode (page 120).
Secure Connections

2 Under **Host Connection**, click **Setup Connection Security**.

3 (3270 and 5250 terminal sessions only) Under **Security**, click **Security Settings**.

4 In the Security Properties dialog box, on the **Proxy** tab, click **Use proxy server**.

5 Under **Proxy type**, select **HTTP** and then click **Configure**.

### Printer session

1 Open a printer session.

2 On the **Connection** menu, click **Session Setup**.

3 Click **Security**.

4 In the Security Properties dialog box, on the **Proxy** tab, click **Use proxy server**.

5 Under **Proxy type**, select **HTTP** and then click **Configure**.

### FTP Client

1 In the **Connect to FTP Site** dialog box, select a site.

2 Click **Security**.

3 In the Security Properties dialog box, on the **Proxy** tab, click **Use proxy server**.

4 Under **Proxy type**, select **HTTP** and then click **Configure**.

Use this dialog box to designate HTTP proxy servers. You can designate a single HTTP proxy server through which all requested connections must pass or use **Advanced** options to designate multiple HTTP proxy servers.

### HTTP proxy

Enter information to designate a single HTTP proxy server. If you want to configure more than one proxy server or configure specific destination routes, leave the the fields in the **HTTP proxy** group blank and click **Advanced**.

<table>
<thead>
<tr>
<th>Address</th>
<th>Enter the HTTP proxy server address.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Enter the port of the proxy server.</td>
</tr>
<tr>
<td>Basic auth</td>
<td>Select if you want to use authentication that requires a user name and password. (If this is not selected, no authentication is used.)</td>
</tr>
<tr>
<td>User ID</td>
<td>Enter the user name for the proxy server.</td>
</tr>
<tr>
<td>Advanced</td>
<td>Click to configure multiple HTTP proxy servers and destination routing filters for connection requests (see the following Advanced options).</td>
</tr>
</tbody>
</table>
Advanced options

Configure multiple proxy servers in order of preference. When a connection is requested, the client attempts to match the request with these addresses, beginning at the top of the list and moving down. The final line in the list, "Any address on any port", serves as a match for any request and prevents a connection request from being ignored.

To bypass a proxy server, select it from the list of destinations, click Change, and select the Do not use... check box.

Destination Specifies the name or IP address as well as the port number of one or more destination hosts. (Asterisks in an IP address represent wildcard characters.)

Proxy Specifies the name or IP address of the proxy server associated with the corresponding destination address. When a connection request is made to this destination address, the request must go through the proxy server indicated. "(Do not use proxy)" means that a proxy server will not be used when connection requests are made to the corresponding destination address.

Proxy User ID Specifies the user ID associated with a destination address and proxy server. User IDs can serve a variety of purposes: identification, definition of special privileges, etc. A user ID may or may not be required by the associated proxy server. Check with your system administrator to determine if a user ID is required.

New Opens the New Routing Filter dialog box in which you can add new entries to the destination routing list.

Delete Deletes the selected entry on the destination routing list. You cannot delete the final entry in this list.

Change Opens the Change Routing Filter dialog box in which you can edit the selected entry on the destination routing list. You cannot edit the destination in the final entry "Any address on any port".

To bypass click the destination route for which you want to bypass the proxy server.

Up and Down arrows Moves the selected entry up or down one line in the list.

Routing Filter Dialog Box

Getting there

The way you access the Security Properties dialog box depends on the session type you are in.

Terminal session

1. Open the Document Settings dialog box.

The steps depend on your user interface mode (page 120).
Secure Connections

User Interface Mode

**Ribbon or Reflection Browser**
Steps with a session open in Reflection, from the Quick Access Toolbar, click. Tap the Gear icon and then select **Document Settings**.

**TouchUX**

**Steps**

2 Under **Host Connection**, click **Setup Connection Security**.
3 (3270 and 5250 terminal sessions only) Under **Security**, click **Security Settings**.

Printer session

1 Open a printer session.
2 On the **Connection** menu, click **Session Setup**.
3 Click **Security**.

**FTP Client**

1 In the **Connect to FTP Site** dialog box, select a site.
2 Click **Security**.

Specify the destination routing filters for connection requests, for SOCKS or HTTP configurations.

**NOTE:** You cannot change the destination address and port of the final entry in the destination route list. You can, however, change the SOCKS or HTTP proxy information for this entry.

<table>
<thead>
<tr>
<th>Destination address</th>
<th>Specifies the host name or IP address of the destination that is controlled by the associated proxy server (Asterisks in an IP address represent wildcard characters.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Specifies the port associated with the destination address.</td>
</tr>
</tbody>
</table>

**Do not use SOCKS (or HTTP) proxy**

When this check box is selected, a connection request matching this destination route will bypass the proxy server (destination).

**SOCKS (HTTP) proxy**

Specifies the **Address**, **Port**, and **User ID** of the proxy server. These settings are available only if **Do not use SOCKS (or HTTP) proxy** is cleared.

**Kerberos Connections**

In this Section

- “Kerberos Overview” on page 462
- “Connect Using Kerberos” on page 462
- “Reflection Kerberos Initial Configuration Dialog Box” on page 464
- “Kerberos Manager” on page 465
Kerberos Overview

Index Term
Primary: Kerberos (Secure Shell connections)
Secondary: overview

Kerberos is a protocol that uses a trusted third party to enable secure communications over a TCP/IP network. The protocol uses encrypted tickets rather than plain-text passwords for secure network authentication.

A user logs onto a workstation using a password (secret key) that is also known by a trusted third party, the Key Distribution Center (KDC). The KDC authenticates the user and issues a ticket-granting ticket (TGT) that lets the user request and obtain service tickets as needed to access kerberized servers for the lifetime of the TGT. In addition to authenticating the client, Kerberos connections can also be configured to authenticate the server and encrypt the data stream. A Kerberos security scheme involves the interaction of several components:

- The Key Distribution Center (KDC), which authenticates users and issues tickets for kerberized services.
- The kerberized server applications that users want to access. (Kerberized servers may be server daemons, telnetd, or ftpd running on host machines.)
- The kerberized client applications that request authentication and allow the user to access server applications. Because most Reflection applications include Kerberos client services, we'll refer to them collectively as the Reflection Kerberos client throughout this document. (You can configure and manage Kerberos settings for the Reflection Kerberos client using Reflection Kerberos Manager. However, it isn't required.)

Data Encryption Standards

Reflection Kerberos supports the following data encryption standards:

- DES (56-bit)
- TripleDES (168-bit)

Related Topics

- “The Kerberos Authentication Process” on page 465

Connect Using Kerberos

Kerberos is a protocol that uses a trusted third party to enable secure communications over a TCP/IP network. The protocol uses encrypted tickets rather than plain-text passwords for secure network authentication and also supports encryption of the data stream.

After you configure a session using Kerberos, you can export these settings to an XML file in order to deploy them. The first time a user opens a Reflection Kerberos session, these settings are imported into the registry.

**NOTE:** Kerberos connections are available for VT terminal sessions.

Before you start

Make sure you know the following information:
If you are configuring Kerberos using Windows credentials:

- You must be logged into a Windows domain.
- You must know the fully qualified name of a host that is running a kerberized server application (such as `telnetd` or `ftpd`) and that has been joined to the Windows domain.

If you are configuring Kerberos using a KDC, Make sure your system has a KDC server and that you know:

- The fully-qualified name of a host that is properly configured and running a kerberized server application (such as `telnetd` or `ftpd`).
- The fully qualified KDC host name.
- The Kerberos principal (and password) with which you will be authenticating.
- The Kerberos realm.

**To configure a secure terminal session using Kerberos**

1. **Open the Create New Document dialog box.**
   
   The steps depend on your **user interface mode** (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ribbon or Reflection Browser</td>
<td>From the Quick Access Toolbar, click the <strong>New Document</strong> button.</td>
</tr>
<tr>
<td>TouchUx</td>
<td>Tap the Folder icon and then under File, select <strong>New</strong>.</td>
</tr>
</tbody>
</table>

2. From the **Create New Document** dialog box, select a session template and click **Create**.

3. For **Host Name/IP Address**, enter the fully qualified host name.

4. Select **Configure additional settings**, and then click **OK**.

5. Under **Host Connection**, click **Set Up Connection Security**.

6. From the **Security Properties** dialog box, click the **Kerberos** tab, and select **Reflection Kerberos**.

   **NOTE:** Unless your PC has a Kerberos Manager configuration file installed, the **Reflection Kerberos Initial Configuration** (page 464) dialog box is displayed the first time you use **Reflection Kerberos**. You must specify default Kerberos settings in this dialog box before you can make a connection.

7. Do one of the following:
   - Select Use Windows logon values.
   - OR-
   - Enter values for **Default Principal**, **Default Realm**, and **KDC host name**.

8. Click **OK** to close the **Reflection Kerberos Initial Configuration** dialog box.

9. Configure any additional Kerberos options that you want to use for this connection and click **OK** to close the **Security Properties** dialog box.

10. Click **OK** to close the **Settings for VT** dialog box and initiate the connection. When prompted, enter your password.
After a connection is established, click the Save button on the Quick Access toolbar and save the session document.

Click OK to close the open dialog boxes and return to the workspace.

Related Topics

- “Kerberos Authentication” on page 465
- “Configuring and Managing Kerberos Realms” on page 467
- “Obtaining and Managing Kerberos Tickets” on page 478
- “Configuring Encryption” on page 484
- “Exporting Kerberos Settings” on page 498
- “Troubleshooting Kerberos” on page 501

Reflection Kerberos Initial Configuration Dialog Box

Index Term
Primary: Initial Configuration dialog box (Kerberos Manager)

This dialog box appears the first time you use Kerberos, and must be completed before you can make a secure Kerberos connection. Check with your system administrator for values for principal, realm, and KDC host. You can use the default value for the credentials file.

The options are:

**Default Principal**
Specify an entity that's recognized by the Kerberos server. Each principal has a unique name within a realm. The format of a full principal name is:

`principal_name@realm_name`

The default principal is set automatically to your Windows user name (in lowercase).

**Default Realm**
Specify the realm you want to associate with this principal profile. A realm is a name given to a collection of Kerberos principals on a network. If you omit the realm name, the default realm is assumed.

The realm name is case sensitive, and typically uppercase. It is often similar to or the same as the domain name, for example, XYZ.MFG.COM.

**KDC host name**
Specify the default KDC (Key Distribution Center) host, or Windows primary domain controller.

**Credentials file**
Specify the location where you want to store the session key and TGT (ticket granting ticket) issued by the KDC. The client uses these credentials to authenticate itself when it requests a service.

**Use Windows logon values**
Select this option to use your Windows credentials whenever a ticket-granting ticket (TGT) is needed and there is no valid TGT in the cache.

This option is available only if you log on to a Windows domain and your system supports this feature.
NOTE: Information that you configure about Kerberos principals, realms, and tickets is saved in your Windows registry and this information applies to all installed Reflection applications that support Kerberos.

**Kerberos Manager**

Reflection Kerberos Manager is an application that you can use to perform Kerberos management tasks. For example, you can create or modify principal profiles, add or modify realms, set ticket lifetimes, and import and export Kerberos settings.

You may also be able to configure security clients directly from your kerberized client application. For example, in InfoConnect you can configure clients to use Kerberos by specifying your principal name and selecting a realm.

**Related Topics**

- “Starting Kerberos Manager” on page 465
- “Kerberos Overview” on page 462

**Starting Kerberos Manager**

- From the Windows Start Menu, go to Attachmate Reflection > Utilities > Kerberos Manager.
- or -
- Open the Security Properties dialog box, click the Kerberos tab, and then click Kerberos Manager.

**Related Topics**

- “Kerberos Manager” on page 465

**Kerberos Authentication**

**In this Section**

- “The Kerberos Authentication Process” on page 465
- “Authenticate to the Host” on page 466
- “Authenticate Dialog Box” on page 467

**The Kerberos Authentication Process**

Understanding the sequence of events that occurs during Kerberos authentication may help you determine the cause of authentication problems.

1. A principal requests a service that requires Kerberos authentication. For example, a user starts InfoConnect (a Telnet client) and requests a Telnet connection to a host named telnserf.com.
2. The application server (in this case, the Telnet daemon on the host) requests authentication from InfoConnect.
3. InfoConnect checks to see if Kerberos already has a valid ticket-granting ticket (TGT) for this principal. If it doesn't, the Reflection Kerberos client sends a request to the Key Distribution Center (KDC) for a TGT.
4. The KDC verifies that the principal and realm are valid, and then sends a TGT and a session key
to the Reflection Kerberos client.

5. The Reflection Kerberos client prompts the user for a password. If it matches the password the
KDC used to encrypt the TGT and session key, the Reflection Kerberos client can decrypt the
message and obtain the session key. (If the password is incorrect, the user sees an error
message and authentication fails.)

6. The Reflection Kerberos client generates the request for the service that the user originally
requested (a Telnet connection to telnerv.com), and sends it to the KDC. This request contains
the TGT, an authenticator that verifies the principal's identity, and the name of the service the
principal wants to use, all encrypted in the session key.

7. The KDC decrypts the TGT, and then generates a new key for the session between the
workstation and the service (in this case, between the Telnet client and the Telnet daemon on
telnerv.com), and a service ticket for the Telnet connection to telnerv.com, which is encrypted
with the service's secret key. It encrypts this message with the original session key, and returns it
to the Reflection Kerberos client.

8. The Reflection Kerberos client uses the original session key to extract the service ticket and
decrypt the new session key. It then returns control to InfoConnect.

9. InfoConnect presents the service ticket to the Telnet daemon. The Telnet daemon verifies the
credentials and in turn authenticates itself to InfoConnect using information it extracted from the
service ticket. Since the service ticket was encrypted with the service's secret key, only the
service for which the ticket was generated could decrypt the ticket.

10. InfoConnect logs in to the host (telnerv.com).

Authenticate to the Host

Index Term
   Primary: authenticating
   Secondary: from the Reflection Kerberos Manager

After you configure the Reflection Kerberos client, you can authenticate to the host.

NOTE: If the Challenge/Response dialog box opens during authentication, your KDC host requires
hardware pre-authentication. Hardware pre-authentication involves a physical token, typically the size
of a credit card with a touchpad and LCD display, which generates random passwords. Use your pre-
authentication hardware token to enter the correct response, and then click OK.

To authenticate using Kerberos Manager

1. Start Kerberos Manager.
2. Click the tab corresponding with the principal profile you want to use for authentication.
   If the principal profile you want to use is hidden, you must open it.
3. Click the Authenticate button.
4. Modify the ticket features, if desired, and then click OK to continue.
5. Type the password, and then click OK.
   If authentication is successful, a ticket-granting ticket appears in the Kerberos Manager main
   window. If authentication is not successful, Kerberos Manager returns an error.

To authenticate using a kerberized application

1. Configure the kerberized application to use Kerberos security.
   When you connect to the host, you are prompted for your Kerberos password.
Type the password, and then click **OK**.

If authentication was successful, the host prompt appears and a key or padlock icon may appear on the status bar. If the authentication was not successful, an error message appears.

**Related Topics**

- “Authenticate Dialog Box” on page 467
- “Starting Kerberos Manager” on page 465

**Authenticate Dialog Box**

**Index Term**

**Primary:** Authenticate dialog box (Kerberos Manager)

**Getting there**

1. In **Reflection Kerberos Manager**, click the tab of the principal profile you want to use for authentication.
2. Click the **Authenticate** button in the lower-left corner of the tab.

From this dialog box, you can authenticate the named principal, modify the ticket lifetime or renewal time, and enable ticket forwarding. Ticket forwarding and renewable tickets settings apply to the current connection only.

After you authenticate to a particular realm, you can connect to any host in that realm without having to re-type your password, unless you change any ticket options.

The options are:

**Ticket lifetime**

Specify the period of time for which your ticket-granting ticket is valid. Changes you make to this value affect the current ticket only and override the default value, which uses the ticket lifetime from the Realm Defaults tab. The Key Distribution Center (KDC) determines the lifetime of a Kerberos ticket and overrides requests that fall outside of the allowed range.

**Forwardable tickets**

Select this option to allow the TGT to be forwarded to another host and to get service tickets for additional services in the current connection.

**Renewable duration**

Specify a time interval for renewable tickets for the current connection. You must also click **Renew ticket** on the principal profile tab to renew your ticket for the specified interval. If the interval is set to zero, the ticket is not renewable.

**Related Topics**

- “Authenticate to the Host” on page 466

**Configuring and Managing Kerberos Realms**

You must specify the realm that contains the principals and Kerberos authentication services for the network.

**NOTE:** If the **Configure Realms** command is unavailable (dimmed), your system administrator has disabled this capability. Contact your system administrator for information about how to add or change the realms you may use.
Add or Remove a Realm

Index Term
Primary: removing
Secondary: realm

Index Term
Primary: adding
Secondary: realm

1 Start Kerberos Manager.
2 From the Configuration menu, choose Configure Realms.
3 Do one of the following:
   - To add a realm, click Add, type the name of the realm (Kerberos realm names are usually uppercase; in a DCE environment, realms or cells are always lowercase) and type the full name of the host that is running the security server (or KDC (page 888)) for this realm, and then click OK.
   - or -
   - To remove a realm, click Remove, and then when the message appears telling you that removing a realm invalidates any storage using that realm, click OK.

Related Topics
- “Add Realm Dialog Box” on page 473
Specify the Default Realm

Index Term
Primary: realms
Secondary: specify default

Index Term
Primary: defaults (Kerberos Manager)
Secondary: specifying the default realm

1 Start Kerberos Manager.
2 From the Configuration menu, choose Configure Realms.
3 Click the User Defaults tab.
4 In the Default realm box, select the realm you want to use as the default from the list, and click OK.
   The realm you specify here is the default for a new user or profile.

Related Topics
• “User Defaults Tab (Configuration Dialog Box)” on page 477

Add or Remove a KDC from a Realm

Index Term
Primary: removing
Secondary: KDC from a realm

Index Term
Primary: realms
Secondary: arranging the order of KDCs

Index Term
Primary: realms
Secondary: add/remove KDCs

Index Term
Primary: adding
Secondary: KDC to a realm

1 Start Kerberos Manager.
2 From the Configuration menu, choose Configure Realms.
3 From the Configuration tab, select a realm from the Realm list, and then click Properties.
4 Click the KDC tab.
5 Perform one of the following tasks:
   • To add a KDC, click Add, type the fully qualified domain name of the KDC host, and click OK.
     If necessary, adjust the order of the KDCs in the KDC list by clicking the Up or Down buttons.
     -or-
   • To remove a KDC, select the KDC in the KDC list, click Remove, and then, when the confirmation message appears, click Yes.
6 Click OK.
Specify the Administrative KDC for a Realm

If you have multiple KDC hosts configured, specify one KDC as the primary controller or master KDC.

To define the administrative KDC for a realm

1. Start Kerberos Manager.
2. From the Configuration menu, choose Configure Realms.
3. From the Configuration tab, select a realm from the Realm list, and then click Properties.
4. Click the KDC tab.
5. In the Kadmin Server box, type the full name of the host that you want as the administrative KDC, and then click OK.

Related Topics

- “Configuration Tab (Configuration Dialog Box)” on page 475

Add or Remove an Application Server from a Realm

An application server (or host) can belong to only one realm at a time. If an application server already belongs to a realm and you add it to a new realm, Kerberos Manager will delete the application server from the original realm and add it to the currently specified realm.

To add or remove an application server

1. Start Kerberos Manager.
2. From the Configuration menu, choose Configure Realms.
3. From the Configuration tab, select a realm from the Realm list, and then click Properties.
4 Click the **Hosts** tab.

5 Perform one of the following tasks:
   - To add an application server, click **Add**, type the fully qualified domain name of the host (not the IP address of the host), and then click **OK**.
   - or-
   - To remove an application server, select the host in the **Hosts in realm** list, and then click **Remove**.

6 Click **OK**.

**Related Topics**

- “Configuration Tab (Configuration Dialog Box)” on page 475
- “Hosts Tab (Realm Properties Dialog Box)” on page 478

### Configure a Realm to Use Windows Logon Credentials

**Index Term**

Primary: Windows KDC  
Secondary: using Windows logon credentials

**Index Term**

Primary: authenticating  
Secondary: using Windows logon credentials

If you configure a realm to use your Windows logon credentials, the Reflection Kerberos client uses those credentials to get service tickets.

If the Windows realm and user name don't match those specified in your principal profile, you are prompted to authenticate with your Kerberos password.

**To configure a realm to use a Windows logon**

1 Log on to a Windows domain.

2 Start **Kerberos Manager**.

3 From the **Configuration** menu, choose **Configure Realms**.

4 From the **Configuration** tab, select a realm from the **Realm list**, and then click **Properties**.

5 On the **KDC** tab, select **Use Windows logon credentials**, and then click **OK**.

   The required fields complete automatically using your existing credentials.

**Related Topics**

- “KDC Tab (Realm Properties Dialog Box)” on page 476

### Configure a Realm to Use Leash32 Credentials

**Index Term**

Primary: Leash32 credentials

**Index Term**

Primary: authenticating  
Secondary: using Leash32 credentials
If you configure a realm to use Leash32, the Reflection Kerberos client uses your Leash32 credentials to get service tickets. If you authenticate to the KDC through Leash32, you don’t need to reenter your Kerberos passwords.

**NOTE:** This option is available only if your system has the Kerberos for Windows distribution installed to the same folder as the Reflection products, or the folder containing the Kerberos for Windows distribution is in your system's PATH statement. (The Reflection Kerberos client determines if your system is correctly configured by searching for Krb5_32.dll.)

### To configure a realm to use Leash32

1. Start Kerberos Manager.
2. From the Configuration menu, choose Configure Realms.
3. From the Configuration tab, select a realm from the Realm list, and then click Properties.
4. On the KDC tab, select Use Leash32 cache, and then click OK.
5. Click OK.

**Related Topics**

- “KDC Tab (Realm Properties Dialog Box)” on page 476

### Disable Pre-authentication

**Index Term**

- Primary: pre-authentication

**Index Term**

- Primary: authenticating
  - Secondary: using pre-authentication

The Reflection Kerberos client pre-authenticates to the KDC (recommended) by default; however, you may need to disable pre-authentication if it isn't compatible with KDCs in your network.

During pre-authentication, the Reflection Kerberos client prompts the user for a password, and then using a key derived from the password, encrypts a timestamp, which it includes in its authentication request to the KDC. If the KDC can decrypt the timestamp with the user's key (derived from the same password using the same algorithm), it proves that the user knows the password.

### To disable pre-authentication

1. Start Kerberos Manager.
2. From the Configuration menu, choose Configure Realms.
3. From the Configuration tab, select a realm from the Realm list, and then click Properties.
4. Click the Realm Defaults tab.
5. From the Pre-Authentication box, select None, and then click OK.

**Related Topics**

- “Realm Defaults Tab (Realm Properties Dialog Box)” on page 475
Change your Password

Index Term
Primary: passwords
Secondary: changing, (Kerberos Manager)

An administrative KDC (Kadmin server) must be designated for a realm before you can change the password for a principal profile on that realm.

To change a password in Kerberos Manager

1. Start Kerberos Manager.
2. Click the tab for the principal profile for which you want to change the password. If the principal profile you want is hidden, you will need to open it.
3. From the Tools menu, choose Change Password. Confirm that you are changing the password for the correct principal.
4. Type the old password, the new password, and then type the new password again for verification.
5. Click OK.

NOTE: Note for system administrators: If you use MIT Kerberos 5 (Release 1) servers, or other compatible servers, the Kerberos client automatically tries to change the password using the kpasswd method (using service principal kadmin/changepw@REALM). If this fails, the client then tries the v5passwd method (using service principal changpw/REALM@REALM).

If you use the older v5passwd client, the MIT KDC system must run v5passwdd, which isn't installed by default. If you need to specify the port on which the v5passwdd daemon is running, edit the Services file, located in the Windows folder in the \system32\drivers\ folder, to add a line similar to the following:

```
kerberos-adm [port_number]/tcp
```

If the daemon runs on port 1000, for example, add the line:

```
kerberos-adm 1000/tcp
```

Add Realm Dialog Box

Index Term
Primary: Add Realm dialog box

Getting there

1. From the Configuration menu, choose Configure Realms.
2. On the Configuration tab, click Add.

NOTE: If the Configure Realms command is unavailable (dimmed), your system administrator has disabled this capability. Contact your system administrator for information about how to add or change the realms you may use.

From this dialog box, you can add a new realm to the Realm list.
The options are:

**Realm**
Type the realm name that you want to add. The realm name is case sensitive — usually uppercase in a Kerberos environment.

**KDC host**
Type the name of the host that runs the security server for this realm. You must specify at least one KDC (Key Distribution Center) host that will govern the realm. If this realm contains multiple security servers, determine which server is the administrative KDC, and then specify it here.

**Related Topics**
- “Specify the Administrative KDC for a Realm” on page 470

**Add Host to Realm Dialog Box**

**Getting there**
1. From the **Configuration** menu, choose **Configure Realms**.
2. From the **Configuration** tab, select a realm from the **Realm list**, and then click **Properties**.
   
   **NOTE:** If the **Configure Realms** command is unavailable (dimmed), your system administrator has disabled this capability. Contact your system administrator for information about how to add or change the realms you may use.
   
3. Click the **Hosts** tab.
4. Click the **Add** button.

From this dialog box, you can add an application server or host to the realm.

**Host**
Type the name of the application host you want to add to this realm. The application host should be running a kerberized application, such as a kerberized Telnet daemon or kerberized FTP daemon. If the host is running security server software, add it to the **KDC list**.

New hosts appear in the **Hosts in realm** list on the **Hosts** tab. If you add a host that is defined in a different realm, it's added to the current realm and deleted from the list of hosts in the old realm.

**Add KDC Dialog Box**

**Getting there**
1. From the **Configuration** menu, choose **Configure Realms**.
2. From the **Configuration** tab, select a realm from the **Realm list**, and then click **Properties**.
3. Click the **KDC** tab.
4. Click the **Add** button.
NOTE: If the Configure Realms command is unavailable (dimmed), your system administrator has disabled this capability. Contact your system administrator for information about how to add or change the realms you may use.

From this dialog box, you can add a KDC (Key Distribution Center) to the designated realm.

**KDC host**
Type the name of the KDC (Key Distribution Center) you want to add to this realm. The new KDC appears at the bottom of the KDC list on the KDC tab. Use the Up and Down buttons to move it to the position you want in the list.

**Configuration Tab (Configuration Dialog Box)**

**Getting there**
1. From the Configuration menu, choose Configure Realms.
2. Click the Configuration tab.

NOTE: If the Configure Realms command is unavailable (dimmed), your system administrator has disabled this capability. Contact your system administrator for information about how to add or change the realms you may use.

From this tab, you can add a new realm, or remove or modify the properties of an existing realm.

The options are:

**Realm list**
Displays a list of current realms.

**Add**
Click to add a realm and a KDC (Key Distribution Center) host to the Realm list.

**Remove**
Click to remove the selected realm from the Realm list.

**Properties**
Click to reconfigure or view properties for the selected realm.

**Realm Defaults Tab (Realm Properties Dialog Box)**

**Index Term**
Primary: defaults (Kerberos Manager)
Secondary: Realm Defaults tab
Getting there

1. From the **Configuration** menu, choose **Configure Realms**.
2. From the **Configuration** tab, select a realm from the **Realm list**, and then click **Properties**.
3. Click the **Realm Defaults** tab.

**NOTE:** If the **Configure Realms** command is unavailable (dimmed), your system administrator has disabled this capability. Contact your system administrator for information about how to add or change the realms you may use.

From this tab, you can configure the defaults for the selected realm. These settings are used when you create new principal profiles and when you authenticate; however, you can modify your settings when you authenticate to obtain a new TGT (ticket granting ticket).

The options are:

**Ticket lifetime**  
Set the default ticket lifetime using hours, minutes, and seconds. The lifetime is the length of time a ticket-granting ticket will be valid. The KDC (Key Distribution Center) determines the lifetime of a Kerberos ticket, and overrides requests that fall outside of the allowed range.

**Ticket renew time**  
Set a default ticket renewal time using days, hours, and minutes. When no interval is specified, the ticket is not renewable.

**Pre-Authentication**  
Specify whether you want to perform encrypted timestamp pre-authentication.

**Forwardable ticket**  
Select this option to forward your TGTs (and TGTs for all principal profiles in this realm) to another host and get service tickets on your behalf.

**Ticket Address**  
Specify the IP address or a network host name used in the TGT. You can enter up to four IP addresses separated by commas. By default, InfoConnect uses your computer's current IP address. If you connect through a firewall or in a NAT (Network Address Translation) environment, you may need to specify your firewall or NAT IP address.

Clear this box to obtain a ticket that contains no IP address.

**Reset**  
Click to reset the IP address used in the TGT to your computer's IP address.

**KDC Tab (Realm Properties Dialog Box)**

**Index Term**  
**Primary:** Key Distribution Center (KDC)  
**Secondary:** arranging the order

**Index Term**  
**Primary:** KDC tab

Getting there

1. From the **Configuration** menu, choose **Configure Realms**.
2. From the **Configuration** tab, select a realm from the **Realm list**, and then click **Properties**.
3. Click the **KDC** tab.
NOTE: If the Configure Realms command is unavailable (dimmed), your system administrator has disabled this capability. Contact your system administrator for information about how to add or change the realms you may use.

From this tab, you can add or remove a KDC (Key Distribution Center), and rearrange the order of KDCs for the selected realm. You can also define an administrative KDC for the realm and specify UDP or TCP for communications.

The options are:

**KDC list**
Displays the current list of KDCs. The order of hosts in the KDC list determines the order in which the KDCs attempt to service an authentication request. If the first KDC in the list fails to service a request, the next KDC makes an attempt, and so on.

Use the **Up** and **Down** buttons to change the order of the list.

**Kadmin server**
Specifies the administrative KDC or master for this realm. You must specify a master KDC to change passwords.

**Use Windows logon credentials**
When selected, Reflection uses your Windows credentials to supply Kerberos identification and authentication.

This option is available only if you're logged on to a Windows domain and your system is configured to support this feature.

**Use Leash32 cache**
When selected, the Reflection Kerberos client uses your Leash32 credentials cache to obtain service tickets. If you authenticate to the KDC through Leash32, you don't need to reenter your Kerberos passwords.

This option is available only if you installed Leash32 on your system.

**Maximum UDP packet size**
Specifies the maximum packet size for UDP communications with the KDC. The Reflection Kerberos client uses UDP as the default protocol for communications unless the packet size exceeds the value specified, in which case, it uses TCP.

Set the value to zero to use only TCP.

Decrease this value if you have trouble authenticating to a Windows KDC and you belong to a large number of groups, or if **Use Windows logon credentials** is selected.

**Related Topics**
- “Configure a Realm to Use Windows Logon Credentials” on page 471
- “Configure a Realm to Use Leash32 Credentials” on page 471

**User Defaults Tab (Configuration Dialog Box)**

**Index Term**
Primary: User Defaults tab (Kerberos Manager)

**Index Term**
Primary: defaults (Kerberos Manager)
Secondary: User Defaults tab

**Getting there**
1. From the **Configuration** menu, choose **Configure Realms**.
2. Click the **User Defaults** tab.
NOTE: If the Configure Realms command is unavailable (dimmed), your system administrator has disabled this capability. Contact your system administrator for information about how to add or change the realms you may use.

From this tab, you can specify the default realm and storage medium for your PC.

The options are:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default realm</td>
<td>Select a realm from the list. This default determines the realm that the Reflection Kerberos client uses when a new user requests Kerberos authentication.</td>
</tr>
<tr>
<td>Default storage media</td>
<td>Specify the storage medium you want to use when you create a new principal profile. (You can not use hidden storage as a default.) You can override the Default storage media setting by selecting a Storage media setting when you create a new profile.</td>
</tr>
</tbody>
</table>

Hosts Tab (Realm Properties Dialog Box)

Index Term
Primary: Hosts tab (Kerberos Manager)

Getting there

1. From the Configuration menu, choose Configure Realms.
2. From the Configuration tab, select a realm from the Realm list, and then click Properties.
3. Click the Hosts tab.

NOTE: If the Configure Realms command is unavailable (dimmed), your system administrator has disabled this capability. Contact your system administrator for information about how to add or change the realms you may use.

From this tab, you can add or remove an application server or host for the realm specified on the Configuration tab. Any host running a KDC (Key Distribution Center) is automatically included in the KDC list.

The options are:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hosts in realm</td>
<td>Displays all hosts for the realm.</td>
</tr>
<tr>
<td>Add</td>
<td>Click to add a host to the realm.</td>
</tr>
<tr>
<td>Remove</td>
<td>Click to remove the selected host from the realm.</td>
</tr>
</tbody>
</table>

NOTE: To connect to the hosts on this tab, a kerberized application (such as a kerberized Telnet daemon or kerberized FTP daemon) must be installed and running.

Obtaining and Managing Kerberos Tickets

To gain access to a kerberized application, you must first obtain a ticket-granting ticket (TGT).

In this Section

- "Kerberos Tickets" on page 479
Kerberos Tickets

There are two types of tickets in a Kerberos security system: ticket-granting tickets and service tickets. To gain access to a kerberized application, you must first obtain a ticket-granting ticket (TGT).

Ticket-Granting Tickets

When a user requests access to a service that requires Kerberos authentication, the KDC generates a TGT that consists of the user's principal name, the ticket expiration time, and a unique session key, all encrypted with the master key for the KDC. The KDC returns this TGT to the Reflection Kerberos client with a copy of the unique session key that is encrypted with a key derived from the user's password. If the Reflection Kerberos client can decrypt the session key (proving that the user knows the password), it can use the session key and TGT to obtain a service ticket.

After you've been granted a valid TGT, the Reflection Kerberos client obtains service tickets for this principal each time you request access to a kerberized application, throughout the lifetime of the ticket-granting ticket. As long as the TGT is valid, you can log in to kerberized applications as often as necessary without having to obtain another TGT.

A renewable ticket is a special TGT with a flag set indicating that it can be renewed. When a TGT is about to expire, the user can request that it be renewed. If the TGT is renewable, the KDC sends the Reflection Kerberos client a new TGT that is valid for the period of time specified in the Kerberos tab of the Security Properties dialog box. The maximum lifetime and number of renewals are set by the system administrator of the KDC.

A forwardable ticket is a TGT that you can forward to another host and get service tickets for additional services without having to repeat the authentication process with the KDC. Tickets that have been forwarded once may be forwarded again.

Service Tickets

To gain access to a service that requires Kerberos authentication, the client application must present a valid service ticket. When the Reflection Kerberos client sends a service ticket request along with a valid TGT, the KDC issues a service ticket that consists of the user's principal name, a new session key for the workstation, and the service to use for this session, all encrypted with the service's master key. The KDC returns the service ticket to the Reflection Kerberos client with the name of the requested service and a copy of the new session key, which it encrypts with the original TGT session key.

The Reflection Kerberos client uses the original session key to decrypt the message, and extract the service ticket and key that it will use to establish a session with the service.

A service ticket usually remains valid for the life of the TGT. A new service ticket is required to log in to a different host, and may be required when requesting a different service on the same host.
Related Topics

- “Set Values for Ticket-Granting Tickets” on page 480
- “Renew a Ticket-Granting Ticket” on page 480
- “Obtain a Service Ticket” on page 481
- “Delete Tickets for Principal Profiles” on page 481

Set Values for Ticket-Granting Tickets

Index Term
Primary: tickets
Secondary: setting the ticket lifetime

Index Term
Primary: defaults (Kerberos Manager)
Secondary: setting ticket lifetime

You must specify the default values of all ticket-granting tickets for new principal profiles on the Realm Defaults tab. Changing the default value doesn't affect the ticket values for existing principal profiles.

The KDC (Key Distribution Center) ultimately determines the lifetime of a Kerberos ticket. The KDC can be configured to allow ticket lifetimes within a certain range, and overrides your request if it falls outside of the allowed range. (To get a TGT, you must authenticate to the host.)

NOTE: You can modify the settings for a current ticket in the Authenticate dialog box when you obtain a new ticket.

To set the default values for all tickets issued for a realm

1. Start Kerberos Manager.
2. From the Configuration menu, choose Configure Realms.
3. From the Configuration tab, select a realm from the Realm list, and then click Properties.
4. Click the Realm Defaults tab.
5. Specify a value for Ticket lifetime.
6. Select the Forwardable check box to enable ticket forwarding.
7. Specify a value for Ticket renew time, and then click OK.
8. Click OK.

Related Topics

- “Authenticate to the Host” on page 466

Renew a Ticket-Granting Ticket

Index Term
Primary: tickets
Secondary: renewing

Index Term
Primary: renewing a valid ticket (Kerberos Manager)
If your TGT (ticket-granting ticket) is still valid, you can renew it using Kerberos Manager or InfoConnect.

To renew a ticket from Kerberos Manager

- Click Renew Ticket from the principal profile tab.

To renew a ticket from InfoConnect

- Click Renew from the Kerberos tab of the Security Properties dialog box.

**Obtain a Service Ticket**

Index Term
Primary: service ticket, obtaining from Kerberos Manager

Index Term
Primary: obtaining a service ticket

1 In Kerberos Manager, complete the authentication process to obtain a ticket-granting ticket.
2 From the Credentials menu, choose Get Service Ticket.
3 In the Host name box, type the fully qualified domain name of the host for which you want a service ticket.
   Do not type the IP address of the host.
4 In the Service name box, specify the service type for the host you specified in step 3, and then click OK.
   For example, if you request a service ticket for a Telnet connection, the Service Name is "host."

**Delete Tickets for Principal Profiles**

Index Term
Primary: deleting tickets for principal profiles

Index Term
Primary: clearing tickets from a principal profile

1 Start Kerberos Manager.
2 Perform one of the following tasks:
   - To delete tickets for a principal profile, click the corresponding tab, and choose Credentials > Clear Tickets.
   -or-
   - To delete all tickets on the computer, choose Credentials > Clear All Tickets, or click the Clear All Tickets button from the toolbar.
3 Click Yes to confirm.

**NOTE:** To automatically delete tickets when the last kerberized application quits, choose Configuration > Clear All Tickets on Shutdown.

**Challenge/Response Dialog Box**

Index Term
Primary: Challenge/Response dialog box
If you connect to a KDC host that requires hardware pre-authentication, the **Challenge/Response** dialog box appears. You must use the required hardware token to determine the correct response to authenticate and complete the secure connection.

The options are:

- **A challenge issued by your host**: Displays the challenge issued by the KDC host.
- **A box for your response**: Type the password provided by the hardware pre-authentication token.

### Ticket Encryption Types Dialog Box

**Index Term**

**Primary**: Ticket Encryption Types dialog box

**Getting there**

1. From the **Configuration** menu, choose **Configure Realms**.
2. From the **Configuration** tab, select a realm from the **Realm list**, and then click **Properties**.
3. Click the **Encryption** tab.
4. Click the **Configure Encryption Types** button.

**NOTE:** If the **Configure Realms** command is unavailable (dimmed), your system administrator has disabled this capability. Contact your system administrator for information about how to add or change the realms you may use.

From this dialog box, you can define the ticket encryption types to request from the KDC. To require a specific encryption type for all connections, delete all other encryption types from the **Requested KDC encryption types** list. To ensure that a specific encryption type is used on servers that support it, move it to the top of the list.

**NOTE:** To configure the encryption type (or a list of encryption types) for a particular realm, select the realm on the **Configuration** tab before you add the encryption type in this dialog box.

The options are:

- **Requested KDC encryption types**: Displays all the requested encryption types.
- **Use password as MD5 IV**: When selected, your password is used as the initialization vector for MD5 encryption. (This option is required if you use the CyberSafe Kerberos implementation.) When cleared, zeros are used.
- **Add**: Click to add a new encryption type to the list.
- **Remove**: Click to remove the selected encryption type from the list.
- **Up / Down**: Move the selected item in the list.

**Related Topics**

- “Encryption Types” on page 485
Credential Properties Dialog Box

Index Term
Primary: Credential Properties dialog box

Getting there

1. From the Principal profile tab, under Service, right-click any current ticket.
2. Choose Properties.

This dialog box provides read-only information about the status of any ticket in the credentials cache.

Principals

<table>
<thead>
<tr>
<th>Owner</th>
<th>Displays the principal name for whom the credential was issued.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service</td>
<td>Displays the service for which the ticket is valid. krbtgt identifies a TGT (ticket-granting ticket) that provides service tickets. host, ftp, and other services identify tickets for a specific service on a specific host.</td>
</tr>
</tbody>
</table>

Times

| Time of authentication | Displays the time that the initial TGT was acquired. (This is the same as Start time for non-renewable tickets.) |
| Start time | Displays the starting date and time from which the ticket's lifetime is measured (after ticket renewal, if applicable). |
| End time | Displays the date and time when the current ticket will no longer be valid, and a new ticket will need to be acquired. |
| Renew time | Displays the date and time when the current ticket is no longer valid and a new ticket must be acquired. (This value appears for renewable tickets only.) |

Addresses

Specifies the IP address of the system for which the ticket was issued.

Ticket encryption type

Identifies the ticket encryption type used.

Ticket Flags

| Initial | If selected, indicates that the ticket is the initial TGT. |
| Renewable | If selected, indicates that the ticket is renewable. |
| Forwardable | If selected, indicates that the ticket can be forwarded to other systems in the same realm, and used to acquire additional service tickets. |
| Proxiable | If selected, indicates that the ticket can be used by an authenticated service provider to acquire further service tickets on your behalf. (This functionality is not currently implemented.) |
| Pre-Auth | If selected, indicates that pre-authentication was performed to acquire this ticket. |
| Hardware-Auth | If selected, indicates that hardware pre-authentication was performed to acquire this ticket |
Get Service Ticket Dialog Box

Getting there

- From the Credentials menu, choose Get Service Ticket.

**NOTE:** The Get Service Ticket menu option is available only if you have a TGT (ticket-granting ticket).

From this dialog box, you can troubleshoot connectivity problems. (You wouldn't normally use this dialog box to request a service ticket because the Reflection Kerberos client automatically obtains a service ticket for you anytime you request a kerberized service with a valid TGT.)

The options are:

- **Realm**
  Specify the realm for which you want a service ticket.

- **Host name**
  Specify the name (not the IP address) of the host for which you want a service ticket. The host must belong to the realm you entered in the preceding box.

- **Service name**
  Specify the type of service (on the host in the preceding box) for which you want a service ticket. For example, if you request a service ticket for a Telnet connection, the Service name is "host." For an FTP connection, the Service name may be "host" or "ftp."

Configuring Encryption

Kerberos connections can be configured to authenticate the server and encrypt the data stream. The Reflection Kerberos client supports the Data Encryption Standards DES (56-bit) and Triple DES (168-bit).

In this Section

- "Encryption Types" on page 485
- "Checksum Types" on page 485
- “Specify the Encryption for a Realm” on page 486
- “Specify the Checksum” on page 486
- “Add Encryption Type Dialog Box” on page 487
- “Encryption Tab (Realm Properties Dialog Box)” on page 487
Encryption Types

In Kerberos Manager, you specify the encryption types you want the KDC and the application server to use when issuing tickets. The server decides which encryption type is actually used, but tries to find the most compatible match between the encryption types the client requests and those available on the server. See your server documentation for supported encryption types.

The encryption type name describes the three parts of the encryption type: the actual encryption; the encryption mode (or method); and the integrity check algorithm. For example, DES-CBC-CRC uses Data Encryption Standard (DES) for encryption, Cipher Block Chaining (CBC) for the encryption mode, and Cyclic Redundancy Code (CRC) for error detection. Kerberos servers may refer to encryption types by their hexadecimal equivalent.

The Reflection Kerberos client supports the following encryption types:

<table>
<thead>
<tr>
<th>Encryption Type</th>
<th>Hexadecimal Equivalent</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>DES-CBC-CRC</td>
<td>1</td>
<td>Kerberos Manager uses DES-CBC-CRC as the default, followed by DES-CBC-MD5. Both types work in most environments.</td>
</tr>
<tr>
<td>DES-CBC-MD4</td>
<td>2</td>
<td>MD4 (a message digest algorithm) is used for error detection.</td>
</tr>
<tr>
<td>DES-CBC-MD5</td>
<td>3</td>
<td>MD5 authentication is supported automatically by some KDCs. If your KDC doesn't support MD5 authentication, you may receive error messages when you try to connect after configuring DES-CBC-MD5 as the preferred encryption.</td>
</tr>
<tr>
<td>RAW-DES-CBC</td>
<td>4</td>
<td>This encryption type does not perform an integrity check.</td>
</tr>
<tr>
<td>DES3-HMAC-SHA1</td>
<td>10</td>
<td>DES3-HMAC-SHA1 is equivalent to DES3_CBC_SHA1.</td>
</tr>
</tbody>
</table>

Checksum Types

By default, the Reflection Kerberos client uses RSA_MD5 as the checksum algorithm for communicating with the KDC and the application server. Most servers support this type of checksum. If your server doesn't support the specified checksum, it will issue an error message.

Kerberos servers may refer to checksums by their hexadecimal equivalent.
The Reflection Kerberos client supports the following checksum types:

<table>
<thead>
<tr>
<th>Checksum Type</th>
<th>Hexadecimal Equivalent</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRC32</td>
<td>01</td>
<td></td>
</tr>
<tr>
<td>RSA_MD4</td>
<td>02</td>
<td>HP DCE security and application servers use the RSA_MD4 checksum type.</td>
</tr>
<tr>
<td>RSA_MD4_DES</td>
<td>03</td>
<td></td>
</tr>
<tr>
<td>DES_CBC</td>
<td>04</td>
<td></td>
</tr>
<tr>
<td>RSA_MD5</td>
<td>07</td>
<td></td>
</tr>
<tr>
<td>RSA_MD5_DES</td>
<td>08</td>
<td></td>
</tr>
<tr>
<td>SHA1</td>
<td>09</td>
<td></td>
</tr>
<tr>
<td>HMAC_SHA1_DES3</td>
<td>0c</td>
<td></td>
</tr>
</tbody>
</table>

### Specify the Encryption for a Realm

1. **Start Kerberos Manager.**
2. From the **Configuration** menu, choose **Configure Realms**.
3. From the **Configuration** tab, select a realm from the **Realm list**, and then click **Properties**.
4. From the **Encryption** tab, click the **Configure Encryption Types** button.
5. Move the encryption type you want to the top of the list (select it, and click the **Up** button), and then click **OK**.
   - If the encryption type you want isn't available, click the **Add** button and select it.

**NOTE:** If your KDC uses the CyberSafe implementation of Kerberos, use DES_CBC_MD5 as the encryption type, and select **Use password as MD5-IV**.

6. Click **OK**.

### Related Topics

- “Encryption Types” on page 485

### Specify the Checksum

**Index Term**
- Primary: checksum
- Secondary: configuring

You can configure the checksum type for communication between both Kerberos and a KDC, and Kerberos and an application server.

### To configure a checksum

1. **Start Kerberos Manager.**
2. From the **Configuration** menu, choose **Configure Realms**.
3. From the **Configuration** tab, select a realm from the **Realm list**, and then click **Properties**.
4. Click the **Encryption** tab.
Perform one of the following tasks, and then click **OK**.

- For a KDC, select a checksum type from the list in the KDC request sum type box.
- For an application server, select a checksum type from the list in the Application request sum type box.

**Related Topics**

- "Checksum Types" on page 485
- "Encryption Tab (Realm Properties Dialog Box)" on page 487

### Add Encryption Type Dialog Box

**Index Term**

Primary: Add Encryption Type dialog box

**Getting there**

1. From the **Configuration** menu, choose **Configure Realms**.
2. From the **Configuration** tab, select a realm from the **Realm list**, and then click **Properties**.
3. Click the **Encryption** tab.
4. Click the **Configure Encryption Types** button.
5. Click the **Add** button.

**NOTE:** If the **Configure Realms** command is unavailable (dimmed), your system administrator has disabled this capability. Contact your system administrator for information about how to add or change the realms you may use.

From this dialog box, you can specify encryption types for the KDC and the application server (host). The KDC chooses the most compatible encryption type from those the client uses and those available on the server. See the server documentation for a list of supported encryption types.

**Encryption type**

Displays a list of ticket encryption types. From the drop-down list, choose the type to add to the list of preferred encryption types.

**Related Topics**

- "Encryption Types" on page 485

### Encryption Tab (Realm Properties Dialog Box)

**Index Term**

Primary: Encryption tab (Kerberos Manager)

**Getting there**

1. From the **Configuration** menu, choose **Configure Realms**.
2. From the **Configuration** tab, select a realm from the **Realm list**, and then click **Properties**.
3. Click the **Encryption** tab.
NOTE: If the Configure Realms command is unavailable (dimmed), your system administrator has disabled this capability. Contact your system administrator for information about how to add or change the realms you may use.

From this tab, you can specify the preferred checksum for communication between the Kerberos client and the KDC, and between the Kerberos client and an application server (host).

The options are:

**KDC request sum type**  
Specifies the checksum algorithm that the Key Distribution Center (KDC) uses when receiving information from Kerberos Manager.

**Application request sum type**  
 Specifies the checksum algorithm the application server uses when receiving information from Kerberos Manager.

**Configure Encryption types**  
Opens the Ticket Encryption Types dialog box, from which you can define the ticket encryption types that the KDC and the application server use when they issue tickets.

**Related Topics**

- “Encryption Types” on page 485

**Principal Profiles**

Your principal name identifies you within the network. It’s stored in a database on one or more KDCs (Key Distribution Centers) with all of the other principals in the realm. When you authenticate and get ticket-granting tickets, your associated credentials are stored in your profile, in the location and format that you specify.

**In this Section**

- “Configuring Principal Profiles” on page 489
- “Managing Multiple Principal Profiles” on page 491
- “Storing Principal Profiles and Credentials” on page 491
- “Add Principal Dialog Box” on page 493
- “Enter Principal Dialog Box” on page 493
- “Create New Principal Profile Dialog Box” on page 494
- “Create New Profile Browse Dialog Box” on page 494
- “Import Profile Dialog Box” on page 495
- “Import Profile Browse Dialog Box” on page 495
- “Modify Principal Profile Dialog Box” on page 495
- “Change Password Dialog Box” on page 496
- “Hidden Profiles Tab” on page 497
- “User Preferences Tab (Preferences Dialog Box)” on page 497
Configuring Principal Profiles

Using Kerberos Manager, you can create a new principal profile or select a different profile to use as the default. Or, you can modify an existing principal profile, and select it. You can also import credentials (from earlier versions of Reflection security products, and from MIT or Cybersafe Trustbroker file caches).

In this Section

- "Create a Principal Profile" on page 489
- "Import a Principal Profile" on page 489
- "Change the Default Principal Profile" on page 490
- "Add or Remove Principal Names from a Profile" on page 490

Create a Principal Profile

Index Term
Primary: principal profile
Secondary: creating

1 Start Kerberos Manager.
2 From the Credentials menu, choose New Principal Profile.
3 Type the Principal name or select it from the drop-down list.
4 Select the Realm name from the list.
5 Click OK.
The Create New Principal Profile dialog box opens.
6 If you want to change the principal profile storage name, type the new name or path in the Storage name box.
7 Select the storage media you want to use for this principal profile, and then click Create.
   If you select Hidden, in the Storage Name box, type the name you want to use to access the hidden principal profile, click Create, retype it for verification, and then click OK.

   NOTE: You cannot change the storage medium after you create the principal profile.
   Unless you chose to hide the principal profile, Kerberos Manager creates a new tab for this principal profile.

Import a Principal Profile

You can import credentials from earlier versions of Reflection security products, and from MIT or Cybersafe Trustbroker file caches.

To import a principal profile

1 Start Kerberos Manager.
2 From the Credentials menu, choose Import Principal Profile.
3 Type the filename or browse to add the principal profile you want to import, and then click OK.
   Kerberos Manager creates a new tab for this principal profile.

Related Topics

- "Import Profile Dialog Box" on page 495
**Change the Default Principal Profile**

Index Term  
Primary: principal profile  
Secondary: changing the default

You can modify a principal profile or select a different profile to use as the default. You can also remove a principal profile, provided it's not the default principal profile.

*Kerberos Manager* uses the default profile whenever a kerberized client application requests a service that requires Kerberos authentication.

**To change the principal profile**

1. Start *Kerberos Manager*.
2. Select a principal profile by clicking the corresponding tab. If the principal profile you want is hidden, open it first.
3. Perform one of the following tasks:

<table>
<thead>
<tr>
<th>To</th>
<th>Do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modify the principle profile</td>
<td>Click <strong>Modify</strong>, make the changes you want, and then click <strong>OK</strong>.</td>
</tr>
<tr>
<td>Remove the principle profile</td>
<td>Choose <strong>Credentials &gt; Remove Principle Profile</strong>, and then click <strong>Yes</strong> to confirm.</td>
</tr>
<tr>
<td>Select the principle profile as the default</td>
<td>Click the <strong>Set As Default Profile</strong> button. A blue check mark appears on the tab, indicating that this principal profile is now the default.</td>
</tr>
</tbody>
</table>

**Add or Remove Principal Names from a Profile**

Index Term  
Primary: removing  
Secondary: principal names from a profile

Index Term  
Primary: principal profile  
Secondary: add/remove principal names

Index Term  
Primary: adding  
Secondary: principal names to a profile

You can add names to a profile that you use to access different servers, or remove names from the principal list that you no longer use. This list pertains to the current user only, not to the workstation as a whole.

**To add or remove a principal name**

1. Start *Kerberos Manager*.
2. From the **Configuration** menu, choose **Preferences**.
Perform one of the following tasks, and then click OK.

Click Add, and then type the principal name you want to add.

-or-

Select a principal name from the Principal list, and then click Remove.

Managing Multiple Principal Profiles

In most security environments, a single principal profile will meet your needs for accessing services that require Kerberos authentication. In some situations, however, you may need to access different kerberized services, or services in different realms that aren't configured to "trust" and validate each others' ticket-granting tickets (TGTs).

If you maintain only one principal profile, you must request a new ticket each time you access a different service or realm. As an alternative, you can set up multiple principal profiles — each one acquiring its own TGT — and switch between profiles to access different services.

Storing Principal Profiles and Credentials

Kerberos Manager provides several options for storing your principal profile and credentials information: in a file, in memory, or hidden (in memory). You can choose a storage medium when you create a principal profile, or you can select a default setting that Kerberos Manager selects automatically each time you create a principal profile.

Storing Your Credentials in a File

Credentials files are stored in your default credential folder, and remain on the PC until you delete them. The default filename is principal@realm.cch.

An advantage of storing credentials in a file is that Kerberos Manager saves your principal profile settings (principal, realm, ticket lifetime) from session to session. The disadvantage is that anyone who finds the file on your PC can use your credentials until the ticket lifetime expires. If a person can guess your password, he or she can continue to use your credentials for access to kerberized services. Because Kerberos Manager creates a tab in its main window for each credentials file, these tabs are visible to anyone who opens Kerberos Manager on your PC while you’re logged in.

NOTE: You can restrict access to credentials stored on your PC by implementing the NTFS file system.

For greater security, select the Memory or Hidden storage options.
Storing Your Credentials in Memory

If you store your credentials in memory, the Reflection Kerberos client automatically deletes them when you quit Kerberos Manager and all other kerberized applications. The tab representing the principal profile on the Kerberos Manager main window also disappears.

If the principal profile you choose as your default is stored in memory, the Reflection Kerberos client saves the profile information, but not your password, in your Windows registry.

For added security, you can hide credentials stored in memory by selecting the Hidden option.

Hiding Your Credentials from the Desktop

Hidden credentials are always stored in memory, do not display a tab on the Kerberos Manager main window, and are deleted when Kerberos Manager and all kerberized applications are closed.

Because you must know the name of the credentials storage, it is unlikely that someone else will find this information on your PC.

NOTE: To restrict access to credentials on your PC, you must implement the NTFS file system.

Related Topics

- “Specify the Default Storage Medium” on page 492
- “Specify the Default Credential Folder” on page 493
- “Create a Principal Profile” on page 489

Specify the Default Storage Medium

Index Term
Primary: defaults (Kerberos Manager)
Secondary: specifying the default storage medium

Specify the storage medium and location you prefer for each new principal profile that you create. You can override this setting when you create a new profile.

To configure the default storage medium

1 Start Kerberos Manager.
2 From the Configuration menu, choose Configure Realms.
3 Click the User Defaults tab.
4 Under Default storage media, select File to store your credentials in a file on your PC.
   -or-
   Select Memory to keep credentials in memory until you quit all kerberized applications. (Memory is the most secure storage medium.)

NOTE: To choose a hidden location in memory for credentials, when you create the profile, select Hidden from the Create New Principal Profile dialog box.

Related Topics

- “User Defaults Tab (Configuration Dialog Box)” on page 477
Specify the Default Credential Folder

Index Term
Primary: defaults (Kerberos Manager)
Secondary: specifying the default credential folder

The credential folder setting pertains to the current user only, not to the workstation as a whole.

To set the credential folder

1. Start Kerberos Manager.
2. From the Configuration menu, choose Preferences.
3. Perform one of the following tasks, and then click OK.
   - Type the path in the Credential folder box or browse for the folder you want.
   - or-
   - Select Use default credential folder to use your personal documents folder to store credentials.

Add Principal Dialog Box

Index Term
Primary: Add Principal dialog box

Getting there

1. From the Configuration menu, choose Preferences.
2. Click the Add button.

From this dialog box, you can add a principal name to the current user's Principals list.

Principal

Specify the principal name you want to add to the principal list.

After a principal name has been added, it is available for selection from the principal list when you create or modify a profile.

Enter Principal Dialog Box

Index Term
Primary: Enter Principal dialog box

Getting there

- From the Credentials menu, choose New Principal Profile.

From this dialog box, specify the principal and realm, which is the first step in creating a new principal profile.
The options are:

**Principal** Type or select from the list the name you want to associate with this principal profile. The principal name is unique within the realm and can be any user or client that the realm's KDC recognizes. If you include the "at" character (@) in the name, you must precede it with a backslash (\).

**Realm** Select a realm (from the list of realms that have been configured for your computer) that you want to associate with this principal profile. A realm is the name given to a collection of Kerberos principals on a network and is case sensitive (usually uppercase). It is often similar to or the same as the domain name, for example, XYZ.MFG.COM.

Create New Principal Profile Dialog Box

**Index Term**  
Primary: Create New Principal Profile dialog box

**Getting there**

1. From the **Credentials** menu, choose **New Principal Profile**.
2. In the **Enter Principal** dialog box, type a **Principal** and **Realm**, and click **OK**.

From this dialog box, you can define the characteristics of a new principal profile.

The options are:

**Principal full name**  
Displays the full name of the stored principal and realm.

**Credentials storage**

<table>
<thead>
<tr>
<th>Storage name</th>
<th>Specify the storage area for the principal profile and credentials.</th>
</tr>
</thead>
</table>

**Storage media**

**File** Select to save the principal and its associated credentials to a file on your hard disk. The disadvantage to this option is that anyone who has access to this file can use your credentials until the ticket lifetime expires. If a person can guess your password, he or she can continue to use your credentials for access to kerberized services.

**Memory** Select to save the principal and its associated credentials in memory. When you quit all of your kerberized applications, the credentials are deleted. During a session, the principal appears on a tab. If the principal is the default, the profile is saved in the Windows registry.

**Hidden** Select to save the principal and its associated credentials in memory. You access hidden principal profiles from a single tab in the main window by entering the name of the hidden profile.

Create New Profile Browse Dialog Box

**Index Term**  
Primary: Create New Profile Browse dialog box
Getting there

1. From the **Credentials** menu, choose **New Principal Profile**.
2. In the **Enter Principal** dialog box, click **OK**.
3. In the **Create New Principal Profile** dialog box, click **Browse**.

From this dialog box, you can select the location and name for the new principal profile that you create.

The options are:

- **File name**
  - The default filename is `principal@realm.cch`. You can accept the default or type a new name. **Kerberos Manager** appends the extension `.cch` to the filename.

- **Save as type**
  - To show only `.cch` files, select Credentials Storage; to show all files, select All Files.

**Import Profile Dialog Box**

Index Term

Primary: Import Profile dialog box

Getting there

- From the **Credentials** menu, choose **Import Principal Profile**.

From this dialog box, you can import a principal profile to **Kerberos Manager** if you have principal profiles (or credentials caches) on your desktop that you created using earlier versions of Reflection, or if you have file caches that use MIT version 2 or 3 format.

- **File name**
  - Specify the filename of the principal profile you want to import or browse to select it.

**Related Topics**

- "**Import a Principal Profile**" on page 489

**Import Profile Browse Dialog Box**

Getting there

1. From the **Credentials** menu, choose **Import Principal Profile**.
2. From the **Import Profile** dialog box, click **Browse**.

From this dialog box, you can select a credential file that you want to import. When you import it, **Kerberos Manager** adds a new tab in the main window for the imported credentials.

The options are:

- **File name**
  - The default extension `.cch`. Select the file you want from the list, or type the name in the box.

- **Files of type**
  - To show only `.cch` files, select Credentials Storage; to show all files, select All Files.

**Modify Principal Profile Dialog Box**

Index Term

Primary: Modify Principal Profile dialog box

The default extension `.cch`. Select the file you want from the list, or type the name in the box.
Getting there

1. In **Reflection Kerberos Manager**, click the tab of the principal profile you want to modify.
2. Click **Modify**.

Use this dialog box to modify a principal profile that you've already created. (If you modify the name or location of the principal profile, **Kerberos Manager** deletes the original.)

The options are:

**Principal full name**

- **Principal**
  - Specify the principal name you want to associate with this principal profile. This may be any user or client that the realm’s KDC recognizes. Each principal has a unique name within a realm.

- **Realm**
  - Specify the realm you want to associate with this principal profile from the list of realms that have been configured on your PC. A realm is a name given to a collection of Kerberos principals on a network.

  The realm name is case sensitive — usually uppercase. It is often similar to or the same as the domain name, for example, **XYZ.MFG.COM**.

**Credentials storage**

- **Storage name**
  - Specifies the filename and folder where **Kerberos Manager** stores this principal profile.

**Storage media**

- **File**
  - Select to save the principal and its associated credentials to a file on your hard disk. The disadvantage to this option is that anyone who has access to this file can use your credentials until the ticket lifetime expires. If a person can guess your password, he or she can continue to use your credentials for access to kerberized services.

- **Memory**
  - Select to save the principal and its associated credentials in memory. When you quit all of your kerberized applications, the credentials are deleted. During a session, the principal appears on a tab. If the principal is the default, the profile is saved in the Windows registry.

- **Hidden**
  - Select to save the principal and its associated credentials in memory. You access hidden principal profiles from a single tab in the main window by entering the name of the hidden profile.

**Change Password Dialog Box**

*Index Term*

Primary: **Change Password dialog box (Kerberos Manager)**

Getting there

- From the **Tools** menu, choose **Change Password**.

From this dialog box, you can change the password for the designated principal.
NOTE: Before you can change passwords, you must first define an administrative Key Distribution Center (KDC).

The options are:

<table>
<thead>
<tr>
<th>Principal</th>
<th>Displays the selected principal. To change the password for a different principal, select it before you open this dialog box.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Old password</td>
<td>Type the password you want to change.</td>
</tr>
<tr>
<td>New password</td>
<td>Type the new password you want to use.</td>
</tr>
<tr>
<td>Verify new password</td>
<td>Retype the new password, to verify that you entered it correctly.</td>
</tr>
</tbody>
</table>

Related Topics

- “Specify the Administrative KDC for a Realm” on page 470

Hidden Profiles Tab

Index Term
Primary: Hidden Profiles tab

Getting there

1. Start Kerberos Manager.
2. Click the Hidden Profiles tab.

From this tab, you can open a hidden principal profile. You must know the storage name of the hidden principal profile to open it.

| Storage name | Type the name under which Kerberos Manager stores this principal profile and its associated credentials. |

User Preferences Tab (Preferences Dialog Box)

Index Term
Primary: User Preferences tab (Kerberos Manager)

Index Term
Primary: Preferences dialog box (prod_auth_short)

Getting there

- From the Configuration menu, choose Preferences.

From this tab, you can add principal names and specify a credential folder for the current user.
The options are:

**Principal list**
A list of principal names for the current user, from which he or she can choose when creating or modifying principal profiles.

**Credential folder**
Specifies the local folder where Kerberos Manager stores principal profiles and their associated credentials. Applies to credentials stored in a file format only. This box is unavailable if the **Use default credential folder** check box is selected.

**Use default credential folder**
Select to use the Windows personal documents folder (as shown by the path in the **Credential folder** box) to store credentials.

## Exporting Kerberos Settings

**Index Term**
Primary: exporting Kerberos settings

You can configure Kerberos on other computers by exporting your configuration settings to a file.

**In this Section**

- “Export Kerberos Settings” on page 498
- “Configure Kerberos from a Settings File” on page 498
- “Deploy Kerberos Settings with a Companion Installer” on page 499
- “Export Kerberos Configuration File Dialog Box” on page 500
- “Export Kerberos Settings Dialog Box” on page 500

### Export Kerberos Settings

After you configure a session using Kerberos, you can export these settings to an XML file in order to deploy them. The first time a user opens a Reflection Kerberos session, these settings are imported into the registry.

**To export Kerberos settings**

1. From the Start menu, under **Programs > Attachmate Reflection > Utilities**, choose **Kerberos Manager**.
2. From the Reflection Kerberos Manager, choose **Tools > Export Settings > As Configuration File**.
3. In the Export Kerberos Configuration File dialog box, click **OK**.
4. To deploy the session, add the Rsrb5.xml file to a companion installer file and deploy the file as shown in [A2D unwrapped a broken link to: admin_install_custom_companion in an excluded topic].Creating a Companion Install Package.

### Configure Kerberos from a Settings File

**Index Term**
Primary: importing Kerberos settings

**Index Term**
Primary: configuration files, (Kerberos Manager)
Secondary: importing settings from
You can configure the Reflection Kerberos client from a configuration file or a registry file. If the system administrator added a configuration file to your PC at installation, the Reflection Kerberos client is automatically configured the first time you start Kerberos Manager or InfoConnect. The configuration file is protected by a checksum that prevents manual changes to the file.

To import the Kerberos settings from a configuration file

1. On the PC being used to import the file, place a copy of Rsckrb5.xml in a InfoConnect folder located in either the common application data folder or the user-specific application data folder.
2. Start Kerberos Manager.
3. From the Tools menu, choose Import Settings.

To import Kerberos settings from a registry file

1. Make sure Regedit.exe is installed on your system. This executable is installed by default with the Windows operating system.
2. Place a copy of the registry entry (*.reg) file on the user's PC.
3. Double-click the registry entry (*.reg) file to import the settings to the Windows registry.

Related Topics

- “Deploy Kerberos Settings with a Companion Installer” on page 499

Deploy Kerberos Settings with a Companion Installer

Index Term
Primary: deploying Kerberos settings, custom installations

Index Term
Primary: administrative installation
Secondary: deploying Kerberos settings, custom installations

System administrators can configure the Reflection Kerberos client on other computers by including Kerberos configuration settings in a custom installation.

To deploy Kerberos settings

1. Install Reflection (including Kerberos Manager).
2. Start Kerberos Manager and configure the settings you want to export.
3. Choose Tools > Export Settings > As Configuration File.
4. (Optional) Clear Allow Configuration to disable the Configure Realms and Export Settings commands on the end-users' PCs.
5. Save the file to a location you can easily find, such as the desktop, and then click OK.
6. Create an administrative installation of InfoConnect (or use an existing one).
7. From your administrative installation point, open the Attachmate Customization Tool from a A2D unwrapped a broken link to: act_setup_shortcut in an excluded topic shortcut or by typing the following command line:
   `<path_to_setup>\setup.exe /admin`
8. From the Select Customization dialog box, select Create a new Companion installer (or open an existing MSI), and then click OK.
9. From the navigation pane, select Specify install locations.
10. Under Installation type, specify either Installs to all users of a machine or Installs only for the user who installs it.
11 From the navigation pane, select Add files.
12 Browse to select the Kerberos configuration file.
13 Under Add files to, specify one of the following locations:

<table>
<thead>
<tr>
<th>To install Kerberos settings</th>
<th>Specify this location</th>
</tr>
</thead>
<tbody>
<tr>
<td>For all users of the computer</td>
<td>[CommonAppDataFolder]\Attachmate\Reflection</td>
</tr>
<tr>
<td>Only for the user who installs this package</td>
<td>[AppDataFolder]\Attachmate\Reflection</td>
</tr>
</tbody>
</table>

14 Click File > Save As and enter a name for your installer file (for example, KerberosSettings.msi)
15 Install this package with Reflection.

When the configuration file is installed correctly, the Reflection Kerberos client is configured automatically the first time the user uses Kerberos.

Export Kerberos Configuration File Dialog Box

Getting there

- From the Tools menu, choose Export Settings > As Configuration File.

**NOTE:** If the Export Settings command is unavailable (dimmed), your system administrator has disabled this capability. Contact your system administrator for information about how to add or change the realms you may use.

From this dialog box, you can save your current realm settings to a configuration file.

The options are:

- **Kerberos Configuration File**
  Displays the location to which you're saving the configuration file.

- **Allow configuration**
  Clear this check box to create a configuration file that disables the Configure Realms and Export Settings commands in Kerberos Manager, preventing users from configuring these settings.

Export Kerberos Settings Dialog Box

**Index Term**
Primary: Export Kerberos Settings dialog box

Getting there

- From the Tools menu, choose Export Settings > As Registry File.

**NOTE:** If the Export Settings command is unavailable (dimmed), your system administrator has disabled this capability. Contact your system administrator for information about how to add or change the realms you may use.
From this dialog box, you can save your current realm settings to a registry entries (*.reg) file.

**Allow configuration**

Clear this check box to create a realm settings file that disables the **Configure Realms** and **Export Settings** commands in *Kerberos Manager*, preventing users from configuring these settings.

**Troubleshooting Kerberos**

This section includes information about how to resolve problems that may arise when using the Reflection Kerberos client.

**Diagnosing Problems**

*Index Term*

Primary: diagnosing
Secondary: problems

This section includes information on how to identify and resolve problems that you may encounter using *Kerberos Manager*.

**Problems Getting Ticket-Granting Tickets**

*Index Term*

Primary: troubleshooting (*Kerberos Manager*)
Secondary: problems getting ticket-granting tickets

If you have problems obtaining Kerberos ticket-granting tickets (TGT), inspect the KDC (Key Distribution Center), and verify that:

- The KDC is running and configured correctly.
- The clocks on your PC and the KDC are synchronized.
- The clocks on the KDC and the application servers are synchronized.

**Problems Caused by Multiple Installations**

*Index Term*

Primary: troubleshooting (*Kerberos Manager*)
Secondary: problems caused by multiple installations

If you experience unexpected behavior from *Kerberos Manager* (for example, you are prompted for a password even though you already have a ticket-granting ticket), you may have multiple installations of *Kerberos Manager*.

- Verify that you have only one copy of *Kerberos Manager* on your PC.

You can do this by searching for multiple copies of the Rskrb5.dll file. If you find multiple copies of this file, uninstall all but one copy of *Kerberos Manager*.

**Resolving Telnet Connections**

*Index Term*

Primary: Windows KDC
Secondary: resolving Telnet connections
Index Term
Primary: ticket-granting server, testing

If you cannot make a connection (for example, Telnet), but you can acquire a TGT (ticket-granting ticket), the cause may be your Telnet daemon (application server) or the ticket-granting server.

- Make sure you have a valid TGT, and then obtain a service ticket (Credentials > Get Service Ticket).

If you succeed in obtaining a service ticket, the application server is likely the cause.

Related Topics
- “Get Service Ticket Dialog Box” on page 484

Logon Problems Using a .k5login File

Index Term
Primary: troubleshooting (Kerberos Manager)
Secondary: problems using a .k5login file

Index Term
Primary: authenticating
Secondary: using a .k5login file

If a user with valid credentials is prompted for a password while requesting access to a kerberized application, the .k5login file may be the cause. A .k5login file determines which principals can access the user’s account. This file is required in Cybersafe environments, and in situations where the user logs on with a different name from the principal name (in such cases, the user’s home directory on the server must have a copy of the .k5login file). Try the following:

- Verify that the .k5login file is located in the home directory of the UNIX user.
- Verify that only the .k5login account owner has write access to the file.
- If you’re the .k5login account owner, edit the file to ensure access to the specified principals. For example, if your principal name doesn’t match your UNIX account name, add your full principal name using the principal@realm format. Similarly, if you use the same principal name for several different realms, you must add a separate principal@realm name for each realm.

Configure the IP Address Used in the TGT

Index Term
Primary: troubleshooting (Kerberos Manager)
Secondary: firewall and NAT connections

Index Term
Primary: troubleshooting (Kerberos Manager)
Secondary: configuring the IP address used in the TGT

If your network environment uses a firewall or Network Address Translation (NAT), and you have a valid ticket-granting ticket (TGT) in the credentials cache, but receive an error when you request a service ticket from the KDC, troubleshoot your connections using the following procedure.

**NOTE:** Do not change your IP address if you can successfully connect using the default.

To configure the IP address used in the TGT

1. Start Kerberos Manager.
2 From the **Configuration** menu, choose **Configure Realms**.
3 From the **Configuration** tab, select a realm from the **Realm list**, and then click **Properties**.
4 Click the **Realm Defaults** tab.
5 For the **Ticket Address**, perform one of the following tasks, and then click **OK**.

<table>
<thead>
<tr>
<th>To</th>
<th>Do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify the firewall or NAT IP address</td>
<td>Type up to four IP addresses separated by commas.</td>
</tr>
<tr>
<td>Obtain the IP address used by a given host on your network</td>
<td>Type a host name that is recognized on your network. The ticket contains the IP address used by that host (and appears in the <strong>Credential Properties</strong> dialog box).</td>
</tr>
<tr>
<td>Obtain a ticket that contains no IP address</td>
<td>Delete the contents of the <strong>Ticket Address</strong> box.</td>
</tr>
<tr>
<td>Specify the current IP address of your computer</td>
<td>Click <strong>Reset</strong>. The IP address of your computer resets to the value specified in your <strong>Network Properties</strong> dialog box, or assigned by your DHCP server.</td>
</tr>
</tbody>
</table>

**Related Topics**

- "Incorrect Network Address" on page 507

**Set the Maximum UDP Packet Size**

**Index Term**

Primary: UDP communications with the KDC

**Index Term**

Primary: troubleshooting (Kerberos Manager)

Secondary: setting the maximum UDP packet size

**Index Term**

Primary: TCP communications with the KDC

**InfoConnect** supports both TCP and UDP protocols for communicating with the KDC. By default, **InfoConnect** attempts to communicate using UDP. However, if the packet size exceeds the value specified for the **Maximum UDP packet size**, **InfoConnect** switches to TCP (which may require more time to initiate a connection).

If you are having problems authenticating to a Windows KDC and you belong to a large number of groups, or if **Use Windows logon credentials** is selected, decreasing the value for **Maximum UDP packet size** may help. Alternatively, try increasing the the setting for the **Maximum UDP packet size**.

**To change the maximum UDP packet size**

1 Start **Kerberos Manager**.
2 From the **Configuration** menu, choose **Configure Realms**.
3 From the **Configuration** tab, select a realm from the **Realm list**, and then click **Properties**.
4 On the KDC tab, specify a value for **Maximum UDP packet size**. To use only TCP communications, set this value to 0.
Related Topics

- “KDC Unreachable” on page 508
- “Pre-authentication Failed” on page 509

Diagnosing Error Messages

Index Term
Primary: troubleshooting (Kerberos Manager)
Secondary: diagnosing error messages

Index Term
Primary: error messages
Secondary: Kerberos Manager

Index Term
Primary: diagnosing
Secondary: error messages

Following is a list of common error messages. See the relevant topic for more information about the probable cause and possible solutions.

In this Section

- “Checksum Type Not Supported” on page 505
- “Client Principal Not Found in Kerberos Database” on page 505
- “Client's Entry in Kerberos Database Has Expired” on page 505
- “Configuration File Import Failed” on page 505
- “Decrypt Integrity Check Failed” on page 506
- “Difference Between Expected and Actual KDC Reply Time Too Great” on page 506
- “Difference Between Expected and Actual Ticket Time is Too Great” on page 506
- “Encryption Type Not Supported” on page 506
- “End of Tag Expected” on page 507
- “Generic Error” on page 507
- “Incorrect Network Address” on page 507
- “Invalid or Incomplete Host Name” on page 508
- “KDC Unreachable” on page 508
- “Password has expired (KDC023)” on page 508
- “Pre-authentication Failed” on page 509
- “Pre-authentication Method Not Supported” on page 509
- “Reflection Kerberos Has Not Been Configured Properly” on page 509
- “Security Mechanism is Invalid or Unsupported” on page 509
- “Server Principal Not Found in Kerberos Database” on page 510
- “Server's Entry in Kerberos Database Has Expired” on page 510
- “The KDC Reply Was Modified” on page 510
- “Ticket Not Yet Valid” on page 510
- “Unknown Realm” on page 511
**Checksum Type Not Supported**

Index Term
Primary: Checksum type not supported (error message)

**Problem:** The KDC does not support the checksum type specified in the Reflection Kerberos client.

**Solution:** Consult your KDC documentation and change the checksum type to one that the KDC supports.

If you are trying to establish a telnet connection to a DCE application server, change both the **Application request sum type** and the **KDC request sum type** to RSA_MD4_DES.

**Related Topics**
- “Specify the Checksum” on page 486
- “Checksum Types” on page 485

**Client Principal Not Found in Kerberos Database**

Index Term
Primary: Client principal not found in Kerberos database (error message)

**Problem:** The KDC could not find the user principal in the principal database.

**Solution:** Verify that you entered the principal name correctly, and that it is valid for the current realm — you may need to modify the principal profile.

**Related Topics**
- “Change the Default Principal Profile” on page 490

**Client’s Entry in Kerberos Database Has Expired**

Index Term
Primary: Client’s entry in Kerberos database has expired (error message)

**Problem:** The principal has expired in the KDC database.

**Solution:** Contact your Kerberos system administrator to confirm the reason for the expiration and to re-enable the client entry in the KDC.

Until the KDC is updated (and propagated to any slave KDCs, if applicable), you will be unable to acquire a TGT ticket.

**Configuration File Import Failed**

Index Term
Primary: configuration files, (Kerberos Manager)
Secondary: import failed message

Index Term
Primary: Configuration file import failed (error message)
Problem: When you attempt to import a Kerberos Manager configuration file, an error may occur because:

- There is no configuration file (Rskrb5.xml) on your PC in the Reflection subfolder for the common application data folder or the user-specific data folder.
- The configuration file has been manually edited. (The Rsckrb5.xml file uses a checksum to ensure that no manual changes can be made to this file. If the file is changed in any way, it is no longer recognized as valid.)

Solution: Contact your Kerberos system administrator for a valid configuration file (Rskrb5.xml).

Related Topics

- "Configure Kerberos from a Settings File" on page 498

Decrypt Integrity Check Failed

Index Term
Primary: Decrypt integrity check failed

Problem: Your password entry failed.

Solutions

- Confirm that you entered the password correctly.
  
  Passwords are case-sensitive. Make sure that the Caps Lock key is off, and then re-enter your password.
- Double-check the principal name, and then verify that you are entering the correct password for that principal.

Difference Between Expected and Actual KDC Reply Time Too Great

Index Term
Primary: Difference between expected and actual KDC reply time too great (error message)

Problem: The PC and KDC host clocks are not synchronized.

Solution: Check the times on both and manually adjust the clock on the PC to match that on the KDC.

Difference Between Expected and Actual Ticket Time is Too Great

Index Term
Primary: Difference between expected and actual ticket time is too great (error message)

Problem: The KDC and kerberized server clocks are not synchronized.

Solution: Notify the system administrator to adjust the clock on the kerberized server to match that on the KDC.

Encryption Type Not Supported

Index Term
Primary: Encryption type not supported (error message)

Problem: The KDC does not support the encryption types specified in the Reflection Kerberos client.

Solution: Consult your KDC documentation and then change the encryption type to one that the KDC supports.
**End of Tag Expected**

Index Term  
Primary: End of tag expected (error message)

**Problem:** This message could indicate that you typed an incorrect password.

**Solutions:**

- Re-type your password.
- If your preferred encryption type is RAW-DES-CBC, the Reflection Kerberos client cannot detect an incorrect password, and doesn't return a descriptive error message. Try changing the encryption type to see whether the Reflection Kerberos client returns a descriptive message.

**Related Topics**

- "Encryption Types" on page 485
- "Specify the Encryption for a Realm" on page 486

**Generic Error**

Index Term  
Primary: Generic error (error message)

**Problem:** The KDC does not support the preferred encryption types specified in Kerberos Manager.

**Solution:** Change your list of preferred encryption types to those the KDC supports.

**Related Topics**

- "Specify the Encryption for a Realm" on page 486
- "Encryption Types" on page 485

**Incorrect Network Address**

Index Term  
Primary: Incorrect network address (error message)

**Possible causes for this error message:**

- **Problem:** The Hosts file may contain the incorrect address for the Kerberos host.
  
  **Solution:** Verify that the Hosts file (on the server and the PC) contains the correct address for the Kerberos host.

- **Problem:** The IP address for your PC may be incorrect.
  
  **Solution:** Verify that the IP address for your PC is correct.

- **Problem:** If you use dynamic IP addressing, or if you switch between a local network connection and a wireless connection, your ticket-granting ticket may contain an old IP address.
  
  **Solution:** Clear your tickets, acquire a new ticket-granting ticket, and try the connection again.

- **Problem:** If your network environment uses a firewall or Network Address Translation (NAT), and you have a valid ticket-granting ticket (TGT) in the credentials cache, but you receive an error when you request a service ticket from the KDC.
  
  **Solution:** Configure the IP address used in the TGT.

**Related Topics**

- "Configure the IP Address Used in the TGT" on page 502
**Invalid or Incomplete Host Name**

Index Term
Primary: Invalid or incomplete host name (error message)

The host name could not be resolved to a network address. Try entering the fully qualified host name (for example, telnserv.com instead of telnserv). Also check your DNS server settings or your Hosts file.

**Problem:** The host name could not be resolved to a network address.

**Solutions**
- Try entering the fully qualified host name (for example, telnserv.com instead of telnserv).
- Verify your DNS server settings or your Hosts file.

**KDC Unreachable**

Index Term
Primary: KDC unreachable (error message)

Possible causes for this error message:
- **Problem:** The KDC (Key Distribution Center) may not be running.
  - **Solution:** Confirm that the KDC is running.
- **Problem:** You may need to enter a fully qualified host name.
  - **Solution:** Check your realm configuration. If necessary, enter a fully qualified host name.
- **Problem:** The server’s host may be down.
  - **Solution:** Verify that the server’s host is running.
- **Problem:** If you run the Reflection Kerberos client using an SLIP or PPP connection, and use DNS only for host name resolution, you may be having a timeout problem.
  - **Solution:** Try connecting again at a later time, or check to see whether the network is having problems.
- **Problem:** You may need to run Kerberos 5 security server software.
  - **Solution:** Contact your Kerberos system administrator to verify that your system is running the appropriate security server software.
- **Problem:** The maximum UDP packet size setting may have been set to 0 for this KDC, which forces TCP protocol for all communications with the KDC. The KDC to which you are authenticating may require UDP protocol.
  - **Solution:** Set the maximum UDP packet size to a value greater than 0.

**Related Topics**
- “Contacting Technical Support” on page 511
- “Set the Maximum UDP Packet Size” on page 503

**Password has expired (KDC023)**

Index Term
Primary: Password has expired (error message)

**Problem:** Your Kerberos password has expired.

**Solution:** Use Kerberos Manager to change your password.
Related Topics

- “Change your Password” on page 473

Pre-authentication Failed

Index Term
Primary: Pre-authentication failed (error message)

Possible causes for this error message:

- **Problem:** You may have entered your password incorrectly.
  
  **Solution:** Confirm that you entered the password correctly. Passwords are case-sensitive. Make sure that the Caps Lock key is off, and then re-enter your password.

- **Problem:** KDC requires you to perform pre-authentication, but you have not configured it.
  
  **Solution:** Verify your host authentication settings.

- **Problem:** The KDC does not support the preferred encryption types specified in Kerberos Manager.
  
  **Solution:** Change your list of preferred encryption types to be compatible with those supported by the KDC.

- **Problem:** The KDC to which you are authenticating requires TCP protocol for packets over a certain size (this is seen on some Windows KDCs).
  
  **Solution:** Try changing the value for Maximum UDP packet size to less than 1500.

Related Topics

- “Disable Pre-authentication” on page 472
- “Set the Maximum UDP Packet Size” on page 503

Pre-authentication Method Not Supported

Index Term
Primary: Pre-authentication method not supported (error message)

**Problem:** The Reflection Kerberos client only supports the encrypted timestamp method of pre-authentication.

**Solution:** If your KDC expects a different method of pre-authentication, contact your Kerberos system administrator and request to have pre-authentication disabled for your principal.

Reflection Kerberos Has Not Been Configured Properly

Index Term
Primary: Reflection Kerberos has not been configured properly (error message)

**Problem:** There is an error in the Windows registry entries for the Kerberos principal, realm, or KDC host.

**Solution:** Try repairing or reinstalling InfoConnect.

Security Mechanism is Invalid or Unsupported

Index Term
Primary: Security mechanism is invalid or unsupported (error message)
Problem: This error message may have been caused because:
- The security mechanism requested is invalid or unsupported.
- The Reflection Kerberos client could not find the encryption .DLL files.

Solution: Try repairing or reinstalling InfoConnect.

Server Principal Not Found in Kerberos Database

Problem: The KDC could not find the host you requested in the principal database.

Solutions
- Verify that the host table (on the server and on the PC) contains the fully qualified name of the requested host.
- Verify that the requested host name is entered correctly in the realm configuration.
- Make sure that the requested host name is not an alias. You must use the actual host name (both in your request and in the realm configuration). Typically, you need to use the fully qualified host name (for example, telnserv.com instead of telnserv).
- Double-check that you are using the correct ticket-granting ticket. Your TGT must be valid for the same realm as the host you’re logging in to (unless your environment is set up for cross realm authentication).

Server’s Entry in Kerberos Database Has Expired

Problem: The server principal has expired in the database for the KDC.

Solution: Contact your Kerberos system administrator to confirm the reason for the expiration and to re-enable the server entry in the KDC.

Until the KDC is updated (and propagated to any slave KDCs, if applicable) you will be unable to acquire a service ticket.

The KDC Reply Was Modified

Problem: The PC and host clocks are not synchronized.

Solution: Check the times on both the PC and host clocks, and then manually adjust the clock on the PC to match that on the KDC.

Ticket Not Yet Valid

Possible causes for this error message:
- Problem: The KDC and application server clocks are out of sync.
Secure Connections

Solution: Consult your server documentation.

- Problem: Your ticket may not yet be valid. (Some servers are configured to allow issuance of tickets that will become valid at some future time.)

  Solution: Verify the time in the Start time field of the Credential Properties dialog box.

Related Topics

- “Credential Properties Dialog Box” on page 483

Unknown Realm

Index Term
Primary: Unknown realm (error message)

Possible causes for this error message:

- Problem: The host name is invalid or your security server cannot find it.

  Solution: Verify your realm configuration.

- Problem: A connection to the host could not be established.

  Solution: Make sure that the host is functioning properly.

- Problem: There is a problem with your principal profile.

  Solution: Confirm that your default principal profile is correct.

- Problem: Double-check the case you used when entering the realm name.

  Solution: Typically, it should be uppercase. If you are using a DCE security server, the cell name (DCE equivalent of realm) must be lowercase.

Contacting Technical Support

Attachmate is committed to high-quality technical support. We know that the success of your enterprise depends on keeping your information systems running smoothly — and your software is a key component.

For technical support information, visit the Attachmate Web site (http://support.attachmate.com/techdocs).

Security Properties Dialog Box

Getting there

The way you access the Security Properties dialog box depends on the session type you are in.

Terminal session

1. Open the Document Settings dialog box.

   The steps depend on your user interface mode (page 120).
Under Host Connection, click Setup Connection Security.

(3270 and 5250 terminal sessions only) Under Security, click Security Settings.

Printer session

1. Open a printer session.
2. On the Connection menu, click Session Setup.
3. Click Security.

FTP Client

1. In the Connect to FTP Site dialog box, select a site.
2. Click Security.

Which Protocols Can I Use?

Index Term
Primary: secure connections
Secondary: available protocols
The security protocols available to you depend on which connection type you are configuring.

<table>
<thead>
<tr>
<th>Connection Type</th>
<th>Supported Protocols</th>
</tr>
</thead>
<tbody>
<tr>
<td>3270 terminal and printer</td>
<td>SSL/TLS</td>
</tr>
<tr>
<td>or</td>
<td>SOCKS</td>
</tr>
<tr>
<td>5250 terminal and printer</td>
<td>Secure Shell</td>
</tr>
<tr>
<td>VT terminal</td>
<td>Kerberos</td>
</tr>
<tr>
<td></td>
<td>SSL/TLS</td>
</tr>
<tr>
<td></td>
<td>SOCKS</td>
</tr>
<tr>
<td></td>
<td>HTTP</td>
</tr>
</tbody>
</table>

**Related Topics**

- “Kerberos Overview” on page 462
- “Secure Shell Connections (FTP Client)” on page 756
- “SOCKS Overview” on page 455
- “SSL/TLS Overview” on page 337

**Firewall Tab (Security Properties Dialog Box)**

**Getting there (FTP Client)**

1. In the **Connect to FTP Site** dialog box, select a site.
2. Click **Security**.

The **Firewall** tab of the **Security Properties** dialog box is visible only if you are running the Reflection FTP Client.

**Use Firewall**

Enables connections through a firewall. You must select this check box before you can set other items.

**Style**

The FTP Client sends different commands for logging onto a firewall and connecting to an FTP server based on the **server style** (page 750) you specify.

**Server name**

Specify the name of the firewall that you use to log onto an FTP server.

**User name**

Specify a valid user name registered on the firewall server. For case-sensitive servers, you must use the appropriate case.

This setting is unavailable if **Style** is set to `username@servername` and the **Password authentication** check box is cleared.
Kerberos is a protocol that uses a trusted third party to enable secure communications over a TCP/IP network. The protocol uses encrypted tickets rather than plain-text passwords for secure network authentication and also supports encryption of the data stream.

### Kerberos Tab (Security Properties Dialog Box)

**Index Term**
- **Primary**: Security Properties dialog box
- **Secondary**: Kerberos tab

#### Getting there (Terminal session)

1. Open the Document Settings dialog box:
   - The steps depend on your user interface mode (page 120).]

   **User Interface Mode**
   - **Steps**
     - **Ribbon or Reflection Browser**: With a session open in Reflection, from the Quick Access Toolbar, click .
     - **TouchUx**: Tap the Gear icon and then select Document Settings.

2. Under **Host Connection**, click **Setup Connection Security**.
3. (3270 and 5250 terminal sessions only) Under **Security**, click **Security Settings**.

#### Getting there (FTP Client)

1. In the Connect to FTP Site dialog box, select a site.
2. Click **Security**.

Related Topics

- “Which Protocols Can I Use?” on page 512

---

**Password**

Enter your password for the firewall server. The specified string is saved as obfuscated text in the settings file and sent to the firewall as part of the login sequence when you open a connection.

**Save password**

If the check box is selected, the string entered in the Password box is saved as obfuscated text in your FTP settings file. Each character in the password will display as an asterisk (*) in user interface text boxes and in the FTP command window (page 815).

When this check box is cleared, the password is not saved, and you are prompted for a password each time an FTP server connection is opened using the firewall.

**Password authentication**

This setting is available when **Style** is set to username@servername. If your firewall is set up to authenticate the user prior to opening a connection to an FTP server, select this check box.

If you have selected a firewall style that requires authentication, this option is selected automatically and you cannot change it.
The options are:

**Reflection Kerberos**

Enables Kerberos authentication. You must select this check box before you can set other items.

**Principal**

Specifies the principal for which you want to obtain Kerberos credentials. A full principal name includes both the principal name and the realm name, in the format `<principal>@<realm name>`.

**Realm**

Specifies the realm portion of the full principal name. This list contains all the realms that have been configured on your computer.

**User ID**

By default Reflection logs into the host using your principal name for your User Name (or User ID). Change the value for User ID if you want to log into your host with a user name that is different from your principal name.

**Mutual Authentication**

Select this check box if, in addition to authenticating this principal to a service that requires Kerberos authentication, you want the service to authenticate itself to the principal in return.

**Encrypt Data Stream**

Select this check box to encrypt the data transmitted between the host and the Kerberos client. When this check box is clear, the authentication (login) process is encrypted, but not subsequent data transmission. Enabling data stream encryption will decrease transmission speed.

*CAUTION:* Caution for Reflection X sessions: When Encrypt data stream is selected, the initial authentication and commands sent via the Telnet connection are encrypted, but the X11 protocol data stream is not encrypted.

**Verify Data Integrity**

Select this check box to verify the integrity of data transmitted between the host and the Kerberos client.

This is only available from the Reflection FTP Client. You must select the Reflection Kerberos and Mutual authentication check boxes to enable this feature. Verify data integrity is not available for Telnet connections.

**Forward Ticket**

Enables forwarding of Ticket Granting Tickets (TGT). Ticket forwarding allows you to forward your TGT to another host and get service tickets for additional services without having to repeat the authentication process with the KDC. Tickets that have been forwarded may be forwarded again. You must have Mutual authentication enabled to enable ticket forwarding.

**Kerberos Manager**

Opens the Reflection Kerberos Manager. If the Kerberos Manager is not installed, this button opens the Reflection Kerberos Initial Configuration dialog box.

**Renewable ticket (Days, Hours, Minutes)**

Ticket granting tickets (TGT) are renewable for the time specified. Click Renew to renew your ticket for the specified interval. When no time interval is given, tickets are not renewable.

**Renew**

Renews your current ticket for the period of time specified in Days, Hours, and Minutes. Your ticket must still be valid when you use this button.

**Related Topics**

- “Which Protocols Can I Use?” on page 512
Secure Shell Tab (Security Properties Dialog Box)

Getting there (FTP Client)

1. In the Connect to FTP Site dialog box, select a site.
2. Click Security.

The Secure Shell tab of the Security Properties dialog box is visible only if you are running the FTP Client.

Secure Shell is a protocol for securely logging onto a remote computer and executing commands. It provides a secure alternative to Telnet, FTP, rlogin, or rsh. Secure Shell connections require both server and user authentication, and all communications pass between hosts over an encrypted communication channel. You can also use Secure Shell connections to forward X11 sessions or specified TCP/IP ports through the secure tunnel.

The options are:

- **Use Reflection Secure Shell**: Specifies that the connection be made using the Secure Shell protocol. You must select this check box before you can set other items.

- **SSH Config scheme**: Reflection saves Secure Shell settings to the specified SSH configuration scheme (page 403) and uses these settings whenever you specify this SSH configuration scheme name. If you leave this blank, Reflection uses the current host name for the SSH configuration scheme name.

- **Configure**: Opens the Reflection Secure Shell Settings dialog box. Use this dialog box to configure additional Secure Shell settings.

- **SFTP**: When this option is selected, the FTP Client will connect using SFTP (Secure FTP) protocol. SFTP supports fewer commands than the full FTP protocol.

- **Preserve timestamps and file attributes**: This setting affects SFTP connections. When this option is selected, files transferred to and from the server retain their date, time, and file attributes.

**NOTE**

- If you have configured default file attributes for transfers from FTP Client using Tools > Options > Attributes, these values are applied even if this option is selected.

- Server file dates are not preserved when files are dragged from the FTP Client to the Windows desktop or Windows explorer folder. Use the local pane of the FTP Client to preserve file dates.

- **Use structured listing data**: This setting is relevant for Secure Shell servers. Use it as a troubleshooting tool if information from your server is missing or is not correctly displayed in the FTP Client’s server pane. This setting specifies which data list style sent by the server is used to create the directory display in the right pane of the FTP Client. When this setting is not selected (the default), the FTP Client uses the standard UNIX-style data list. When it is selected, the FTP Client uses the structured data list.

- **Send Window Size**: Changing Buffer size and Number of buffers can improve transfer speed. The optimum values depend on your network and server setup. Changing these values may also affect how quickly you can cancel a transfer.
<table>
<thead>
<tr>
<th>Related Topics</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>“Which Protocols Can I Use?” on page 512</td>
<td>“Connect Using Secure Shell (FTP Client)” on page 756</td>
</tr>
<tr>
<td>“Connect using Secure Shell (SSH)” on page 349</td>
<td>“Configure Client Authentication using Certificates” on page 385</td>
</tr>
</tbody>
</table>

### Proxy Tab (Security Properties Dialog Box)

**Index Term**
- Primary: SOCKS
- Secondary: SOCKS tab (Security Properties dialog box)

**Getting there**

The way you access the Security Properties dialog box depends on the session type you are in.

#### Terminal session

1. Open the Document Settings dialog box.

   The steps depend on your user interface mode (page 120).

   **User Interface Mode**
   - Ribbon or Reflection Browser
   - TouchUx

   **Steps**
   - With a session open in Reflection, from the Quick Access Toolbar, click .
   - Tap the Gear icon and then select Document Settings.
1 Under **Host Connection**, click **Setup Connection Security**.
2 (3270 and 5250 terminal sessions only) Under **Security**, click **Security Settings**.

### Printer session

1 Open a printer session.
2 On the **Connection** menu, click **Session Setup**.
3 Click **Security**.

### FTP Client

1 In the **Connect to FTP Site** dialog box, select a site.
2 Click **Security**.

You can configure your application to connect through a SOCKS or HTTP server.

---

**NOTE:** If you want to set up an SSH (Secure Shell) connection through a SOCKS or HTTP proxy server, use the Proxy tab in the **Reflection Secure Shell Settings** (page 353) to enable and configure the server, not the Proxy tab in the Security Properties dialog.

---

**Use proxy server**
- Specifies to use a proxy server to make the connection. You must select this check box before you can set other items.

**SOCKS**
- Specifies to use a SOCKS proxy server.

**HTTP**
- Specifies to use an HTTP proxy server.

**Configure**
- Opens the Configuration dialog box, in which you can enter the server address and other settings.

### Related Topics

- “Which Protocols Can I Use?” on page 512
- “Socks Configuration Dialog Box” on page 455
- “SOCKS Overview” on page 455

### SSL/TLS Tab (Security Properties Dialog Box)

**Index Term**
- Primary: Security Properties dialog box
- Secondary: SSL/TLS tab

**Getting there (InfoConnect)**

1 Open the Document Settings dialog box.
   - The steps depend on your **user interface mode** (page 120).
Under Host Connection, click Setup Connection Security.

(3270 and 5250 terminal sessions only) Under Security, click Security Settings.

Getting there (FTP Client)

1. In the Connect to FTP Site dialog box, select a site.
2. Click Security.

The Secure Sockets Layer protocol (SSL) and its compatible successor, the Transport Layer Security protocol (TLS), enable a client and server to establish a secure, encrypted connection over a public network. When you connect using SSL/TLS, the client authenticates the server before making a connection, and all data passed between InfoConnect and the server is encrypted. Depending on the server configuration, the server may also authenticate the client.

The options are:

- **Use SSL/TLS Security**: Enables SSL/TLS connections. You must select this before you can set other values on the SSL/TLS tab. When Use SSL/TLS security is selected, Reflection will only connect to the host if a secure SSL/TLS connection can be established.

  Before making an SSL/TLS connection, Reflection must authenticate the host. Authentication is handled through the use of digital certificates. These certificates are part of the same Public Key Infrastructure (PKI) that is used to secure internet transactions. Your computer must be configured to recognize the digital certificate presented by your host and, if necessary, to provide a certificate for client authentication. If your computer is not properly configured, or if the certificates presented for authentication are not valid, you will not be able to make SSL/TLS connections. Depending on how a host certificate was issued, you may need to install a certificate on your local computer.

- **Configure PKI**: Opens the PKI Configuration (page 523) dialog box, which you can use to configure PKI settings for Reflection SSL/TLS sessions.

- **Encryption Strength**: Specify the desired level of encryption for SSL/TLS connections. The connection will fail if this level cannot be provided.

  If you select Default, any encryption level is permitted, and Reflection will negotiate with the host system to choose the strongest encryption level supported by both the host and the client. If you are running in FIPS mode and select Default, Reflection will negotiate using only FIPS compliant encryption levels.

- **SSL/TLS version**: Specifies which SSL or TLS version to use.
Use Reflection security proxy and related settings are visible if you use Reflection Security Gateway (available separately from Attachmate) to manage sessions and you launched this session from the Administrative WebStation. With these options, Reflection connects to your host via the Reflection Security Proxy included in Reflection Security Gateway. You can use this Security Proxy to configure secure connections even if your host is not running an SSL/TLS-enabled Telnet server.

**NOTE**

- When the Security Proxy is used, the connection between the client and the Security Proxy server is secured and encrypted using the SSL/TLS protocol. By default, the information sent between the proxy server and the destination host is in the clear. If you enable the **End-to-End encryption** option (available for 5250, 3270, and VT sessions), information sent between the Security Proxy and the destination host is also encrypted. (**End-to-End encryption** requires that the host support SSL/TLS.)

- If you configure sessions that connect through the Security Proxy with authorization enabled, users must log onto the Reflection Security Gateway server before they can connect using these sessions.

<table>
<thead>
<tr>
<th>Retrieve and validate certificate chain</th>
<th>Specifies whether certificates presented for host authentication are checked to determine if they are valid and signed by a trusted CA. Note: Certificate validation is required when SSL/TLS version is set to TLS version 1.0 or TLS version 1.2. To clear this setting (which disables certificate validation), you must set SSL/TLS version to SSL Version 3.0. <strong>CAUTION:</strong> Clearing this setting creates a security risk by allowing host authentication with unvalidated certificates.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Reflection Security Proxy Server Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Use Reflection security proxy and related settings are visible if you use Reflection Security Gateway (available separately from Attachmate) to manage sessions and you launched this session from the Administrative WebStation. With these options, Reflection connects to your host via the Reflection Security Proxy included in Reflection Security Gateway. You can use this Security Proxy to configure secure connections even if your host is not running an SSL/TLS-enabled Telnet server.</td>
<td></td>
</tr>
<tr>
<td><strong>NOTE</strong></td>
<td></td>
</tr>
<tr>
<td>- When the Security Proxy is used, the connection between the client and the Security Proxy server is secured and encrypted using the SSL/TLS protocol. By default, the information sent between the proxy server and the destination host is in the clear. If you enable the <strong>End-to-End encryption</strong> option (available for 5250, 3270, and VT sessions), information sent between the Security Proxy and the destination host is also encrypted. (<strong>End-to-End encryption</strong> requires that the host support SSL/TLS.)</td>
<td></td>
</tr>
<tr>
<td>- If you configure sessions that connect through the Security Proxy with authorization enabled, users must log onto the Reflection Security Gateway server before they can connect using these sessions.</td>
<td></td>
</tr>
<tr>
<td><strong>Use Reflection security proxy</strong></td>
<td>Configure this session to use the Reflection Security Proxy for the server connection.</td>
</tr>
<tr>
<td><strong>Security proxy</strong></td>
<td>Select the proxy server name from the drop-down list shows, which shows available servers.</td>
</tr>
<tr>
<td><strong>Proxy port</strong></td>
<td>Select the proxy server port from the drop-down list.</td>
</tr>
<tr>
<td><strong>Destination host</strong></td>
<td>If client authorization is enabled on the Security Proxy, enter the destination host name. If client authorization is not enabled, this box is read only. When you select a security port, the destination host configured to use that port is displayed automatically.</td>
</tr>
<tr>
<td><strong>Destination port</strong></td>
<td>If client authorization is enabled on the Security Proxy, enter the destination host name. If client authorization is not enabled, this box is read only. When you select a security port, the destination port and destination host are displayed automatically.</td>
</tr>
<tr>
<td><strong>End-to-End encryption</strong></td>
<td>This option tunnels a direct SSL/TLS connection to the host, while still connecting through the Reflection Security Proxy Server. These connections require two certificates and two SSL/TLS handshakes—one for the client/proxy server connection and another for the client/host connection.</td>
</tr>
<tr>
<td><strong>Proxy cipher suites</strong></td>
<td>A read-only list of cipher suites supported by this Reflection proxy host and port. This list is only visible when the product is launched from the Administrative WebStation (included with Reflection Security Gateway).</td>
</tr>
</tbody>
</table>
SSL/TLS Tab (FTP Options)

Getting there (FTP Client)

1. In the Connect to FTP Site dialog box, select a site.
2. Click Security.

The Secure Sockets Layer protocol (SSL) and its compatible successor, the Transport Layer Security protocol (TLS), enable a client and server to establish a secure, encrypted connection over a public network. When you connect using SSL/TLS, the client authenticates the server before making a connection, and all data passed between InfoConnect and the server is encrypted. Depending on the server configuration, the server may also authenticate the client.

The options are:

- **Use SSL/TLS Security**: Enables SSL/TLS connections. You must select this before you can set other values on the SSL/TLS tab. When Use SSL/TLS security is selected, Reflection will only connect to the host if a secure SSL/TLS connection can be established.

  Before making an SSL/TLS connection, Reflection must authenticate the host. Authentication is handled through the use of digital certificates. These certificates are part of the same Public Key Infrastructure (PKI) that is used to secure internet transactions. Your computer must be configured to recognize the digital certificate presented by your host and, if necessary, to provide a certificate for client authentication. If your computer is not properly configured, or if the certificates presented for authentication are not valid, you will not be able to make SSL/TLS connections. Depending on how a host certificate was issued, you may need to install a certificate on your local computer.

- **Configure PKI**: Opens the PKI Configuration (page 523) dialog box, which you can use to configure PKI settings for Reflection SSL/TLS sessions.

- **Encryption Strength**: Specify the desired level of encryption for SSL/TLS connections. The connection will fail if this level cannot be provided.

  If you select Default, any encryption level is permitted, and Reflection will negotiate with the host system to choose the strongest encryption level supported by both the host and the client. If you are running in FIPS mode and select Default, Reflection will negotiate using only FIPS compliant encryption levels.

- **Encrypt Data Stream**: Specifies whether or not data is encrypted when the FTP client is configured to use SSL/TLS encryption. When this checkbox is selected, all communication between your computer and the FTP server is encrypted. When this checkbox is cleared, the FTP command channel (which is used for all FTP commands, including your user name and password) is encrypted. However, the data channel (which is used for directory listings and the contents of the files you transfer) is not encrypted.

- **Clear command channel**: When this is enabled, FTP Client sends a CCC command to the host. If the host supports this option, this turns off encryption for the command channel only.
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL/TLS version</td>
<td>Specifies which SSL or TLS version to use.</td>
</tr>
<tr>
<td>Retrieve and validate</td>
<td>Specifies whether certificates presented for host authentication are checked to determine if they are valid and signed by a trusted CA. Certificate validation is required when SSL/TLS version is set to TLS version 1.0 or TLS version 1.2. To clear this setting (which disables certificate validation), you must set SSL/TLS version to SSL Version 3.0.</td>
</tr>
<tr>
<td>certificate chain</td>
<td>CAUTION: Clearing this setting creates a security risk by allowing host authentication with unvalidated certificates.</td>
</tr>
<tr>
<td>Implicit SSL/TLS connection</td>
<td>By default the FTP Client makes SSL/TLS connections using Explicit security. In order to establish the SSL connection, explicit security requires that the FTP client issue a specific command (AUTH TLS) to the FTP server after establishing a connection. If the server gives a success response, the client begins the TLS negotiation. The default FTP server port (21) is used.</td>
</tr>
<tr>
<td>Connect through a NAT server</td>
<td>Select this setting if your FTP Client connects through a NAT (Network Address Translation) server. When this setting is selected, the FTP Client ignores IP addresses in FTP commands returned from the server.</td>
</tr>
<tr>
<td>Run in FIPS Mode</td>
<td>When you run in FIPS mode, all connections are made using security protocols and algorithms that meet FIPS 140-2 standards. In this mode some standard connection options are not available. A FIPS mode icon is visible on the status bar when a connection is made using FIPS mode.</td>
</tr>
</tbody>
</table>

**Reflection Security Proxy Server Settings**

- **Use Reflection security proxy** and related settings are visible if you use Reflection Security Gateway (available separately from Attachmate) to manage sessions and you launched this session from the Administrative WebStation. With these options, Reflection connects to your host via the Reflection Security Proxy included in Reflection Security Gateway. You can use this Security Proxy to configure secure connections even if your host is not running an SSL/TLS-enabled Telnet server.

**NOTE**

- When the Security Proxy is used, the connection between the client and the Security Proxy server is secured and encrypted using the SSL/TLS protocol. By default, the information sent between the proxy server and the destination host is in the clear. If you enable the...
End-to-End encryption option (available for 5250, 3270, and VT sessions), information sent between the Security Proxy and the destination host is also encrypted. (End-to-End encryption requires that the host support SSL/TLS.)

- If you configure sessions that connect through the Security Proxy with authorization enabled, users must log onto the Reflection Security Gateway server before they can connect using these sessions.

<table>
<thead>
<tr>
<th>Use Reflection security proxy</th>
<th>Configure this session to use the Reflection Security Proxy for the server connection.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security proxy</td>
<td>Select the proxy server name from the drop-down list shows, which shows available servers.</td>
</tr>
<tr>
<td>Proxy port</td>
<td>Select the proxy server port from the drop-down list.</td>
</tr>
<tr>
<td>Destination host</td>
<td>If client authorization is enabled on the Security Proxy, enter the destination host name. If client authorization is not enabled, this box is read only. When you select a security port, the destination host configured to use that port is displayed automatically.</td>
</tr>
<tr>
<td>Destination port</td>
<td>If client authorization is enabled on the Security Proxy, enter the destination host name. If client authorization is not enabled, this box is read only. When you select a security port, the destination port and destination host are displayed automatically.</td>
</tr>
<tr>
<td>End-to-End encryption</td>
<td>This option tunnels a direct SSL/TLS connection to the host, while still connecting through the Reflection Security Proxy Server. These connections require two certificates and two SSL/TLS handshakes—one for the client/proxy server connection and another for the client/host connection.</td>
</tr>
<tr>
<td>Proxy cipher suites</td>
<td>A read-only list of cipher suites supported by this Reflection proxy host and port. This list is only visible when the product is launched from the Administrative WebStation (included with Reflection Security Gateway).</td>
</tr>
</tbody>
</table>

Related Topics

- “Which Protocols Can I Use?” on page 512
- “Digital Certificates in SSL/TLS Sessions” on page 341

PKI Configuration Dialog Box

Index Term
Primary: SSL/TLS
Secondary: strict host name checking

Index Term
Primary: PKI
Secondary: PKI Configuration dialog box

Getting there

1. Open the Security Properties (page 511) dialog box.
2. On the SSL/TLS tab, select Use SSL/TLS security.
3. Click Configure PKI.
Use the **PKI Configuration** dialog box to configure PKI (page 438) settings for Reflection SSL/TLS sessions.

**NOTE:** To configure PKI settings for Secure Shell sessions use the **PKI** tab in the **Reflection Secure Shell Settings** dialog box.

The options are:

**Certificate host name must match host being contacted**

Specifies whether host name matching is required when validating host certificates. When this setting is enabled (the default), the host name you configure in Reflection must exactly match a host name or IP address entered in either the **CommonName** or the **SubjectAltName** field of the certificate.

**Use OCSP**

Specifies whether Reflection checks for certificate revocation using **OCSP** (page 888) (Online Certificate Status Protocol) responders when validating host certificates. OCSP responders may be specified in the AIA extension of the certificate itself. You can also specify OCSP responders using the **OCSP** (page 453) tab in the Reflection Certificate Manager.

**Use CRL**

Specifies whether Reflection checks for certificate revocation using **CRLs** (page 887) (Certificate Revocation Lists) when validating host certificates. CRLs may be specified in the CDP extension of the certificate itself. You can also specify CRL using the **LDAP** (page 451) tab in the Reflection Certificate Manager.

**Note:** The default value of this setting is based on your current system setting for CRL checking. To view and edit the system setting, launch Internet Explorer, and go to **Tools > Internet Options > Advanced**. Under **Security**, look for **Check for server certificate revocation**.

**Client Authentication**

When **Find certificate for authentication** is selected, all available personal certificates are presented to the server for client authentication.

To specify a particular certificate, select **Use selected certificate for authentication**, then click **Select** to specify which certificate.

**Reflection Certificate Manager**

Opens the **Reflection Certificate Manager**, which you can use to manage certificates in the Reflection stores and to specify PKI settings.

**View System Certificates**

Opens the **Windows Certificate Manager**, which you can use to manage certificates in your system stores.

**Related Topics**

- “PKI Overview” on page 438
Printing from IBM Sessions

InfoConnect supports several types of printing. You can:

- Print the current host screen.
- Configure InfoConnect for 3270 printer emulation and use your local printer to print host print jobs.
- Configure InfoConnect for 5250 printer emulation and use your local printer to print host print jobs.

All three of these types of printing share some dialog boxes, such as Page Setup and Print Setup, but changes to shared dialog boxes in one session won't be saved in the same dialog box in a different session.

In this Section

- “3270 Printer Emulation” on page 526
- “5250 Printer Emulation” on page 535
- “Configure Printer Session Settings” on page 546
- “Page Setup Dialog Box” on page 548
- “Page Options Dialog Box” on page 550
- “Page Scaling Dialog Box” on page 551
3270 Printer Emulation

In this Section

- “Create a 3270 Printer Session” on page 526
- “Associate a 3270 Printer Session with a Terminal Session” on page 527
- “Session Setup Dialog Box (3270 Printer Sessions)” on page 528
- “IBM 3270 Printer Panel” on page 529
- “Status Messages (3270 Printer Sessions)” on page 531
- “Advanced 3270 Telnet Dialog Box (Printer Sessions)” on page 532
- “Printer Session Setup Dialog Box (3270 Printer Sessions)” on page 533

Create a 3270 Printer Session

InfoConnect 3270 printer sessions emulate IBM 3287 printers. Data sent from the host to the printer session is passed on to the local printer.

To create a 3270 printer session from the InfoConnect Workspace

1. Open the Create New Document dialog box.
   The steps depend on your user interface mode (page 120).

   - **User Interface Mode**
     - Ribbon or Reflection Browser: From the Quick Access Toolbar, click the New Document button.
     - TouchUx: Tap the Folder icon and then under File, select New.

2. Select 3270 Printer and click Create.
3. In the Enter Host Name or IP Address dialog box, type a host name or IP address, and click Connect to connect immediately, or Cancel to configure more than just the host name.
To create a 3270 printer session from the Windows Start menu

1. From the Windows Start menu, choose **All Programs > Attachmate Reflection > Reflection IBM Printer**.
   
   Printer sessions created this way use 3270 printer emulation by default.

2. In the **Enter Host Name or IP Address** dialog box, type a host name or IP address, and click **Connect** to connect immediately, or **Cancel** to configure more than just the host name.

Related Topics

- “Associate a 3270 Printer Session with a Terminal Session” on page 527
- “Configure Printer Session Settings” on page 546
- “IBM 3270 Printer Panel” on page 529
- “Printing from IBM Sessions” on page 525

## Associate a 3270 Printer Session with a Terminal Session

**Index Term**

*Primary:* TN association

**Index Term**

*Primary:* association string

**Index Term**

*Primary:* associating printer sessions with terminals

There are two ways to associate a 3270 terminal session with a printer session:

<table>
<thead>
<tr>
<th>To</th>
<th>Link the terminal session to</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open the printer session automatically when the terminal session connects, and close it when the terminal session closes</td>
<td>A printer session document.</td>
</tr>
<tr>
<td>Retain manual control over opening and closing printer sessions</td>
<td>A printer session using an association string.</td>
</tr>
</tbody>
</table>

### To link a terminal session to a printer session document

1. Open a 3270 terminal session.

2. **Open the Document Settings dialog box.**
   
   The steps depend on your **user interface mode** (page 120).

   **User Interface Mode** | **Steps** |
   | | |
   | Ribbon or Reflection Browser | With a session open in Reflection, from the **Quick Access Toolbar**, click **.** |
   | TouchUx | Tap the Gear icon and then select **Document Settings**. |

3. Under **Host Connection**, click **Configure Advanced Connection Settings**.


5. Select the **Associated 3270 printer session** option.
To link a terminal session to a printer session using an association string

1. Open a 3270 terminal session.
2. Open the Document Settings dialog box.
   - The steps depend on your user interface mode (page 120).
3. Under Host Connection, click Configure Advanced Connection Settings.
5. Select Association string, and type the association string you want to use.
6. Click OK.
7. Open a 3270 printer session.
   - Disconnect it if necessary. If you are creating a new session, don’t connect to the host yet.
8. From the Connection menu, choose Session Setup.
9. Under Transport, from the Connection type list, choose Associate.
10. In the TN Association box, type the printer string you specified for Association string in your terminal session.
11. Click OK.

Related Topics
- “Create a 3270 Printer Session” on page 526
- “Configure Advanced Connection Settings Dialog Box” on page 221
- “Printing from IBM Sessions” on page 525

Session Setup Dialog Box (3270 Printer Sessions)

Index Term
Primary: sessions
Secondary: Session Setup dialog box (3270 printer session)

Index Term
Primary: Session Setup dialog box (3270 printer session)

Getting there

1. Open a printer session.
2. From the Connection menu, choose Session Setup.

Use the Session > Setup dialog box to configure the connection to an IBM host for printer emulation sessions.
NOTE: You cannot configure the settings from this dialog box when you are connected to a host.

Session

**Type**
Select the type of printer session you want. The options on this dialog box (and the Help topic) change if you modify this setting.

**Model ID**
InfoConnect 3270 printer sessions emulate IBM 3277 printers.

Transport

**Type**
Select the transport to use.

**Enter Host (or System) Name or IP Address**
Identify the host to which you will connect. Type the host name, alias, or numeric IP address.

**Port**
Type the host port or socket number that the session should use. This field accepts any number between 0 and 66,535 (default = 23).

**Connection type (Telnet Extended)**
Select Connect when the LU name to which you are connecting is the name of a particular printer device. Select Associate to associate the printer session to a terminal session using an association string.

**Host LU name**
When you connect as a 3277 printer, some hosts require a host LU name. The name can be up to 32 characters in length.

**TN association (Telnet Extended)**
This option is available when Connection type is set to Associate. It displays a list of association strings you can configure using the Configure Advanced Connection Settings dialog box in a terminal session.

**Advanced**
Configure advanced Telnet settings.

Connect options

**Auto connect**
Select to establish a host connection as soon as the printer session is started.

**Security**
Secure data communications with SOCKS or SSL/TLS.

Related Topics

- “Configure Printer Session Settings” on page 546
- “Printer Session Setup Dialog Box (3270 Printer Sessions)” on page 533

IBM 3270 Printer Panel

Index Term
Primary: program attention keys
Secondary: 3270 printer panel
InfoConnect 3270 printer sessions emulate IBM 3287 printers. Data sent from the host to the printer session is passed on to the local printer.

The following items appear on the 3270 printer panel.

**Printer Control**

- **Hold/Enable**
  
  Click **Hold** to stop sending data to the printer. The word **Hold** appears in the Status box and the **Hold** button becomes the **Enable** button. While the printer is on hold, the **Reset** and **Flush** buttons become available. To cancel a hold, click **Enable**.

- **Cancel**
  
  Send a Cancel Print message to the host. **Cancelled** is displayed in the Status box.

- **Reset**
  
  Clear an error or cancel a condition. After a reset, printing continues (any hold is terminated and the status message becomes **Printing**.)

- **Flush**
  
  Force any pending printer output to the printer. If you’re printing to a file, this action forces data to the file, and then closes the file.

**Forms Control**

- **Form feed**
  
  Advance the paper in the printer to the top of the next page. This button is available only when the printer is on hold.

- **Line feed**
  
  Advance the paper in the printer one line. This button is available only when the printer is on hold.

**Host Control**

- **PA1 and PA2**
  
  Send a Program Attention signal to the host.
Additional Items

<table>
<thead>
<tr>
<th>Status</th>
<th>Displays printer status messages.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test page</td>
<td>Print a test page. If you are connected, click Hold first. If no errors are detected, the printer goes back online automatically after the test.</td>
</tr>
<tr>
<td>Setup</td>
<td>Open the Printer Session Setup dialog box, from which you can configure host-related printing options.</td>
</tr>
<tr>
<td>Info</td>
<td>Display information about your current printer configuration and font selection.</td>
</tr>
</tbody>
</table>

Related Topics

- “Status Messages (3270 Printer Sessions)” on page 531
- “Configure Printer Session Settings” on page 546
- “Printing from IBM Sessions” on page 525

Status Messages (3270 Printer Sessions)

Index Term
Primary: status messages
Secondary: 3270 printer sessions

Index Term
Primary: bells
Secondary: status message (3270 Printer Sessions)

Printer messages that appear in the Status box are color-coded:

- Green indicates that the printer session is online.
- Yellow indicates that the printer session is offline.
- Red indicates an error condition.
The messages that can appear in the Status box (and their respective colors) are:

<table>
<thead>
<tr>
<th>Message</th>
<th>Meaning</th>
<th>Color</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bell</td>
<td>The Bell data stream control was received.</td>
<td>Green</td>
</tr>
<tr>
<td>Cancelled</td>
<td>The pending print job (if any) has been cancelled.</td>
<td>Yellow</td>
</tr>
<tr>
<td>Command Rejected</td>
<td>An invalid or unsupported data stream control was encountered.</td>
<td>Red</td>
</tr>
<tr>
<td>Data Check</td>
<td>Invalid print data was received.</td>
<td>Red</td>
</tr>
<tr>
<td>Disconnected</td>
<td>No host connection.</td>
<td>Yellow</td>
</tr>
<tr>
<td>Error</td>
<td>An unknown error has occurred.</td>
<td>Red</td>
</tr>
<tr>
<td>Hold</td>
<td>The printer is offline.</td>
<td>Yellow</td>
</tr>
<tr>
<td>Host Link Down</td>
<td>The link between the gateway and the host has been lost.</td>
<td>Yellow</td>
</tr>
<tr>
<td>Operation Check</td>
<td>An illegal buffer address or incomplete data stream control was received.</td>
<td>Red</td>
</tr>
<tr>
<td>Printer Error</td>
<td>An error has occurred in writing to the printer.</td>
<td>Red</td>
</tr>
<tr>
<td>Printing</td>
<td>The printer is printing.</td>
<td>Green</td>
</tr>
<tr>
<td>Ready</td>
<td>The printer is ready to print.</td>
<td>Green</td>
</tr>
</tbody>
</table>

Related Topics

- “IBM 3270 Printer Panel” on page 529
- “Configure Printer Session Settings” on page 546

Advanced 3270 Telnet Dialog Box (Printer Sessions)

Index Term
Primary: terminal ID
Secondary: 3270 printer sessions

Index Term
Primary: telnet location
Secondary: 3270 printer sessions

Index Term
Primary: response mode (3270 printing)

Index Term
Primary: keep alive
Secondary: 3270 printer sessions

Getting there

1. Open a printer session.
2. From the Connection menu, choose Session Setup.
3. From the Type list, choose a printer session type.
4. Click the Advanced button.
The options are:

**Terminal ID**
This setting is not available when configuring Telnet Extended sessions.
Specify a terminal model only if you are unable to connect to the host using the available Model ID settings from the Session Setup dialog box.

If the host can't recognize the specified Telnet Terminal ID string, you may have difficulty connecting, or, once connected, you may experience emulation problems.

**Telnet location**
(Optional) Type up to 41 characters of descriptive text to provide information about your session. For example, you might include your PC's location, computer name, or IP address.

This features uses the SEND-LOCATION option supported under Telnet connections (RFC779).

**Response mode** *(Telnet Extended)*
Select to send a response from the PC each time a message is received from the host.

For improved performance, clear this option.

**Send Keep Alive packets**
Select to provide a constant check between your session and the host so that you become aware of connection problems as they occur.

Choose one of the three types of keep-alive packets:

<table>
<thead>
<tr>
<th>Choose</th>
<th>To cause</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System</strong></td>
<td>The TCP/IP stack to keep track of the host connection. This method requires less system resources than Send NOP Packets or Send Timing Mark Packets. However, most TCP/IP stacks send Keep Alive packets infrequently.</td>
</tr>
<tr>
<td><strong>Send NOP Packets</strong></td>
<td>InfoConnect to periodically send a No Operation (NOP) command to the host. The host is not required to respond to these commands, but the TCP/IP stack can detect if there was a problem delivering the packet.</td>
</tr>
<tr>
<td><strong>Send Timing Mark Packets</strong></td>
<td>InfoConnect to periodically send a Timing Mark Command to the host to determine if the connection is still active. The host should respond to these commands. If InfoConnect does not receive a response or there is an error sending the packet, it shuts down the connection.</td>
</tr>
</tbody>
</table>

**Keep Alive timeout in seconds**
Select the interval between the keep-alive requests. The range of values is 1 to 9999 seconds; the default value is 600 seconds.

---

### Printer Session Setup Dialog Box (3270 Printer Sessions)

**Index Term**
Primary: EBCDIC
Secondary: translate in the SCS TRN command (ebcdic)
Getting there

1. Open a 3270 printer session.
2. From the printer panel, click the Setup button.

The options are:

Character translation

- **National character set**: Determines how host characters (EBCDIC) are mapped to PC characters (ANSI). This setting should match the national character set used by your host system.

- **Country Extended Graphics Code**: Select to make additional characters available in the configured National character set. See your host documentation for details.

- **Transparent mode**: Select this check box for printer-ready documents that require no page formatting. In Transparent mode, all page format settings (Characters per line and Lines per page) are ignored.

- **Translate EBCDIC in SCS TRN transparent mode**: When this check box is selected, InfoConnect translates EBCDIC characters in the SCS TRN command.

- **Bypass Windows print driver in transparent mode**: Select to disable Windows handling of fonts, font size, font style, and lines-per-inch configuration while in Transparent mode.

Flush printing options

- **Flush when End of Job record received**: Select if you want an in-progress print job to close if an end-of-job condition is sent from the host.

- **Host print timeout for flushing**: Specify the number of seconds to wait after the host stops sending data to a printer session before forcing all pending printer output to the printer.
Form feed options

- **Emulate form feed with line feed**
  Select to have InfoConnect simulate a form feed by issuing line feeds until the end of the page is reached.

- **Send form feed at end of job**
  Select to send a form feed at the conclusion of host print jobs.

Related Topics

- “Configure Printer Session Settings” on page 546
- “Session Setup Dialog Box (3270 Printer Sessions)” on page 528

5250 Printer Emulation

In this Section

- “Create a 5250 Printer Session” on page 535
- “Session Setup Dialog Box (5250 Printer Sessions)” on page 536
- “IBM 5250 Printer Panel” on page 538
- “Status Messages (5250 Printer Sessions)” on page 539
- “Exception Messages (5250 Printing)” on page 540
- “Advanced 5250 Telnet Dialog Box (Printer Sessions)” on page 541
- “5250 Printer Device Initialization Dialog Box” on page 542
- “Printer Session Setup Dialog Box (5250 Printer Sessions)” on page 544
- “Font Mapping (5250 Printer Sessions)” on page 545
- “Fonts Dialog Box” on page 546

Create a 5250 Printer Session

InfoConnect 5250 printer sessions emulate IBM 3812 printers. Data sent from the host to the printer session is passed on to the local printer.

To create a 5250 printer session from the InfoConnect Workspace

1. Open the Create New Document dialog box.

   The steps depend on your user interface mode (page 120).

   **User Interface Mode** | **Steps**
   | Ribbon or Reflection Browser | From the Quick Access Toolbar, click the New Document button.
   | TouchUx | Tap the Folder icon and then under File, select New.
2 Select **5250 Printer** and click **Create**.

3 In the **Enter Host Name or IP Address** dialog box, type a host name or IP address, and click **Connect** to connect immediately, or **Cancel** to configure more than just the host name.

**To create a 5250 printer session from the Windows Start menu**

1 From the Windows Start menu, choose **All Programs > Attachmate Reflection > Reflection IBM Printer**.

   Printer sessions created this way use 3270 printer emulation by default.

   Use the following steps to change to a 5250 printer session.

2 Click **Cancel** to close the **Enter Host Name or IP Address** dialog box.

3 From the **Connection** menu, choose **Session Setup**.

4 Under **Session**, from the **Type** list, choose **IBM 5250 Printer**.

5 For **Host Name/IP Address**, enter the fully qualified host name.

6 Click **Connect** to connect immediately, or click **OK** to configure additional settings.

**Related Topics**

- “Configure Printer Session Settings” on page 546
- “IBM 5250 Printer Panel” on page 538
- “Printing from IBM Sessions” on page 525

**Session Setup Dialog Box (5250 Printer Sessions)**

**Index Term**

Primary: sessions
Secondary: Session Setup dialog box (5250 printer session)

**Index Term**

Primary: Session Setup dialog box (5250 printer session)

Getting there

1 *Open a printer session.*

2 From the **Connection** menu, choose **Session Setup**.

Use the **Session > Setup** dialog box to configure the connection to an IBM host for printer emulation sessions.

Note: You cannot configure the settings from this dialog box when you are connected to a host.

**Session**

**Type**

Select the type of printer session you want. The options on this dialog box (and the Help topic) change if you modify this setting.

**Model ID**

Select the printer model to emulate.

**Transport**

**Type**

5250 printer sessions use Telnet.
Enter Host (or System) Name or IP Address

Identify the host to which you will connect. Type the host name, alias, or numeric IP address.

**NOTE**: Both IPv4 addresses (in the form 127.0.0.1) and IPv6 addresses (in the form 2001:0db8:3c4d:0015:0000:0000:abcd:ef12) are accepted.

Port

Type the host port or socket number that the session should use. This field accepts any number between 0 and 66,535 (default = 23).

Device name

Specify the terminal device name (also called the display name or the workstation ID) that the AS/400 should use for your session. If you leave this box blank, the AS/400 creates a device to use for your session.

The device name can be up to ten characters long. You can include any of the following characters as part of the value in the Device name box.

<table>
<thead>
<tr>
<th>Character</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Replaced by A, B, C, and so on to create a unique device name. If the entire alphabet is used, the generated device names continue with AA, AB, AC, and so on.</td>
</tr>
<tr>
<td>%</td>
<td>Replaced by P for printer sessions and S for display sessions.</td>
</tr>
<tr>
<td>=</td>
<td>Replaced by 1, 2, 3, and so on to create a unique device name.</td>
</tr>
<tr>
<td>&amp;COMPN</td>
<td>Replaced by the local workstation name, left-trimmed, if the generated name exceeds 10 characters.</td>
</tr>
<tr>
<td>&amp;USERN</td>
<td>Replaced by the local user name, left-trimmed, if the generated name exceeds 10 characters.</td>
</tr>
<tr>
<td>+</td>
<td>Specifies right-trimming instead of left-trimming. Use with &amp;COMPN or &amp;USERN. This character can be placed anywhere in the string.</td>
</tr>
</tbody>
</table>

**NOTE**

- You can use only one string in combination with these characters. If you use separated strings, the second string is dropped. For example, %MyDevice= is valid. However, %My=Device is not valid, and will be treated by the system as if it were &My=.
- You cannot use both &COMPN and &USERN in the same string.
- To have InfoConnect generate unique device names automatically based on the special characters described above, the Generate Device Names setting must be enabled. In printer sessions, this setting is off by default. To enable it, see the “Generate Device Names” on page 588 topic.

Advanced

Configure advanced Telnet settings.
Connect options

Auto connect
Select to establish a host connection as soon as the printer session is started.

Initialize
Create and initialize printer devices on your AS/400 host.

Security
Secure data communications with SOCKS or SSL/TLS.

Related Topics
• “Configure Printer Session Settings” on page 546
• “Printer Session Setup Dialog Box (5250 Printer Sessions)” on page 544

IBM 5250 Printer Panel

InfoConnect 5250 printer sessions emulate IBM 3812 printers. Data sent from the host to the printer session is passed on to the local printer.

The following items appear on the 5250 printer panel.

Printer Control

Hold/Enable
Click Hold to stop sending data to the printer. The word Hold appears in the Status box and the Hold button becomes the Enable button. While the printer is on hold, the Reset and Flush buttons become available. To cancel a hold, click Enable.

Cancel
Send a Cancel Print message to the host.

Cancelled is displayed in the Status box.

Reset
Clear an error or cancel a condition.

After a reset, printing continues (any hold is terminated and the status message becomes Printing.)

Flush
Force any pending printer output to the printer. If you’re printing to a file, this action forces data to the file, and then closes the file.
Forms Control

Form feed
Advance the paper in the printer to the top of the next page. This button is available only when the printer is on hold.

Line feed
Advance the paper in the printer one line. This button is available only when the printer is on hold.

Additional Items

Status
Displays printer status messages.

Test page
Print a test page. If you are connected, click Hold first. If no errors are detected, the printer goes back online automatically after the test.

Setup
Open the Printer Session Setup dialog box, from which you can configure host-related printing options.

Info
Display information about your current printer configuration and font selection.

Related Topics

- “Status Messages (5250 Printer Sessions)” on page 539
- “Configure Printer Session Settings” on page 546
- “Printing from IBM Sessions” on page 525

Status Messages (5250 Printer Sessions)

Printer messages that appear in the Status box are color-coded:

- Green indicates that the printer session is online.
- Yellow indicates that the printer session is offline.
- Red indicates an error condition.
The messages that can appear in the Status box (and their respective colors) are:

<table>
<thead>
<tr>
<th>Message</th>
<th>Meaning</th>
<th>Color</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bell</td>
<td>The Bell data stream control was received.</td>
<td>Green</td>
</tr>
<tr>
<td>Cancelled</td>
<td>The pending print job (if any) has been cancelled.</td>
<td>Yellow</td>
</tr>
<tr>
<td>Connected</td>
<td>Indicates the session is connected, but the host is not yet ready to</td>
<td>Yellow</td>
</tr>
<tr>
<td></td>
<td>send print data.</td>
<td></td>
</tr>
<tr>
<td>Disconnected</td>
<td>No host connection.</td>
<td>Yellow</td>
</tr>
<tr>
<td>Error</td>
<td>An unknown error has occurred.</td>
<td>Red</td>
</tr>
<tr>
<td>Exception nn</td>
<td>A data stream formatting error has been encountered; nn is the exception code.</td>
<td>Red</td>
</tr>
<tr>
<td>Hold</td>
<td>The printer is offline.</td>
<td>Yellow</td>
</tr>
<tr>
<td>Host Link Down</td>
<td>The link between the gateway and the host has been lost.</td>
<td>Yellow</td>
</tr>
<tr>
<td>Printer Error</td>
<td>An error has occurred in writing to the printer.</td>
<td>Red</td>
</tr>
<tr>
<td>Printing</td>
<td>The printer is printing.</td>
<td>Green</td>
</tr>
<tr>
<td>Ready</td>
<td>The printer is ready to print.</td>
<td>Green</td>
</tr>
</tbody>
</table>

Related Topics

- “Exception Messages (5250 Printing)” on page 540
- “Configure Printer Session Settings” on page 546

Exception Messages (5250 Printing)

Index Term

Primary: exception messages (5250 printer)

If you are running a 5250 printer emulation code, you may see an exception code display in the printer panel Status box. Refer to the following table for more information.

<table>
<thead>
<tr>
<th>Code</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>The data stream control is unsupported or unrecognized.</td>
</tr>
<tr>
<td>11</td>
<td>Printing will occur outside the specified left or right margin.</td>
</tr>
<tr>
<td>12</td>
<td>An illegal superscript or subscript character was received.</td>
</tr>
<tr>
<td>13</td>
<td>The data stream control is not supported unless the Bypass Windows print driver in transparent mode (page 544) check box is selected.</td>
</tr>
<tr>
<td>14</td>
<td>A graphics character is unprintable.</td>
</tr>
<tr>
<td>15</td>
<td>The data stream control is not supported while the Bypass Windows print driver in transparent mode (page 544) check box is selected.</td>
</tr>
<tr>
<td>16</td>
<td>Printing will occur above or below the specified top or bottom margin.</td>
</tr>
<tr>
<td>17</td>
<td>A control in the data stream is illegally nested.</td>
</tr>
<tr>
<td>20</td>
<td>A supported control exists at an invalid position in the data stream.</td>
</tr>
</tbody>
</table>
**Advanced 5250 Telnet Dialog Box (Printer Sessions)**

**Index Term**
- Primary: telnet location
- Secondary: 5250 printer sessions

**Index Term**
- Primary: keep alive
- Secondary: 5250 printer sessions

**Getting there**

1. Open a printer session.
2. From the **Connection** menu, choose **Session Setup**.
3. From the **Type** list, choose a printer session type.
4. Click the **Advanced** button.

The options are:

<table>
<thead>
<tr>
<th>Code</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>21</td>
<td>An invalid indent level was received or there is no tab stop at the specified indent level.</td>
</tr>
<tr>
<td>22</td>
<td>No horizontal tab stop setting found.</td>
</tr>
<tr>
<td>23</td>
<td>The length of a line exceeds the justified right margin or the margin exceeds the page width.</td>
</tr>
<tr>
<td>24</td>
<td>Backspacing will occur beyond the leftmost physical print position.</td>
</tr>
<tr>
<td>25</td>
<td>Text will be printed below the bottom of the page.</td>
</tr>
<tr>
<td>26</td>
<td>Justify control violation.</td>
</tr>
<tr>
<td>30</td>
<td>Unsupported data stream control.</td>
</tr>
<tr>
<td>31</td>
<td>A required control parameter is missing.</td>
</tr>
<tr>
<td>32</td>
<td>An unsupported control parameter has been detected.</td>
</tr>
<tr>
<td>40</td>
<td>Invalid parameter value in multi-byte control.</td>
</tr>
</tbody>
</table>

**Telnet location**

(Optional) Type up to 41 characters of descriptive text to provide information about your session. For example, you might include your PC’s location, computer name, or IP address.

This feature uses the SEND-LOCATION option supported under Telnet connections (RFC779).

*InfoConnect* does not initiate a WILL SEND command unless you activate the **Telnet location** option by typing information in this box.
**Send Keep Alive packets**

Select to provide a constant check between your session and the host so that you become aware of connection problems as they occur.

Choose one of the three types of keep-alive packets:

<table>
<thead>
<tr>
<th>Choose</th>
<th>To cause</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System</strong></td>
<td>The TCP/IP stack to keep track of the host connection. This method requires less system resources than Send NOP Packets or Send Timing Mark Packets. However, most TCP/IP stacks send Keep Alive packets infrequently.</td>
</tr>
<tr>
<td><strong>Send NOP Packets</strong></td>
<td>InfoConnect to periodically send a No Operation (NOP) command to the host. The host is not required to respond to these commands, but the TCP/IP stack can detect if there was a problem delivering the packet.</td>
</tr>
<tr>
<td><strong>Send Timing Mark Packets</strong></td>
<td>InfoConnect to periodically send a Timing Mark Command to the host to determine if the connection is still active. The host should respond to these commands. If InfoConnect does not receive a response or there is an error sending the packet, it shuts down the connection.</td>
</tr>
</tbody>
</table>

**Keep Alive timeout in seconds**

Select the interval between the keep-alive requests. The range of values is 1 to 9999 seconds; the default value is 600 seconds.

![This content is pasted into objects 7112 and 14460 (3270 and 5250 adv conn)](image-url)

**Related Topics**

- “Session Setup Dialog Box (5250 Printer Sessions)” on page 536
- “Configure Printer Session Settings” on page 546

**5250 Printer Device Initialization Dialog Box**

**Index Term**

Primary: initialization, 5250 printer device

**Index Term**

Primary: device

Secondary: initialization, 5250 printer

**Getting there**

1. Open a 5250 printer session.
2. From the **Connection** menu, choose **Session Setup**.
3. Click the **Initialize** button.

Create and initialize 3812 printer devices on your AS/400 host.
The options are:

**Message library**
Select the library that contains the message queue for exception messages. Consult your system administrator before changing this value.

**Message queue**
Select the message queue to which exception messages should be sent. For example, the AS/400 may need to tell the printer to switch to another paper tray. Consult your system administrator before changing this value.

**Font typestyle ID**
Select the default font typestyle to use for printing.

**Forms mode**
Select the way forms are fed into the printer.

<table>
<thead>
<tr>
<th>Select</th>
<th>To feed</th>
</tr>
</thead>
<tbody>
<tr>
<td>*AUTOCUT</td>
<td>Single-cut sheets into the printer automatically.</td>
</tr>
<tr>
<td>*CONT</td>
<td>Continuous forms into the printer automatically.</td>
</tr>
<tr>
<td>*CUT</td>
<td>Single-cut sheets into the printer manually.</td>
</tr>
</tbody>
</table>

**Host Print Transform**

**Host print transform**
Select to specify the manufacturer type and model, the paper sources, and the envelope source on your AS/400 print device.

**Manufacturer type**
Select a printer manufacturer type and model. This must match a manufacturer type and model string defined on the AS/400. If your printer does not appear in the list, ask your system administrator for the string identifying your printer, and type it in.

If you select a printer that begins with *WSCST, you must also specify the Workstation Customizing Object > Name and Library, which the AS/400 will use to print jobs.

**Paper source 1**
Select the primary paper source on the host printer. You can specify a particular paper size or one of the following:

<table>
<thead>
<tr>
<th>Select</th>
<th>To do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>*MFRTYPMODEL</td>
<td>Substitute the value most common for your printer.</td>
</tr>
<tr>
<td>*NONE</td>
<td>No paper source is specified.</td>
</tr>
<tr>
<td>*SAME</td>
<td>Use the currently configured host value.</td>
</tr>
<tr>
<td>Windows Printer</td>
<td>Use the value specified by the default Windows printer.</td>
</tr>
</tbody>
</table>

**Paper source 2**
Select the secondary paper source on the host printer.

**Envelope source**
Select the envelope source on the host printer.

**Name**
Type the name of a workstation customizing (WSCST) object that gives the AS/400 information about the functions supported by your ASCII printer.

**Library**
Select the location of the WSCST object.
Related Topics

- “Configure Printer Session Settings” on page 546
- “Session Setup Dialog Box (5250 Printer Sessions)” on page 536

Printer Session Setup Dialog Box (5250 Printer Sessions)

Index Term
Primary: transparent mode
Secondary: 5250 printer sessions

Index Term
Primary: Printer Session Setup dialog box (5250)

Index Term
Primary: national character set
Secondary: 5250 printer sessions

Index Term
Primary: form feed
Secondary: printing options, 5250

Index Term
Primary: flush
Secondary: printing options, 5250

Index Term
Primary: bypass Windows print driver
Secondary: 5250 printer sessions

Getting there

1. Open a 5250 printer session.
2. From the printer panel, click the Setup button.

The options are:

Character translation

<table>
<thead>
<tr>
<th>National character set</th>
<th>Determines how host characters (EBCDIC) are mapped to PC characters (ANSI). This setting should match the national character set used by your host system.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transparent mode</td>
<td>Select this check box for printer-ready documents that require no page formatting. In <strong>Transparent mode</strong>, all page format settings (Characters per line and Lines per page) are ignored.</td>
</tr>
<tr>
<td>Bypass Windows print driver in transparent mode</td>
<td>Select to disable Windows handling of fonts, font size, font style, and lines-per-inch configuration while in <strong>Transparent</strong> mode.</td>
</tr>
</tbody>
</table>

Flush printing options

<table>
<thead>
<tr>
<th>Flush when End of Job record received</th>
<th>Select if you want an in-progress print job to close if an end-of-job condition is sent from the host.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host print timeout for flushing</td>
<td>Specify the number of seconds to wait after the host stops sending data to a printer session before forcing all pending printer output to the printer.</td>
</tr>
</tbody>
</table>
Form feed options

- **Emulate form feed with line feed**
  Select to have InfoConnect simulate a form feed by issuing line feeds until the end of the page is reached.

- **Send form feed at end of job**
  Select to send a form feed at the conclusion of host print jobs.

- **Font mapping (button)**
  Click to open the Fonts dialog box, from which you can map your local printer fonts to typestyle IDs used by a host.

**Related Topics**
- “Configure Printer Session Settings” on page 546
- “Session Setup Dialog Box (5250 Printer Sessions)” on page 536
- “Font Mapping (5250 Printer Sessions)” on page 545
- “Fonts Dialog Box” on page 546

**Font Mapping (5250 Printer Sessions)**

You can map local printer fonts to typestyle IDs used in AS/400 documents. You can then insert these typestyle IDs into source documents on the AS/400, and assign various font, style, and size configurations to these typestyle IDs.

If you don't map typestyle IDs to fonts, InfoConnect attempts to match the font. However, the output may only approximate what is specified in the documents.

**To map a typestyle ID to a font**

1. Open a 5250 printer session.
2. From the printer panel, click the Setup button.
3. From the Printer Session Setup dialog box, click the Font mapping button.
4. From the Fonts dialog box, type a number in the Typestyle ID text box.
5. Select a font, font size, and font style.
6. Click Map font to ID.

A line similar to the following is added to the Mapped fonts box:

```
151   Courier,   10, Regular
```

In this case, the display shows that text associated with typestyle ID 151 will be printed in 10-point Courier, in a regular style (that is, neither bold nor italic).

**Related Topics**
- “Fonts Dialog Box” on page 546
Fonts Dialog Box

Getting there

1. Open a 5250 printer session.
2. From the printer panel, click the Setup button.
3. From the Printer Session Setup dialog box, click the Font mapping button.

The options are:

- **Typestyle ID**: Select a typestyle ID used in your AS/400 documents to map to a local Windows font.
- **Font**: Select a local Windows font to map to the selected typestyle ID.
- **Size**: Select a size to map to.
- **Font style**: Select a style to map to. The styles available depend on the font selected.
- **Sample**: A sample of the local Windows font is displayed when a font, size, and style have all been specified.
- **Script**: Select a language script to make the character set for that language available. The scripts available depend on the font selected.
- **Mapped fonts**: This list displays all of the fonts you have mapped for the current session.
- **Map font to ID**: With a typestyle ID selected, and a local Windows font, size, and style selected, click this button to map the font to the ID.
- **Clear font mapping**: To delete a mapping, select an item from the Mapped fonts list, and then click this button.

Related Topics

- "Font Mapping (5250 Printer Sessions)" on page 545
- "Printer Session Setup Dialog Box (5250 Printer Sessions)" on page 544

Configure Printer Session Settings

Index Term
Primary: printing
Secondary: configuring printer settings (IBM sessions)

Using InfoConnect printer sessions, you can print host jobs using your Windows printer.

To configure printer session settings

1. Open a printer session.
2 Configure settings using any of the following:

To Configure host-related printing options
   From the printer panel, do this
   From the Connection menu, choose Session Setup.
   The Session Setup dialog box appears.

Configure the way text and images are arranged on the page
   From the File menu, choose Page Setup.

Select a printer or configure printer properties
   From the File menu, choose Print Setup.

View a complete list of current printing settings
   From the Setup menu, choose View Settings.

3 To save the changes to your printer session file, from the printer panel, from the File menu, choose Save.

Printer session files use a *.rsf file extension.

Related Topics

- “Create a 3270 Printer Session” on page 526
- “IBM 3270 Printer Panel” on page 529
- “Create a 5250 Printer Session” on page 535
- “IBM 5250 Printer Panel” on page 538
- “Reset Printer Session to Defaults” on page 554

Enter Host (or System) Name or IP Address Dialog Box

This dialog box appears when you start a session for which no host has been specified. (This is the default configuration for a new printer session).

The options are:

Enter Host (or System) Name or IP Address
   Type the host name or IP address of the terminal to which you want to connect.

Connect
   Click to connect the session immediately.

Cancel
   Click to configure more than just the host name for this session.
   - If you are setting up a printer session, configure the session in the IBM 3270 (or 5250) Printer dialog box.
   - If you are setting up a host session, on the quick access toolbar at the top of the workspace, click . Then, under Host Connection, click Configure Connection Settings.

Related Topics

- “Configure Printer Session Settings” on page 546
- “Create a 3270 Printer Session” on page 526
Choose Template Dialog Box

Index Term
Primary: templates
Secondary: printer sessions

Getting there
1. Open a printer session.
2. From the File menu, click New Session.

The options are:

Current settings
Create a new printer session using the same settings as your current session.

Default 3270 Printer
Create a new 3270 printer session.

Default 5250 Printer
Create a new 5250 printer session.

Related Topics
- “Configure Printer Session Settings” on page 546
- “Create a 3270 Printer Session” on page 526
- “Create a 5250 Printer Session” on page 535

Page Setup Dialog Box

Index Term
Primary: paper settings
Secondary: Page Setup dialog box (IBM)

Index Term
Primary: page setup (printing)
Secondary: Page Setup dialog box (IBM)

Index Term
Primary: orientation, page
Secondary: Page Setup dialog box (IBM)

Index Term
Primary: margins, page
Secondary: Page Setup dialog box (IBM)

Getting there (host screen printing)
1. Open a terminal session.
2. Open the Page Setup dialog box as follows:
The steps depend on your user interface mode (page 120).

- If you are using the Ribbon or Browser mode, click on the Quick Access Toolbar and then click Page Setup.
- If you are using the TouchUx mode, tap the Folder icon and then under Print, select Page Setup.

Getting there (printer emulation)

1. Open a printer session.
2. From the File menu, choose Page Setup.

Configure page layout options for host screen printing and printer emulation sessions.

Paper

- **Size**
  - Select the size of the paper or envelope you want to use.
- **Source**
  - Choose the tray where the paper you want to use is located in the printer. Different printer models support different paper sources.

Orientation

- Choose how the document is positioned on the page. The Page Preview at the top of the dialog box shows an example of the currently selected orientation.

Margins (inches)

- Use the settings in this group box to set the printing area for the page. InfoConnect will not print outside the boundaries you specify. The Page Preview at the top of the dialog box shows an example of the currently selected margins.

  **Override the orientation specified by the host**

  - Select to make sure that your selected orientation is used.

  In terminal sessions, page orientation is not set explicitly by the host but may be implied by the host page size. For example, by default the host page size is defined by the number of columns and lines on the terminal display. If the display is narrower than it is long, portrait orientation is implied. If the display is wider than it is long, landscape orientation is implied.

  In printer sessions, the host may explicitly set a particular orientation in the data stream, or an orientation may be implied by the host page size, as described above for terminal sessions.

  **Page Options**

  - Open the Page Options dialog box, from which you can set the font to use for printed output, and specify the number of rows and columns to appear on the page.

Related Topics

- “Page Options Dialog Box” on page 550
- “Configure Printer Session Settings” on page 546
- “Printing IBM Host Terminal Screens” on page 557
- “Printing from IBM Sessions” on page 525
Page Options Dialog Box

Index Term
Primary: page setup (printing)
Secondary: lines per page

Index Term
Primary: page setup (printing)
Secondary: characters per line

Index Term
Primary: Page Options dialog box (IBM)

Index Term
Primary: fonts
Secondary: configuring printer fonts (IBM sessions)

Getting there

1. Open a terminal session.
2. Open the Page Setup dialog box as follows:
   The steps depend on your user interface mode (page 120).
   - If you are using the Ribbon or Browser mode, click on the Quick Access Toolbar and then click Page Setup.
   - If you are using the TouchUx mode, tap the Folder icon and then under Print, select Page Setup.
3. From the Page Setup dialog box, click the Page Options button.

Configure text layout options for host screen printing and printer emulation sessions.

Text Format

- **Use printer fonts only**
  Select to print using only fonts residing on the host printer.

- **Override host page format**
  When this check box is selected, page formatting specified in the printer session document (Characters per line, Lines per page, Font, and Margins) is used regardless of what the host specifies.

- **Font**
  Select a font to use.
  **NOTE:** When you print all or part of a host screen from a terminal session, the font used is the currently configured display font, not the printer font setting configured here.

- **Page Scaling**
  Click to open the Page Scaling dialog box.

Characters per line

Select the maximum number of characters that can be printed on a single line. If a line longer than this value is sent from the host, the line is automatically wrapped.

These settings are ignored when, from the Printer Session Setup dialog box, Transparent mode is selected.
Lines per page
Select the number of lines to be printed on each page.
These settings are ignored when, from the Printer Session Setup dialog box, Transparent mode is selected.

Related Topics
- “Page Setup Dialog Box” on page 548
- “Configure Printer Session Settings” on page 546
- “Printing IBM Host Terminal Screens” on page 557
- “Printing from IBM Sessions” on page 525

Page Scaling Dialog Box
Index Term
Primary: scaling printed pages

Index Term
Primary: Page Scaling dialog box

Getting there
1 Open a printer session.
2 Open the Page Setup dialog box as follows:
   The steps depend on your user interface mode (page 120).
   - If you are using the Ribbon or Browser mode, click on the Quick Access Toolbar and then click Page Setup.
   - If you are using the TouchUx mode, tap the Folder icon and then under Print, select Page Setup.
3 Select Page Options.
4 From the Page Options dialog box, click the Page Scaling button.
The options are:

**Scaling Options**

- **No scaling**
  When you select **No Scaling**, InfoConnect prints the screen or host print job as it is received from the host.

- **Scale the page size specified by the host to fit on the Windows printer page**
  Automatically reduce or expand the page size specified by the host to fit the page size currently defined in the **Page Setup** dialog box.

- **Choose a host page size and scale it to fit on the Windows printer page**
  When selected, enables the **Host page size** list box.
  
  If you can get better results scaling from a host page size that is different from the one specified by the host, you can select one from the **Host page size** list.

- **Host page size**
  Select the size that best matches the form printout defined on the host.

- **Use scaling factors for reduction or expansion**
  Reduce or enlarge the width and length of the host print job and print it on the page size currently defined in the **Page Setup** dialog box.

---

**NOTE**

- No scaling is performed if either Print to file or Bypass Windows print driver is selected in the **Print Setup** dialog box.

- If the host does not explicitly set a particular page orientation, one may be implied by the host page size. If the host page is narrower than it is tall, portrait orientation is implied. If the host page is wider than it is tall, landscape orientation is implied. To make sure that the Windows printer orientation is used, from the **Page Setup** dialog box, select **Override the orientation specified by the host**.

---

**Related Topics**

- “Page Options Dialog Box” on page 550
- “Page Setup Dialog Box” on page 548
- “Print Setup Dialog Box” on page 552
- “Configure Printer Session Settings” on page 546
- “Printing IBM Host Terminal Screens” on page 557

---

**Print Setup Dialog Box**

Index Term
Primary: printing
Secondary: to file (IBM)

Index Term
Primary: Print Setup dialog box (IBM)

Index Term
Primary: network printer
Secondary: Print Setup dialog box (IBM)
Index Term
Primary: bypass Windows print driver
Secondary: Print Setup dialog box (IBM)

Getting there (host screen printing)
1 Open a terminal session.
2 Open the Print dialog box as follows:
   - If you are using The Ribbon or Browser mode, click on the Quick Access Toolbar and then click Setup.
   - If you are using the TouchUx mode, tap the Folder icon and then under Print, select Print and then click Setup.

Getting there (printer emulation)
1 Open a printer session.
2 From the File menu, choose Print Setup.

The options are:

**Printer**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Select a printer from this list of printers currently connected to your computer.</td>
</tr>
<tr>
<td>Properties</td>
<td>Click to set printer-specific options.</td>
</tr>
<tr>
<td>Status, Type, Where, Comment</td>
<td>These read-only fields describe the selected printer.</td>
</tr>
</tbody>
</table>

**Print to file**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Print to file</td>
<td>Select to send output to a file instead of a printer.</td>
</tr>
<tr>
<td>Print output to</td>
<td>Type the path and filename for the output file.</td>
</tr>
<tr>
<td>If file exists</td>
<td>Select what to do when the output file already exists in the target location.</td>
</tr>
<tr>
<td>Bypass Windows print driver</td>
<td>Select to send raw data (including printer control escape codes) directly to your printer. Output is sent to the printer immediately, instead of waiting for a whole page of information, and the Windows printing interface is bypassed.</td>
</tr>
</tbody>
</table>

If you're bypassing Windows printing to a PostScript printer, the results may not be what you expect. PostScript printers are controlled by PostScript commands, which are typically sent to the printer from a PostScript printer driver.

Network
Click to connect to a shared network printer.
Multiple screens per page

**Auto formfeed**
Select to add a form feed between each screen print.

**Close printer manually**
Select to send multiple screen prints to a spool file and then print them all at once. (The spool file is sent to the printer when you click the Close Printer button on the status bar.)

Related Topics

- “Configure Printer Session Settings” on page 546
- “Printing IBM Host Terminal Screens” on page 557
- “Page Setup Dialog Box” on page 548
- “Print More Than One Screen per Page” on page 52

Printing to a Form or Label

Index Term
Primary: printing
Secondary: forms or labels

Index Term
Primary: page setup (printing)
Secondary: print to form or label

Index Term
Primary: labels
Secondary: printing to

Index Term
Primary: forms
Secondary: printing to

For information about configuring InfoConnect to print to a form or label, refer to Technical Note 2179 (http://www.support.attachmate.com/techdocs/2179.html).

This technical note details techniques that can be used to configure a print job to fit onto a pre-printed form, such as an invoice or tax document, where the output must align with specifically located fields.

Related Topics

- “Configure Printer Session Settings” on page 546

Reset Printer Session to Defaults

Index Term
Primary: restore default
Secondary: printer session settings

You can create a new session using the templates provided, or use the following procedure to return the settings of your current procedure to the defaults.

To reset default printer values for the current session

- From the Setup menu, select Defaults.
NOTE

- The **Defaults** command is not available when you are connected to a host.
- This action has no effect on saved settings files.

Related Topics

- “Choose Template Dialog Box” on page 548
- “Create a 3270 Printer Session” on page 526
- “Create a 5250 Printer Session” on page 535
- “Configure Printer Session Settings” on page 546

Run a Trace (Printer Sessions)

If you are troubleshooting problems with a printer session, technical support may request that you obtain one or more traces.

**To create a trace file for a printer session**

1. Open a printer session.
   
   If you are connected to the host, disconnect (**Connection > Disconnect**).
2. From the **Connection** menu, chose **Trace > Start Trace**.
3. Select the trace file type.
4 Specify a name for the trace file.

**NOTE:** If you have spoken with a support technician, use your call ID number as the name of your trace file.

5 Click Trace.

A bug symbol appears in the status bar, indicating that the trace is active.

6 Connect to the host.

7 Perform the actions that reproduce the problem you want recorded in the trace.

8 To end the trace, go to Connection > Trace > Stop Trace.

Upload the trace file as a binary file to http://upload.attachmate.com (http://upload.attachmate.com). If the problem relates to a service request you are currently working on with a technician, include the Attachmate service request number with the trace and let the technician know when the file is uploaded.

**Related Topics**

- “Configure Printer Session Settings” on page 546

**Save Changes on Exit (Printer Sessions)**

**Index Term**

Primary: Save Changes on Exit (printer sessions)

By default, you see the Save Changes on Exit dialog box if you have made any changes to settings in the current session.

**NOTE:** To change the default behavior, edit the Save Changes on Exit setting in the View Settings dialog box.
The options are:

**View Changes** Displays the View Settings dialog box, which shows settings which have been changed from the defaults.

**Save** Exits and saves the changes.

**Discard** Exits without saving the changes.

**Cancel** Cancels the exit command and returns you to the session without saving the changes.

Related Topics

- “View Settings Dialog Box (Printer Sessions)” on page 576

# Printing IBM Host Terminal Screens

In this Section

- “Print a Terminal Screen” on page 557
- “Print Dialog Box (Terminal Screen Printing)” on page 558

## Print a Terminal Screen

Index Term
- Primary: printing
- Secondary: terminal screen

Index Term
- Primary: printing
- Secondary: host screen

You can print the contents of the current terminal screen display.

### To print a terminal screen using default print settings

1. Open a terminal session.
2. Navigate to the screen you want to print.
3. Open the Print dialog box.
   
   The steps depend on your user interface mode (page 120):
   
   - If you are using the Ribbon or Browser mode, click on the Quick Access Toolbar.
   - If you are using the TouchUx mode, tap the Folder icon and then under Print, select Print.
4. In the Print dialog box, click OK.

### To modify the screen print settings

1. Open a terminal session.
2. Navigate to the screen you want to print.
3 Open the Print dialog box. The steps depend on your user interface mode (page 120).

- If you are using the Ribbon or Browser mode, click on the Quick Access Toolbar.
- If you are using the TouchUx mode, tap the Folder icon and then under Print, select Print.

4 From the Print dialog box, modify the desired settings.

5 Click OK.

Related Topics

- “Integrate Host Data with Office Tools” on page 192
- “Print Dialog Box (Terminal Screen Printing)” on page 558

Print Dialog Box (Terminal Screen Printing)

Index Term
Primary: Print dialog box (IBM)

Getting there

1 Open a terminal session.
2 Open the Print dialog box as follows:

- If you are using Ribbon or Browser mode, click on the Quick Access Toolbar.
- If you are using TouchUx mode, tap the Folder icon and then under Print, select Print.

Options

- **Copies**: Select the number of copies you want to print.
- **Fast text-only printing**: Print using the current printer font, rather than the display font, and use white for the background.
- **Print status line**: Select to print the host status line in addition to the terminal screen.
- **Monochrome**: Select to print the screen using black and white only. To print the display in color or to print it using grayscale on a non-color printer, clear this check box.
- **Square aspect ratio**: (3270 sessions only) Select to use the pixel dimensions of the 3179-G terminal, and ensure that objects maintain their correct proportions and shapes.
- **Background**: Select a background color.

Print Range

- **All**: Print the complete contents of the terminal window, including the host status line.
- **Selection**: Print the currently highlighted selection.
- **Partition**: (3270 sessions only) Print the current screen partition (which usually corresponds to the entire terminal window, but without the Operator Information Area).
InfoConnect 2014 provides full access to the printing capabilities of your Windows printer, like any Windows application. From a VT session, you can print the screen, the display memory, or just the selected text. In addition, InfoConnect provides a terminal emulation feature called logging, which is similar to printing.

**Setup**
Click to control printer settings that apply only to InfoConnect, or to select a different Windows printer.

**Print what**
(3270 graphics sessions only) Select the part of the terminal display to print: graphics, text, or both.

**Document title**
(Available only when Fast text-only printing is selected.)
Enter the document title. (This text will be inserted where &F appears in the document header or footer text.)

**Header text**
(Available only when Fast text-only printing is selected.)
Enter text or any of the following special characters in the header.

- &D inserts the current date in the format month-day-year (for English) or in an appropriate format for the current locale.
- &T inserts the current time in International format (for example, 14:29:22.86).
- &F inserts the document title or, if no title is specified, the session document name.
- &P inserts the page number.
- &U inserts the configured AS/400 sign-on user ID. If there is no AS/400 sign-on user ID, the current Windows user ID is inserted.
- &H inserts the configured host name.
- &N inserts a new line.
- && inserts an ampersand ('&').

**Footer text**
(Available only when Fast text-only printing is selected.)
Enter text or special characters in the footer. The special characters allowed for the header can also be used for the footer.

**Related Topics**

- “Print a Terminal Screen” on page 557
- “Print Setup Dialog Box” on page 552

**Printing from VT Sessions**

Index Term
Primary: VT
Secondary: printing

Index Term
Primary: printing
Secondary: from VT sessions
The Difference Between Printing and Logging

It's important to understand the difference between printing output and logging output. When logging is turned on, lines are buffered immediately as they appear on the screen. This continues until you turn logging off, when the output is actually printed. This type of "printing" parallels terminal-host printing, and, typically, the host controls printing, bypassing InfoConnect.

The Windows printer driver is still used, unless you select **Bypass Windows print driver** from the **Print Setup** dialog box.

In this Section

- “Print from a VT Session” on page 560
- “Printing Batch Print Jobs” on page 561
- “Prevent Character Translation” on page 562
- “Logging Data” on page 562
- “Configure Printing Options” on page 570

Print from a VT Session

Index Term
Primary: display memory (VT)
Secondary: print

You can print using defaults, or you can choose a print range and number of copies first.

To print using default settings

1. Open a terminal session.
2. Navigate to the screen you want to print.
3. Open the Print dialog box.
   - The steps depend on your **user interface mode** (page 120):
     - If you are using the Ribbon or Browser mode, click \[print\] on the Quick Access Toolbar.
     - If you are using the TouchUx mode, tap the Folder icon and then under **Print**, select **Print**.
4. In the Print dialog box, click **OK**.

To print using custom settings

1. Open a terminal session.
2. Navigate to the screen you want to print.
3. Open the Print dialog box.
   - The steps depend on your **user interface mode** (page 120):
     - If you are using the Ribbon or Browser mode, click \[print\] on the Quick Access Toolbar.
     - If you are using the TouchUx mode, tap the Folder icon and then under **Print**, select **Print**.
   - The Print dialog box opens.
4. Select a Print range option:
To print multiple copies of the selected range, choose a value from the **Copies** box.

6 Click **OK**.

**Related Topics**

- “Printing from VT Sessions” on page 559
- “Print Dialog Box” on page 571
- “Printing Batch Print Jobs” on page 561

## Printing Batch Print Jobs

**Index Term**

**Primary:** batch print jobs (VT)

You can configure **InfoConnect** to accumulate output from a series of print events before you print. You might want to do this, for example, if you're connected to a network printer that is temporarily inoperative—you can collect all your printed output and print it all at once when the printer is again available.

To print a batch of print jobs

1 **Open the Print dialog box.**

   The steps depend on your **user interface mode** (page 120):

   - If you are using the Ribbon or Browser mode, click on the Quick Access Toolbar.
   - If you are using the TouchUx mode, tap the Folder icon and then under **Print**, select **Print**.

2 In the Print Dialog box, click **Setup**.

3 Under **Multiple screens per page**, select **Close printer manually**.

   When you print with this option selected, the print output is spooled until you click **Close Printer** on the Status bar.

4 Clear the **Auto formfeed** box.

   This prevents **InfoConnect** from ejecting the page after each print event — if you're printing to a printer this saves paper; if you're printing to a file, this prevents a page break from being inserted in the output file.

   Clearing this setting can also be useful if your host program sends a series of open printer and close printer escape sequences.

**Related Topics**

- “Print from a VT Session” on page 560
- “Print Setup Dialog Box” on page 571

<table>
<thead>
<tr>
<th>Select</th>
<th>To print</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display memory</td>
<td>The information visible on the display, as well as any information that has scrolled off of the display and is still in memory.</td>
</tr>
<tr>
<td>Screen</td>
<td>Whatever you see in the terminal window.</td>
</tr>
<tr>
<td>Selection</td>
<td>Any selection that is highlighted in the terminal window.</td>
</tr>
</tbody>
</table>
Prevent Character Translation

Character translation is the conversion of one character set to another. You should disable character translation if the host already generates characters in the correct character set for your printer, and your printer is not configured for the default IBM PC code page 437 character set.

The **Disable printer translation** option has little, if any, effect on screen printing or logging. When InfoConnect receives characters from the host, it automatically converts these characters to the ANSI character set before displaying them in Windows. The translation has already taken place before you either turn on logging or print the screen contents. Therefore, this setting is only relevant for host applications that print in controller mode. In this mode, InfoConnect does not know in advance what the host will be sending and does not perform automatic translation.

**To prevent character translation**

1. Open the Print dialog box.
   - The steps depend on your **user interface mode** (page 120).
     - If you are using the Ribbon or Browser mode, click on the Quick Access Toolbar.
     - If you are using the TouchUx mode, tap the Folder icon and then under **Print**, select **Print**.
2. In the Print dialog box, click **Setup**.
3. Select **Bypass Windows print driver**.
4. Select **Disable printer translation**.
   - Characters will be printed exactly the way they arrive from the host.

**Related Topics**

- "Print Setup Dialog Box" on page 571

Logging Data

Logging copies data from display memory to the printer each time a line feed is received so that attributes, such as underline, are printed. For VT terminals, "Controller mode" captures incoming data to the printer. Typically, logging is enabled by the host. However, if you want to configure a user-initiated logging session, you can do this from the **Logging** group on the **Tools** Ribbon.

Logging serves two functions in InfoConnect:

- It accommodates host printing, where an application turns on logging and starts sending data to a printer, a file, or both.
- It provides user-initiated logging of terminal sessions.
You can log to a printer, a file, or a serial device. After logging is started, all printed output is directed to the option selected under **Log output to**. Output is not written to disk or sent to the printer until you (or the host) stop logging.

**Host-Initiated Printing**

Many VT host applications can print to printers that are not attached to the host. This type of host-initiated printing is referred to as slave printing, logging, pass through printing, auto-print, or controller printing.

Typically, host-initiated printing involves selecting the **Print** command from a host menu. To send a print job, the host transmits escape sequences to the terminal or terminal emulator, which signal that the print job should be forwarded to a printer. **InfoConnect** supports host-initiated printing and forwards the print job to the Windows default printer.

To change where the print job is sent, use the **Logging** dialog box to select a different output option.

---

**NOTE:** The **Serial device** option is not used for typical printing, even if you have your Windows printer on the serial port. This option is only used for devices on serial ports, such as bar-code readers, which need to send information back and forth between the host and the device, through **InfoConnect**.

---

**Serial Device-to-Host Communications**

**InfoConnect** supports serial device-to-host communications (also called printer-to-host, bidirectional, or printer 2-way communications). You can enable serial device-to-host communications when you want a device on a serial port (such as a printer or bar-code reader) to be able to send information to a host via **InfoConnect**.

**In this Section**

- “Log Data from a VT Session” on page 563
- “Logging When InfoConnect is in Protect Mode” on page 564
- “Enabling Serial Device-to-host Communications” on page 565
- “Logging Dialog Box” on page 567
- “Configure Serial Device Port Dialog Box” on page 568

---

**Log Data from a VT Session**

Output is not written to disk or sent to the printer until you (or the host) stop logging.

**To configure logging**

1. Open the Logging Settings dialog box.
   1a. Open a VT terminal session;
   1b. Open the Logging Settings dialog box as follows:
The steps depend on your user interface mode (page 120).

### User interface Mode

<table>
<thead>
<tr>
<th>Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ribbon</strong></td>
<td>From the Tools ribbon, in the Logging group, click the Logging &gt; Settings launcher:</td>
</tr>
<tr>
<td><strong>Reflection Browser</strong></td>
<td>In the search box, enter L and then, under Actions, select Logging.</td>
</tr>
<tr>
<td><strong>TouchUx</strong></td>
<td>Tap the Wrench icon and then, under Logging, select Logging.</td>
</tr>
</tbody>
</table>

2 Under **Log output to**, select an output option.

- To select and configure a printer, click **Print Setup**.
- or-
  - To log to a file, select **Disk**, and then type the path and filename for the output file.

3 Click **OK**.

### To start logging

1 Open a VT terminal session.
2 Start logging as follows:
   - The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ribbon</strong></td>
<td>From the Tools tab, in the Logging group, click Start Logging.</td>
</tr>
<tr>
<td><strong>InfoConnect Browser</strong></td>
<td>In the search box, enter L and under Actions, select Start &gt; Logging.</td>
</tr>
<tr>
<td><strong>TouchUx</strong></td>
<td>On the menu, tap the Wrench icon and then, under Logging, select Start &gt; Logging.</td>
</tr>
</tbody>
</table>

### Logging When InfoConnect is in Protect Mode

**Index Term**
- Primary: block mode
- Secondary: logging when emulating

InfoConnect logs data differently when it is emulating a block mode application, such as a WYSE terminal.

Under WYSE 50+ or WYSE 60 emulation, InfoConnect logs the data up to the cursor the moment it receives a line feed from the host. Whether the terminal is in protect mode or unprotect mode, logging in InfoConnect performs the same way.

**Related Topics**

- “Logging Data” on page 562
Enabling Serial Device-to-host Communications

When you want a bidirectional device on a serial port (such as a printer or bar-code reader) to be able to send information via InfoConnect, you can enable serial device-to-host communications. Most hosts automatically initiate serial device-to-host communications (via the Csi?9i control function). If you are using a host application that does not, you may also need to manually enable serial device-to-host communications.

In this Section

- “Automatically Enable Serial Device-to-host Communications” on page 565
- “Manually Enable Serial Device-to-host Communications” on page 566

Automatically Enable Serial Device-to-host Communications

You can enable serial device-to-host communications when you want a bidirectional device on a serial port (such as a printer or bar-code reader) to be able to send information to a host via InfoConnect. Most hosts automatically initiate serial device-to-host communications (via the Csi?9i control function).

To enable serial device-to-host communications automatically

1 Open the Logging Settings dialog box.
   1a Open a VT terminal session.
   1b Open the Logging Settings dialog box as follows:
The steps depend on your user interface mode (page 120).

**User interface Mode**

- **Ribbon**
  - From the Tools ribbon, in the Logging group, click the Logging > Settings launcher: 

- **Reflection Browser**
  - In the search box, enter L and then, under Actions, select Logging.

- **TouchUx**
  - Tap the Wrench icon and then, under Logging, select Logging.

2 Under **Log output to**, select **Serial device**, and then click **Configure**. The **Configure Serial Device Port** dialog box appears.

3 From the **Port** list, select the port to which your serial device is connected. If necessary, change the other settings for the serial connection to your device.

   The **Configure** button from the Terminal Setup Advanced Options dialog box is equivalent to the **Configure** button from the **Logging Settings** dialog box. You can use the button from either dialog box to configure your serial device port.

4 Click **OK**.

5 If the host application needs to send data to the serial device, from the **Logging** dialog box, clear the **Printer** check box. (You can omit this step if data flows only from the serial device to the host.)

6 Click **OK**.

**Related Topics**

- “Manually Enable Serial Device-to-host Communications” on page 566
- “Configure Serial Device Port Dialog Box” on page 568
- “Logging Dialog Box” on page 567
- “Logging Data” on page 562

**Manually Enable Serial Device-to-host Communications**

Although most hosts automatically initiate serial device-to-host communications (via the Csi?9i control function), if you are using a host application that does not, you may also need to manually enable serial device-to-host communications.

**To enable serial device-to-host communications manually**

1 Open a VT terminal session.

2 **Open the Document Settings dialog box.** The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ribbon or Reflection Browser</strong></td>
<td>With a session open in Reflection, from the Quick Access Toolbar, click</td>
</tr>
<tr>
<td><strong>TouchUx</strong></td>
<td>Tap the Gear icon and then select Document Settings.</td>
</tr>
</tbody>
</table>
3 Under **Terminal Configuration**, click **Select Terminal Type**.

4 Under **Terminal Settings**, click **Terminal Setup**.

5 Click the **Advanced** button.

6 Select the **Serial device to host** check box.

   The **Configure** button from the **Terminal Setup Advanced Options** dialog box is equivalent to the **Configure** button from the **Logging Settings** dialog box. You can use the button from either dialog box to configure your serial device port.

7 Click **OK**.

**Related Topics**

- “Automatically Enable Serial Device-to-host Communications” on page 565
- “Configure Serial Device Port Dialog Box” on page 568
- “Logging Dialog Box” on page 567
- “Logging Data” on page 562

**Logging Dialog Box**

**Getting there**

1 Open a VT terminal session.

2 Open the Logging Settings dialog box as follows:
   - The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ribbon</td>
<td>From the <strong>Tools</strong> ribbon, in the <strong>Logging</strong> group, click the <strong>Logging &gt; Settings</strong> launcher: <img src="image" alt="Launcher" /></td>
</tr>
<tr>
<td><strong>InfoConnect</strong> Browser</td>
<td>In the search box, enter !L and then, under <strong>Actions</strong>, select <img src="image" alt="Logging" /></td>
</tr>
<tr>
<td><strong>TouchUx</strong></td>
<td>Tap the Wrench icon and then, under <strong>Logging</strong>, select <strong>Logging</strong>.</td>
</tr>
</tbody>
</table>

Use this dialog box to configure logging and to enable serial device-to-host communications.

The options are:

**Log Output To**

| **Printer** | Select to print the output. The printer selected in **Print Setup** is displayed. |
| **Print Setup** | Click to control printer settings that apply only to **InfoConnect**, or to select a different Windows printer. |
| **Disk** | Select to send output to a file. Type the path and filename for the output file. Create an ASCII text file, and translate line-drawing characters to their closest ANSI equivalent. |
Serial device

Select to send output to the bidirectional serial device connected to the configured serial port. For more information, see the topic Automatically Enabling Serial Device-to-Host Communications (page 565).

NOTE: The Serial device option is not used for typical printing, even if you have your Windows printer on the serial port. This option is only used for devices on serial ports, such as bar-code readers, which need to send information back and forth between the host and the device, through InfoConnect.

Configure

Click to select and configure a serial port.

The Configure button from the Terminal Setup Advanced Options dialog box is equivalent to the Configure button from the Logging Settings dialog box. You can use the button from either dialog box to configure your serial device port.

Related Topics

- “Logging Data” on page 562
- “Automatically Enable Serial Device-to-host Communications” on page 565
- “Configure Serial Device Port Dialog Box” on page 568

Configure Serial Device Port Dialog Box

Index Term
Primary: serial port
Secondary: configuring

Getting there

The Configure button from the Terminal Setup Advanced Options dialog box is equivalent to the Configure button from the Logging Settings dialog box. You can use the button from either dialog box to configure your serial device port.

From the Logging dialog box

1. Open a VT terminal session.
2. Open the Logging Settings dialog box as follows:
   The steps depend on your user interface mode (page 120).

   User interface Mode | Steps
   ---------------------|--------------------------------------------------
   Ribbon               | From the Tools ribbon, in the Logging group, click the Logging > Settings launcher:
   InfoConnect Browser | In the search box, enter L and then, under Actions, select Logging.
   TouchUx              | Tap the Wrench icon and then, under Logging, select Logging.
3. Under Log output to, click the Configure button.
From the Terminal Setup dialog box

1 Open a VT terminal session.
   The steps depend on your user interface mode (page 120).

   User Interface Mode                     Steps
   Ribbon or InfoConnect Browser           With a session open in InfoConnect, from the Quick
   TouchUx                                 Access Toolbar, click .

2 Under Terminal Configuration, click Select Terminal Type.
3 Under Terminal Settings, click Terminal Setup.
4 Click the Advanced button.
5 Next to the Serial device to host check box, click the Configure button.

The options are:

Port                                          Select the communications port to which your target serial device is connected.

Baud rate                                      Set the rate at which InfoConnect transmits and receives data through the selected serial port.
                                                   The baud rate setting must match the baud rate of your direct connection.

Parity                                         Set the parity for data transmission to and from the serial device on this port.
                                                   This setting determines whether a parity bit is generated for each character transmitted. Parity is used to detect errors in data transmission; the number preceding the slash indicates the number of data bits sent.
                                                   To use the multinational character set or 8-bit controls, Parity must be set to one of the values that offers 8-bit controls. If your communications link generates parity, and you set Parity to 8/None, multinational characters appear on your screen. In this case, set Parity to either 8/Even or 8/Odd.

Pacing                                        It is possible for InfoConnect to transmit data to a serial device faster than the device can process it, or for a serial device to transmit data to InfoConnect faster than InfoConnect can process it.
                                                   Should this continue for too long, the slower system's buffer overflows and data is lost. If the serial device recognizes the XON/XOFF handshake, you can prevent the buffer from overflowing by keeping this value set to Xon/Xoff.
Xon/Xoff transmit pacing works as follows:

- When the receive buffer has a limited amount of space left, an XOFF (DC3) character is sent as a signal to stop transmitting.
- After processing most of the backlog of characters in the receive buffer, an XON (DC1) character is sent as a signal to resume transmission.

The two systems continue in this stop-and-go fashion until all the data has been transmitted.

If Hardware is selected, the RTS and CTS pins on the RS-232 serial cable control data flow.

<table>
<thead>
<tr>
<th>Transmit</th>
<th>Select a flow control method to use when InfoConnect transmits data to a serial device on this port.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receive</td>
<td>Select a flow control method to use when the serial device on this port transmits data to InfoConnect.</td>
</tr>
</tbody>
</table>

**Related Topics**

- “Automatically Enable Serial Device-to-host Communications” on page 565
- “Logging Data” on page 562
- “Advanced Options Dialog Box for VT Terminal Types” on page 287

**Configure Printing Options**

Any configuration you perform is saved with your session document.

**To configure printing options**

1. Open a terminal session.

2. **Open the Print dialog box.**

   The steps depend on your user interface mode (page 120).
   - If you are using the Ribbon or Browser mode, click on the Quick Access Toolbar.
   - If you are using the TouchUx mode, tap the Folder icon and then under Print, select Print.

3. In the Print dialog box click **Setup**.

4. From the **Print Setup** dialog box, choose the settings you want, and then click **OK**.

   The settings you choose apply only to InfoConnect.

5. **Open the Page Setup dialog box.**

   Open the Page Setup dialog box as follows:
   The steps depend on your user interface mode (page 120).
   - If you are using the Ribbon or Browser mode, click on the Quick Access Toolbar and then click **Page Setup**.
   - If you are using the TouchUx mode, tap the Folder icon and then under Print, select **Page Setup**.

6. From the **Page Setup** dialog box, choose the settings you want for the paper size and source, the page orientation, and the margins.

7. (Optional) Click the **Page Options** button, and then from the **Page Options** dialog box, set the font to use for printed output, specify the number of rows and columns to appear on the page, and then click **OK**.
From the Page Setup dialog box, click OK.

Related Topics
- “Print Setup Dialog Box” on page 571
- “Page Setup Dialog Box” on page 574
- “Page Options Dialog Box” on page 575

Print Dialog Box

Getting there
1. Open a terminal session.
2. Open the Print dialog box as follows:
   - If you are using Ribbon or Browser mode, click [print] on the Quick Access Toolbar.
   - If you are using TouchUx mode, tap the Folder icon and then under Print, select Print.

The printer selected in Print Setup is shown on this dialog box.

Print range

Display memory
Display memory contains both the information visible on the display and information that has scrolled off of the display.

Screen
Print only what you see on the screen.

Selection
Print the currently highlighted selection.

Copies
Select the number of copies you want to print.

Print Setup
Click to control printer settings that apply only to InfoConnect, or to select a different Windows printer.

Related Topics
- “Print Setup Dialog Box” on page 571
- “Print from a VT Session” on page 560

Print Setup Dialog Box

Index Term
Primary: printing
Secondary: to file (VT)

Index Term
Primary: printing
Secondary: close printer
Getting there

1. Open a terminal session.
2. Open the Print dialog box as follows:
   - If you are using The Ribbon or Browser mode, click on the Quick Access Toolbar and then click Setup.
   - If you are using the TouchUx mode, tap the Folder icon and then under Print, select Print and then click Setup.

Any configuration you perform is saved with your session document.

Printer

Name
Select a printer from this list of printers currently connected to your computer.

Properties
Click to set printer-specific options.

Status, Type, Where,
Comment
These read-only fields describe the selected printer.

Print to file
Create an ASCII text file, and translate line-drawing characters to their closest ANSI equivalent.

Print output to
Type the path and filename for the output file.

Unless you change the path or filename, output continues to be appended to this file each time you perform a print function.
Bypass Windows print driver
Select to send raw data (including printer control escape codes) directly to your printer. Output is sent to the printer immediately, instead of waiting for a whole page of information, and the Windows printing interface is bypassed.

If you’re bypassing Windows printing to a PostScript printer, the results may not be what you expect. PostScript printers are controlled by PostScript commands, which are typically sent to the printer from a PostScript printer driver.

You cannot bypass the Windows print driver when you are printing to a file.

Disable printer translation
If you are bypassing the Windows print driver, you can also disable printer translation. Characters will be printed exactly the way they arrive from the host.

You should disable character translation if the host already generates characters in the correct character set for your printer, and your printer is not configured for the default IBM PC code page 437 character set.

The Disable printer translation option has little, if any, effect on screen printing or logging. When InfoConnect receives characters from the host, it automatically converts these characters to the ANSI character set before displaying them in Windows. The translation has already taken place before you either turn on logging or print the screen contents. Therefore, this setting is only relevant for host applications that print in controller mode. In this mode, InfoConnect does not know in advance what the host will be sending and does not perform automatic translation.

Print ANSI color background
By default, the ANSI background is not printed; a potential savings on printer toner because the ANSI background is often black. To reverse this, select the Print ANSI color background option.

This feature is available only when printing to a printer using a Windows print driver.

Digital LA210 emulation
The LA210 is a type of Digital printer that supports a series of escape sequences for setting the number of columns and rows per page. InfoConnect intercepts the escape sequences and changes the font to emulate the number of columns or rows. This option controls whether InfoConnect translates data when a pass-through method of printing, such as printer controller mode, is being used. If your host software understands PC printers, select this option.

This feature is available only when printing to a printer using a Windows print driver.

Auto formfeed
By selecting this option, an FF character is generated after a print event. Clear this option and the Bypass Windows print driver option if you do not want InfoConnect to eject the page after printing. For example, you may not want a form feed generated when you print multiple selections (using the Selection option under Print > Range in the Print dialog box).

Clearing this setting can also be useful if your host program sends a series of open printer and close printer escape sequences.

Network
Click to connect to a shared network printer.
Close printer

**Manually**  
Select to keep the printer open until you close it manually by clicking the **Close Printer** button; otherwise, the printer closes when the print job is finished.

**After X seconds**  
Select to close the printer automatically after the amount of time you specify. The value you enter here determines how long **InfoConnect** waits after a host print job is completed before automatically closing the printer.

Related Topics

- “Configure Printing Options” on page 570
- “Print Dialog Box” on page 571

Page Setup Dialog Box

Index Term  
Primary: paper settings  
Secondary: Page Setup dialog box (VT)

Index Term  
Primary: page setup (printing)  
Secondary: Page Setup dialog box (VT)

Index Term  
Primary: orientation, page  
Secondary: Page Setup dialog box (VT)

Index Term  
Primary: margins, page  
Secondary: Page Setup dialog box (VT)

Getting there

1. Open a terminal session.
2. Open the Page Setup dialog box as follows:  
   The steps depend on your user interface mode (page 120).  
   - If you are using the Ribbon or Browser mode, click on the Quick Access Toolbar and then click **Page Setup**.
   - If you are using the TouchUx mode, tap the Folder icon and then under **Print**, select **Page Setup**.

   The options are:

   **Paper**

   **Size**  
   Select the size of the paper or envelope you want to use.

   **Source**  
   Choose the tray where the paper you want to use is located in the printer. Different printer models support different paper sources.
Orientation
Choose how the document is positioned on the page. The Page Preview at the top of the dialog box shows an example of the currently selected orientation.

Margins (inches)
Use the settings in this group box to set the printing area for the page. InfoConnect will not print outside the boundaries you specify. The Page Preview at the top of the dialog box shows an example of the currently selected margins.

Page Options
Open the Page Options dialog box, from which you can set the font to use for printed output, and specify the number of rows and columns to appear on the page.

Related Topics
- “Configure Printing Options” on page 570
- “Page Options Dialog Box” on page 575

Page Options Dialog Box

Getting there

1. Open a terminal session.
2. Open the Page Setup dialog box as follows:
The steps depend on your user interface mode (page 120).
   - If you are using the Ribbon or Browser mode, click on the Quick Access Toolbar and then click Page Setup.
   - If you are using the TouchUx mode, tap the Folder icon and then under Print, select Page Setup.
3. From the Page Setup dialog box, click the Page Options button.

Text format

Font
The default font is a TrueType font called r_ansi, installed by InfoConnect. To change the printer font, select a new name from the Font box. Only those fonts supported by your printer are listed.

NOTE: You can print only using monospace TrueType fonts (also known as fixed pitched).

Use printer default font
Select to speed up printing by using your printer’s built-in font.
Print inverse video
Select to print inverse screen text as inverse text; otherwise, inverse screen text is printed as normal text.

**NOTE**

- Your print driver must support inverse-mode printing for this feature to work.
- This option is not available when **Use printer default font** is selected.

Fit font to page
When cleared, InfoConnect considers limiting factors of height or width when determining font size. Printed fonts are always correctly proportioned. However, the text may not fill the printed page.

When selected, InfoConnect adjusts the height and width of the font based on the page size and the number of rows and columns on the page, so that text always fills the printed page.

**NOTE**

- These adjustments may give the font a distorted appearance. To print the optimal amount of text per page, select the **Auto row sizing** check box.
- This option is not available when **Use printer default font** is selected.

Column dimensions

Columns per row
Changing the number of columns is useful for printing wide reports.

**NOTE:** Changing the setting for **Number of characters per row** (from Document Settings > Set up Display Settings > Dimensions) automatically changes the printer columns.

Row dimensions

Rows per page
If the value you select here exceeds what your printer can fit on one page (this number varies from printer to printer), InfoConnect prints the maximum number of lines it can fit on the page.

Auto row sizing
Select to print the optimal number of rows that can fit onto a page, given the values you specified in the **Page Setup** and **Page Options** dialog boxes. If you change those values after selecting this option, InfoConnect automatically calculates a new optimal number of rows to be printed per page.

Related Topics

- “Configure Printing Options” on page 570
- “Page Setup Dialog Box” on page 574

View Settings Dialog Box (Printer Sessions)

Index Term
Primary: View Settings dialog box (printer sessions)
Index Term
Primary: settings (InfoConnect)
Secondary: printer session

Index Term
Primary: printing
Secondary: printer session settings

Index Term
Primary: printer session settings

Getting there

1. Open a printer session.
2. From the Setup menu, choose View Settings.

The View Settings dialog box lists all your current printer session settings. This list includes all settings you can configure using any printer session dialog box, and some additional settings that can only be set from the View Settings dialog box.

You can use the View Settings dialog box to check the current value of a setting, change its value, find out what values can be used, or view help for a setting. You can also find out which settings have been changed from their default values.

When you change a setting in the View Settings dialog box, the corresponding setting in a the printer session dialog box (if there is one) changes also. For example, if you change the value of Auto Connect from No to Yes, the Auto connect check box in the Session Setup dialog box is selected.

The options are:

Search
Enter text to quickly locate settings whose name includes that text.

Reflection settings
Lists printer settings. You can filter this list using the Search and Display settings options.

Display settings
Filters the list so you can view only settings that have been changed from their default values.

Setting details
Shows the value of the currently selected setting.

Help
Displays this help topic.

Setting help
Displays information about the currently selected setting.

Related Topics

• “Printer Emulation Settings” on page 577

Printer Emulation Settings

This list contains the printer settings available in the View Settings (page 576) dialog box.

In this Section

• “AS/400 Host Name” on page 581
• “Assigned AS/400 Host” on page 582
• “Assigned Device Name” on page 582
• “Assigned Encryption Strength” on page 582
• “Assigned Host Name” on page 582
• “Assigned LU Name” on page 583
• “Auto Connect” on page 583
• “Auto Reconnect” on page 583
• “Bypass Windows Printing” on page 583
• “Bypass Windows Printing in Transparent Mode” on page 584
• “C/370 Character Set” on page 584
• “Caption” on page 584
• “Command Line Switches” on page 585
• “Confirm on Exit” on page 585
• “Country Extended Graphics Code” on page 585
• “Create Settings File Shortcut” on page 586
• “Current Display Height” on page 586
• “Current Display Width” on page 586
• “Current Locale” on page 586
• “Current Trace Record” on page 586
• “Default Printer Copies” on page 587
• “Device Name” on page 587
• “Enable Asynchronous Transport Behavior” on page 587
• “Enable Host Alarm” on page 587
• “Font Character Set” on page 587
• “Fully Qualified Remote LU Name” on page 588
• “Generate Device Names” on page 588
• “Host Communication Timeout” on page 589
• “Host Name” on page 590
• “Host Network Address” on page 590
• “Host Print Timeout” on page 590
• “Hosts File Name” on page 590
• “Icon Title” on page 591
• “Language Override” on page 591
• “Locale” on page 592
• “Manufacturer Type” on page 592
• “Maximum Internal Trace File Length (MB)” on page 592
• “Menu Visible” on page 593
• “Message Library” on page 593
• “Message Queue” on page 593
• “National Character Set” on page 593
• “New Session Uses Current Session’s Settings” on page 594
• “New Window on Open” on page 594
• “OLE Application Name” on page 594
“Path and Name of Executable” on page 594
“Path to Executive” on page 594
“Print at End of Document” on page 595
“Print at Start of Document” on page 595
“Print Auto Orientation” on page 596
“Print Auto Word Wrap” on page 596
“Print Compress Font Vertically” on page 596
“Print DBCS:SBCS in 2:3 Ratio” on page 596
“Print DBCS with a Smaller Font” on page 596
“Print Destination” on page 597
“Print Device ASCII 899” on page 597
“Print Device Envelope Source” on page 597
“Print Device Font ID” on page 598
“Print Device Forms Mode” on page 598
“Print Device Paper Source 1” on page 598
“Print Device Paper Source 2” on page 599
“Print File Exists Action” on page 600
“Print File Name” on page 600
“Print Fit Form Size” on page 600
“Print Fit Form to Page” on page 601
“Print Fit to Page” on page 601
“Print Fit User Form Length” on page 601
“Print Fit User Form to Page” on page 601
“Print Fit User Form Width” on page 602
“Print Form Feed on End of Job” on page 602
“Print Hook Enable” on page 602
“Print Honor Form Feed Only in First Column” on page 602
“Print Override Host Format” on page 602
“Print Override Orientation” on page 603
“Print Overstrike” on page 603
“Print Proportional Chars per Inch” on page 603
“Print Retain Host Format” on page 603
“Print Suppress Blank Page” on page 604
“Print Suppress Initial Form Feed” on page 604
“Print Suppress Newlines” on page 604
“Print Suppress Null Lines” on page 604
“Print to File” on page 605
“Print Transform” on page 605
“Print Translate EBCDIC in TRN” on page 605
“Print Transparent” on page 605
• “Print Transverse Orientation” on page 606
• “Print Proportional Lines per Inch” on page 606
• “Printer Case” on page 606
• “Printer Chars per Inch” on page 606
• “Printer Chars per Line” on page 607
• “Printer DBCS Character Rotation Angle” on page 607
• “Printer DBCS Horizontal Font Size” on page 607
• “Printer DBCS Vertical Font Size” on page 607
• “Printer Default Font” on page 608
• “Printer Default Horizontal Tab” on page 608
• “Printer Default Vertical Tab” on page 608
• “Printer Emulate FF with LF” on page 608
• “Printer Flush on End of Job” on page 608
• “Printer Flush on End of Media” on page 609
• “Printer Flush on Form Feed” on page 609
• “Printer Host LU Name” on page 609
• “Printer Line Spacing” on page 609
• “Printer Lines Per Inch” on page 610
• “Printer Lines Per Page” on page 610
• “Printer Margin Bottom” on page 610
• “Printer Margin Left” on page 611
• “Printer Margin Right” on page 611
• “Printer Margin Top” on page 611
• “Printer Maximum Chars per Line” on page 611
• “Printer Maximum Lines per Page” on page 612
• “Printer Orientation” on page 612
• “Printer Output Reduction” on page 612
• “Printer Paper Size” on page 612
• “Printer Paper Source” on page 613
• “Printer SO/SI Presentation” on page 613
• “Representation of Unmapped DBCS Character” on page 613
• “Save Changes on Exit” on page 613
• “Save Window State” on page 614
• “Settings Changed” on page 614
• “Settings File” on page 614
• “Settings Update Type” on page 614
• “Shortcut Folder” on page 615
• “Show Status Bar” on page 615
• “Show Title Bar” on page 615
• “Startup Settings” on page 615
AS/400 Host Name

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.
Use this setting to specify the name of the AS/400 host to which you want to connect when Service Location Protocol (SLP) is enabled. This ensures that you connect to the AS/400 named even if the load balancing features of SLP have connected you to an AS/400 running fewer sessions.

**Assigned AS/400 Host**

*Getting there*

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This read-only setting specifies the AS/400 you’re assigned to when Service Location Protocol (SLP) is enabled.

**Assigned Device Name**

*Getting there*

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This read-only setting specifies which device is assigned for your connection. Applies to 5250 printer sessions only.

**Assigned Encryption Strength**

*Getting there*

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting specifies the encryption strength used by Secure Sockets Layer/Transport Layer Security (SSL/TLS) data stream encryption. You can specify an encryption strength or let the host negotiate an encryption strength with Reflection.

**NOTE:** Before you can this setting, you must enable “Telnet Encryption” on page 617.

**Assigned Host Name**

*Getting there*

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This read-only setting specifies the host to which your session is connected. Applies only to Telnet connections that use Service Location Protocol (SLP).
Assigned LU Name

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This read-only setting specifies which LU (session) is assigned for your connection. Applies to 3270 sessions only.

Auto Connect

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

Select this check box to establish a host connection immediately after you open the associated settings file, and then save your settings to an *.rsf file (the changes take effect the next time you load the file).

For example, if you configure a host named TELSTAR in the Session Setup dialog box and select Auto Connect, and then choose File > Save As and save your settings to a file named Telstar.rsf, Reflection automatically connects to TELSTAR when you open the Telstar.rsf file.

Auto Reconnect

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

If Auto Reconnect is set to Yes, Reflection attempts to reconnect after any disconnection that is not initiated by Reflection. Applies to 5250 connections using Telnet, and 3270 connections using Telnet or Telnet Extended.

Bypass Windows Printing

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting specifies whether to disable having Windows handle fonts, font size, font style, and lines-per-inch configuration. Affects 3812 printing and 3287 printing.

**NOTE:** Bypassing Windows printing is not the same as disabling Windows print spooling, which you can do from the Control Panel. Disabling print spooling is not recommended if you're printing to a network printer or running multiple applications that may be sending data to the printer.
Bypass Windows Printing in Transparent Mode

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting specifies whether to disable having Windows handle fonts, font size, font style, and lines-per-inch configuration while in Transparent mode. Affects 3812 printing and 3287 printing.

**NOTE:** Bypassing Windows printing is not the same as disabling Windows print spooling, which you can do from the Control Panel. Disabling print spooling is not recommended if you're printing to a network printer or running multiple applications that may be sending data to the printer.

C/370 Character Set

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting specifies whether to use the C/370 code page. The C/370 code page provides support for square brackets ("[") and "]").

Caption

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting specifies the string that appears in the Reflection title bar, and is also displayed within the taskbar.

**NOTE:** Note :When Reflection is running, but minimized, the “Icon Title” on page 591 defines the string shown on the taskbar.

Type text and/or shortcuts up to 260 characters in the Settings details box.

<table>
<thead>
<tr>
<th>Shortcut</th>
<th>Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>&amp;w</td>
<td>Attachmate</td>
</tr>
<tr>
<td>&amp;r</td>
<td>Reflection</td>
</tr>
<tr>
<td>&amp;f</td>
<td>Settings File Name (or Untitled if a settings file is not open)</td>
</tr>
<tr>
<td>&amp;s</td>
<td>Session Type</td>
</tr>
<tr>
<td>&amp;t</td>
<td>Transport</td>
</tr>
<tr>
<td>&amp;h</td>
<td>Host Name</td>
</tr>
<tr>
<td>&amp;d</td>
<td>Date</td>
</tr>
</tbody>
</table>
Command Line Switches

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This read-only setting shows the command line switches (also called command line parameters), if any, that were used to start Reflection.

Confirm on Exit

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting specifies whether a confirmation dialog box appears if you try to exit Reflection while connected to a host.

NOTE: Changes you make to this setting are saved to the Windows registry and affect all Reflection sessions.

Country Extended Graphics Code

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

Select to make additional characters available in the configured National character set. See your host documentation for details.
Create Settings File Shortcut

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting specifies whether Reflection automatically creates a shortcut whenever you save a settings file. You can use the shortcut to start Reflection and open your saved settings.

Current Display Height

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This read-only setting specifies the number of rows in the current display height.

NOTE: The value of this setting includes two non-addressable rows that are dedicated to the Operator Information Area (OIA) — the actual number of addressable rows in the display height is the number of addressable rows minus two (2).

Current Display Width

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This read-only setting specifies the number of columns in the current display width.

Current Locale

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This read-only setting shows in which language Reflection is running. Use this setting to determine which language Reflection is using when no language has been specified in either the "Locale" on page 592 or "Language Override" on page 591 settings.

Current Trace Record

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting specifies the current trace record and is relevant only when Pause Playback Trace on EOR is set to Yes (default).
As you play back a trace, you can restart the trace at any point by changing the value of **Current Trace Record**. If you specify a value greater than the number of records in the trace file, trace playback stops.

**Default Printer Copies**

**Getting there**

1. Open a printer emulation session.
2. From the **Setup** menu, choose **View Settings**.

This setting determines the number of copies to print. If you write a command to print, you must specify the number of copies in the command.

**Device Name**

**Getting there**

1. Open a printer emulation session.
2. From the **Setup** menu, choose **View Settings**.

Use this setting to specify the name of the device (up to 32 characters) to which you want to connect.

**NOTE:** You cannot change this value while you’re connected.

**Enable Asynchronous Transport Behavior**

**Getting there**

1. Open a printer emulation session.
2. From the **Setup** menu, choose **View Settings**.

This setting specifies whether Reflection reverts to polling mode for host interactions. Used primarily for diagnostic purposes.

**Enable Host Alarm**

**Getting there**

1. Open a printer emulation session.
2. From the **Setup** menu, choose **View Settings**.

This setting specifies whether the host sounds alarms (beeps) in 5250 sessions.

**Font Character Set**

**Getting there**

1. Open a printer emulation session.
2. From the **Setup** menu, choose **View Settings**.

Specify the character set that Reflection uses for its user interface.
Choose from the following character sets:

- Ansi Character Set (default)
- Arabic Character Set
- Baltic Character Set
- Chinese Big5 Character Set
- East European Character Set
- GB2312 Character Set
- Greek Character Set
- Hangeul Character Set
- Hebrew Character Set
- Johab Character Set
- Oem Character Set
- Russian Character Set
- ShiftJis Character Set
- Thai Character Set
- Turkish Character Set

**Fully Qualified Remote LU Name**

**Getting there**

1. Open a printer emulation session.
2. From the **Setup** menu, choose **View Settings**.

This setting defines the AS/400 system in the following format:

NetId.LuName

**Generate Device Names**

**Getting there**

1. Open a printer emulation session.
2. From the **Setup** menu, choose **View Settings**.

To create device names based on the values you enter for **Device Name** from the **Session Setup** dialog box, set **Generate Device Names** to Yes. Available only for 5250 Telnet sessions.
Type any of the following characters as part of the value in the **Device Name** box:

<table>
<thead>
<tr>
<th>Value</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>For each new session, replaced by &quot;A&quot;, &quot;B&quot;, &quot;C&quot;, and so on. If the entire alphabet is used, the generated device names continue with &quot;AA&quot;, &quot;AB&quot;, &quot;AC&quot;, and so on.</td>
</tr>
<tr>
<td>%</td>
<td>For printer sessions, replaced by &quot;P&quot;; for display sessions, replaced by &quot;S&quot;.</td>
</tr>
<tr>
<td>=</td>
<td>For each new session, replaced by &quot;1&quot;, &quot;2&quot;, &quot;3&quot;, and so on.</td>
</tr>
<tr>
<td>&amp;COMPN</td>
<td>Replaced by the local workstation name; left-trimmed if the generated name exceeds 10 characters. <strong>NOTE:</strong> This character cannot be used with &quot;&amp;USERN&quot;.</td>
</tr>
<tr>
<td>&amp;USERN</td>
<td>Replaced by the local user name; left-trimmed if the generated name exceeds 10 characters. <strong>NOTE:</strong> This character cannot be used with &quot;&amp;COMPN&quot;.</td>
</tr>
<tr>
<td>+</td>
<td>Use anywhere in the string with &quot;&amp;USERN&quot; or &quot;&amp;COMPN&quot; to specify right-trimming instead of left-trimming.</td>
</tr>
</tbody>
</table>

**NOTE:** You can use only one string literal in combination with these characters. If you use separated strings, the second string is dropped. For example, if you use "%My=Device", the second string ("Device") will be ignored when the device name is generated. However, "%MyDevice" contains only one string ("MyDevice") and won't have this problem.

### Examples

**This Device Name setting** | **Generates**
---|---
"%ABC=" | The device name SABC1 for a display session. If this is rejected, Reflection will try SABC2, SABC3, and so on.
"%123*" | The device name S123A for the first display session, S123B for the second session, and so on.
"&COMPN*" | The names puternameA, puternameB, puternameC for the first three sessions, when the computer name is "Computername".
"+&USERN*" | The names victoruA, victoruB, victoruC for the first three sessions, when the computer user name is "victoru".

**NOTE:** In display sessions, the device name appears in the sign-on screen when you connect to the host; in printer sessions, the device name appears in the "Assigned Device Name" on page 582 setting details in the **View Settings** dialog box.

## Host Communication Timeout

### Getting there

1. Open a printer emulation session.
2. From the **Setup** menu, choose **View Settings**.
This setting specifies the number of seconds Reflection should wait for a host connection response. If there is no response from the host in the allotted time, an error results.

**Host Name**

**Getting there**

1. Open a printer emulation session.
2. From the **Setup** menu, choose **View Settings**.

Use this setting to specify the host to which you want to connect. Type a value (up to 260 characters) to indicate an Internet address, an Internet node name, or a name that can be resolved by a Hosts file or a domain name server.

**Host Network Address**

**Getting there**

1. Open a printer emulation session.
2. From the **Setup** menu, choose **View Settings**.

This read-only setting specifies the address of the host.

**Host Print Timeout**

**Getting there**

1. Open a printer emulation session.
2. From the **Setup** menu, choose **View Settings**.

Use this setting to specify the number of seconds to wait after the host stops sending data to a printer session before forcing all pending printer output to the printer. The action performed by this setting is equivalent to pressing the Flush button on the 3287 printer panel.

**Hosts File Name**

**Getting there**

1. Open a printer emulation session.
2. From the **Setup** menu, choose **View Settings**.

Specify the path to the Hosts file (up to a maximum of 260 characters), which maps assigned node names to Internet addresses. Reflection changes the value of this setting when it finds a Hosts file.

Reflection searches for the Hosts file in the following locations (in order):

- In the same path as Wsock32.dll
- If the System or System32 folder of the operating system's root folder
- In the folder where Reflection is installed
- The current folder
- In the operating system's root folder
- The folders in your Path statement
If Reflection cannot find the Hosts file in any of locations in the preceding list, this field remains blank. To locate a Hosts file on your PC, from the View Settings dialog box, select Hosts File Name and click the Browse button, or use the operating system's Find feature.

**NOTE:** Windows TCP/IP software must be able to locate the Hosts file in the Winnt\System32\Drivers\Etc folder before Reflection can generate a list of hosts.

## Icon Title

### Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

Specifies the string that appears on the taskbar when Reflection is minimized. If Reflection is not minimized, the string shown on the taskbar is defined by the Caption setting.

In the Settings details text box, enter text or any of the following predefined options (up to 260 characters).

<table>
<thead>
<tr>
<th>Shortcut</th>
<th>Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>&amp;w</td>
<td>Attachmate</td>
</tr>
<tr>
<td>&amp;r</td>
<td>Reflection</td>
</tr>
<tr>
<td>&amp;f</td>
<td>Settings File Name (or Untitled if a settings file is not open)</td>
</tr>
<tr>
<td>&amp;s</td>
<td>Session Type</td>
</tr>
<tr>
<td>&amp;t</td>
<td>Transport</td>
</tr>
<tr>
<td>&amp;h</td>
<td>Host Name</td>
</tr>
<tr>
<td>&amp;d</td>
<td>Date</td>
</tr>
<tr>
<td>&amp;c</td>
<td>Connection Status (whether you are connected and over what transport)</td>
</tr>
<tr>
<td>&amp;p</td>
<td>Printer Status</td>
</tr>
<tr>
<td>&amp;x</td>
<td>Transfer Status (the percentage complete of file and data transfers)</td>
</tr>
<tr>
<td>&amp;v</td>
<td>Assigned Device Name (relevant only for 5250 sessions that use an assigned Device Name)</td>
</tr>
<tr>
<td>&amp;l</td>
<td>Assigned LU Name (relevant only for 3270 sessions that use an assigned LU Name)</td>
</tr>
<tr>
<td>&amp;o</td>
<td>Profile Name</td>
</tr>
<tr>
<td>&amp;&amp;</td>
<td>A Single Ampersand</td>
</tr>
</tbody>
</table>

## Language Override

### Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.
Specifies the language Reflection uses for menus, dialog boxes, and Help when a new (untitled) session is opened. When set to Off (default), language is based on your current system configuration and the Reflection language support you have installed. The same is true if you specify a language for which you have not installed support. This setting is saved to the registry, and takes effect the next time you start a Reflection session.

This setting is similar to the “Locale” on page 592 setting; however, Locale saves language information to a settings file. When you open a settings file, Reflection uses the current value of the Locale setting, whereas the Language Override setting affects all new sessions.

Locale

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting specifies which language to use in the Reflection user interface and Help files. If you don't have the necessary .DLL file, this setting does not change the language used in the interface and help files. However, it does change some of the accelerator keys to those used in the localized version of the product.

This setting is similar to the “Language Override” on page 591 setting, however Locale saves language information to a settings file. Use Locale to select a language for a particular session for which you have created a settings file. Use Language Override to select a language for all new sessions.

Manufacturer Type

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

Use this setting to specify the printer manufacturer type that the AS/400 will use to print host print jobs when Print Transform is set to Yes.

The Manufacturer Type setting must match a manufacturer type and model defined on the AS/400. To select from a list of possible values, you can set this value using the “5250 Printer Device Initialization Dialog Box” on page 542.

This setting affects only 5250 printer sessions.

Maximum Internal Trace File Length (MB)

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting specifies the maximum size for a trace file, in megabytes. If the internal trace file exceeds this amount, the oldest data is overwritten by the newer data, a process called wrapping. A setting of 0 (default) means that the trace file does not wrap but continues to get bigger for as long as the tracing lasts.
Change this setting from the default value to trace problems that are intermittent or not easily reproducible.

**Menu Visible**

**Getting there**

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting specifies whether the Menu Bar is displayed in the Reflection screen.

**Message Library**

**Getting there**

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting specifies which library contains the message queue for exception messages.

The default value, *LIBL, is sufficient for most cases. Consult your system administrator before changing this value.

**Message Queue**

**Getting there**

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

Use this setting to specify the AS/400 message queue to which exception messages are sent. For example, the AS/400 may need to send a message to the printer to switch paper trays.

The default message queue is contained in QSYSOPR. Consult your system administrator before changing this value.

**National Character Set**

**Getting there**

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting specifies the national character set for your terminal sessions and should match the national character set used by your host system. If it does not, some characters, such as accents, may not display correctly.

See your host documentation for definitions of the characters in each set.
New Session Uses Current Session's Settings

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

When set to No (default), new sessions use the default Reflection settings; when set to Yes, new sessions use the settings and macros configured in your current Reflection session.

NOTE: The system administrator can configure the default session settings using the Reflection profiler.

New Window on Open

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting specifies whether to open a new window when you open a settings file.

OLE Application Name

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This read-only setting returns the name of the Reflection product.

Path and Name of Executable

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This read-only setting returns the full path and filename (including the drive letter) for the Reflection executable file.

Path to Executable

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This read-only setting returns the full path (including the drive letter) for the Reflection executable file.
Print at End of Document

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

Use this setting to specify data that you want to send to the printer at the end of a document. The Bypass Windows Printing setting must be enabled.

When specifying data, use C Constant expressions, such as the following:

\a  bell
\b  backspace
\e  escape
\f  form feed
\n  new line
\r  carriage return
\t  horizontal tab
\v  vertical tab

Print at Start of Document

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

Use this setting to specify data that you want to send to the printer at the start of a document. Data must be formatted using the C constant format and the Bypass Windows Printing setting must be enabled.

When specifying data, use any of the following predefined constants:

\a  bell
\b  backspace
\e  escape
\f  form feed
\n  new line
\r  carriage return
\t  horizontal tab
\v  vertical tab

For example, the string \e\a10\x1A\0\007 would be interpreted as [ESC]&l10[CTRL-Z][NULL][BELL].
Print Auto Orientation

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting determines the orientation from the page dimensions of a print job instead of from an explicit landscape or portrait command. Applies only to 3812 printing (setting corresponds to the automatic orientation control on a 3812 printer).

Print Auto Word Wrap

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting specifies whether to wrap text when the end of a line is reached in a host print job.

Print Compress Font Vertically

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting specifies whether Reflection compresses Thai characters vertically to improve legibility. Applies only to 5250 sessions running in Thai language versions of Reflection.

Print DBCS:SBCS in 2:3 Ratio

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting specifies whether to make double-byte characters up to 1.5 times wider than their default size to make them more readable when printing host print jobs and terminal screens.

When set to Yes, Reflection expands double-byte characters so that two characters occupy the same number of spaces as three single-byte characters. Applicable to 5250 sessions only.

Print DBCS with a Smaller Font

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting specifies whether to print double-byte characters using a smaller font size. Applies only to 5250 sessions.
Print Destination

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

Specifies the destination printer for print jobs. You can specify a printer using this setting or using the Print Setup dialog box.

Related Topics

- “Print Setup Dialog Box” on page 552

Print Device ASCII 899

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting specifies whether the current 5250 printer session supports ASCII code page 899. Valid only if Host Print Transform (page 605) is selected.

Print Device Envelope Source

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting specifies the envelope source on the host printer. Choose from the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*B5</td>
<td>Size B5 (176 × 250 mm) envelopes.</td>
</tr>
<tr>
<td>*C5</td>
<td>Size C5 (162 x 299 mm) envelopes.</td>
</tr>
<tr>
<td>*DL</td>
<td>Size DL (110 × 220 mm) envelopes.</td>
</tr>
<tr>
<td>*MONARCH</td>
<td>Monarch-sized (3.875 × 7.5 in.) envelopes.</td>
</tr>
<tr>
<td>*NONE</td>
<td>No source specified.</td>
</tr>
<tr>
<td>*NUMBER10</td>
<td>Number 10 (4.125 × 9.5 in.) envelopes.</td>
</tr>
<tr>
<td>*NUMBER9</td>
<td>Number 9 (3.875 × 8.875 in.) envelopes.</td>
</tr>
<tr>
<td>*SAME</td>
<td>Reflection uses the currently configured host value for the envelope source.</td>
</tr>
<tr>
<td>Windows printer</td>
<td>Reflection uses the currently configured value for envelope source specified by the default Windows printer.</td>
</tr>
</tbody>
</table>
Print Device Font ID

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting specifies the Font Typestyle ID to use for printing host print jobs.

The default is typestyle ID 11 (Courier 10 point).

Print Device Forms Mode

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting specifies how forms are fed into the printer, or the form feed type used for spooled files.

Choose from the following options:

*AUTOCUT (default) Use when single-cut sheets are fed into the printer automatically (the printer must have the sheet feed attachment).
*CONT Use when continuous forms are fed automatically by the printer.
*CUT Use when single-cut sheets are fed manually into the printer.

**NOTE:** The value for Paper Source 1 overrides the value for Print Device Forms Mode when Host Print Transform (page 605) is enabled.

Print Device Paper Source 1

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting specifies the first or primary paper source to be used by the host printer.

Choose from the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*A3</td>
<td>A3-sized paper (297 × 420 mm)</td>
</tr>
<tr>
<td>*A4</td>
<td>A4-sized paper (210 × 297 mm)</td>
</tr>
<tr>
<td>*A5</td>
<td>A5-sized paper (148 × 210 mm)</td>
</tr>
<tr>
<td>*B4</td>
<td>B4-sized paper (257 × 364 mm)</td>
</tr>
<tr>
<td>*B5</td>
<td>B5-sized paper (182 × 257 mm)</td>
</tr>
<tr>
<td>*CONT132</td>
<td>Continuous form paper (13.2 in. wide)</td>
</tr>
</tbody>
</table>
### Getting there

1. **Open a printer emulation session.**
2. **From the Setup menu, choose View Settings.**

This setting specifies the secondary paper source to be used by the host printer. Choose from the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*CONT80</td>
<td>Continuous form paper (8 in. wide)</td>
</tr>
<tr>
<td>*EXECUTIVE</td>
<td>Executive-sized paper (7.25 × 10.5 in.)</td>
</tr>
<tr>
<td>*LEDGER</td>
<td>Ledger-sized paper (17 × 11 in.)</td>
</tr>
<tr>
<td>*LEGAL</td>
<td>Legal-sized paper (8.5 × 14 in.)</td>
</tr>
<tr>
<td>*LETTER</td>
<td>Standard letter-sized paper (8.5 × 11 in.)</td>
</tr>
<tr>
<td>*MFRTYPMODEL</td>
<td>When you select *MFRTYPMODEL, the AS/400 substitutes the value most common for your printer (*LETTER for page printers, *CONT132 for wide-carriage continuous-feed printers, and so on).</td>
</tr>
<tr>
<td>*NONE</td>
<td>No paper source is specified.</td>
</tr>
<tr>
<td>*SAME</td>
<td>Reflection uses the currently configured host value for the primary paper source.</td>
</tr>
</tbody>
</table>

Windows Printer Reflection uses the currently configured value for primary paper source specified by the default Windows printer.

### Print Device Paper Source 2

#### Getting there

1. **Open a printer emulation session.**
2. **From the Setup menu, choose View Settings.**

This setting specifies the secondary paper source to be used by the host printer. Choose from the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*A3</td>
<td>A3-sized paper (297 × 420 mm)</td>
</tr>
<tr>
<td>*A4</td>
<td>A4-sized paper (210 × 297 mm)</td>
</tr>
<tr>
<td>*A5</td>
<td>A5-sized paper (148 × 210 mm)</td>
</tr>
<tr>
<td>*B4</td>
<td>B4-sized paper (257 × 364 mm)</td>
</tr>
<tr>
<td>*B5</td>
<td>B5-sized paper (182 × 257 mm)</td>
</tr>
<tr>
<td>*CONT132</td>
<td>Continuous form paper (13.2 in. wide)</td>
</tr>
<tr>
<td>*CONT80</td>
<td>Continuous form paper (8 in. wide)</td>
</tr>
<tr>
<td>*EXECUTIVE</td>
<td>Executive-sized paper (7.25 × 10.5 in.)</td>
</tr>
<tr>
<td>*LEDGER</td>
<td>Ledger-sized paper (17 × 11 in.)</td>
</tr>
<tr>
<td>*LEGAL</td>
<td>Legal-sized paper (8.5 × 14 in.)</td>
</tr>
<tr>
<td>*LETTER</td>
<td>Standard letter-sized paper (8.5 × 11 in.)</td>
</tr>
<tr>
<td>*MFRTYPMODEL</td>
<td>When you select *MFRTYPMODEL, the AS/400 substitutes the value most common for your printer (*LETTER for page printers, *CONT132 for wide-carriage continuous-feed printers, and so forth).</td>
</tr>
<tr>
<td>*NONE</td>
<td>No paper source is specified.</td>
</tr>
</tbody>
</table>
**Print File Exists Action**

**Getting there**

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting specifies what Reflection should do if it finds a PC file with the same name as the print file you are generating.

<table>
<thead>
<tr>
<th>Value</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Append</td>
<td>Adds the output to the end of the existing file.</td>
</tr>
<tr>
<td>Ask User (default)</td>
<td>Prompts you to make a decision.</td>
</tr>
<tr>
<td>Autonumber</td>
<td>Creates a new file with an incremented filename.</td>
</tr>
<tr>
<td>Overwrite</td>
<td>Replaces the existing PC file.</td>
</tr>
<tr>
<td>Open Error</td>
<td>Causes the print to file action to fail (return an error) when the PC file already exists.</td>
</tr>
</tbody>
</table>

**Print File Name**

**Getting there**

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

Use this setting to specify the name of the file to which the host print job or screen print is saved.

**Print Fit Form Size**

**Getting there**

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting specifies the size of the form that you want Reflection to fit to the currently configured form on your Windows printer. The values are all the available form sizes for Windows printers. By default, Reflection uses the paper size specified in the Page Setup dialog box.
**Print Fit Form to Page**

*Getting there*

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting specifies whether to print terminal screens or host print jobs to a form defined by Windows. This setting works in conjunction with the Print Fit Form Size setting.

When the terminal screen or host print job is printed, Reflection scales the print output to fit the user-defined form.

**Print Fit to Page**

*Getting there*

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting specifies whether to transform print jobs to maintain the relationship between the printed page (as defined by the host) and the printed page (as defined by the current Windows printer and page configuration).

**Print Fit User Form Length**

*Getting there*

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting specifies the length of the form to which you are printing via the Print Fit User Form to Page setting.

The value is expressed in percent reduction (less than 100%) or expansion (greater than 100%).

**Print Fit User Form to Page**

*Getting there*

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting specifies whether to print host print jobs or terminal screens to a user-defined form. When the host print job or terminal screen is printed, Reflection scales the print output to fit the user-defined form.

Use the settings Print Fit User Form Length and Print Fit User Form Width to define the form you want to which you want to print.
Print Fit User Form Width

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting specifies the width of the form to which you are printing via the Print Fit User Form to Page setting.

Print Form Feed on End of Job

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting specifies whether to send a form feed after printing a host print job.

Print Hook Enable

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

Use this setting to send LU1 (SCS) printer data to a registered printer hook COM object instead of an actual printer for processing.

Print Honor Form Feed Only in First Column

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting specifies whether Reflection honors only form feeds that are in the first column of a print job. When this setting is No (default), all form feeds are honored, regardless of their position in the data stream.

Print Override Host Format

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting specifies whether Reflection page formatting (characters per line, lines per page, font, and margins) is used, regardless of what the host specifies.
Print Override Orientation

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

Enable this setting to override the page orientation set by the host and instead, use the orientation currently defined in the Windows Page Setup dialog box. This option is applicable to both terminal and printer sessions.

In terminal sessions, page orientation is not explicitly set by the host but may be implied by the host page size. For example, by default the host page size is defined by the number of columns and rows that make up the terminal display. If the display is narrower than it is long, portrait orientation is implied. If the display is wider than it is long, landscape orientation is implied.

In printer sessions, the host may explicitly set a particular orientation in the data stream, or an orientation may be implied by the host page size, as described in the preceding text for terminal sessions.

Print Overstrike

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting specifies whether Reflection simulates bold printing by using overstrike printing.

**NOTE:** Simulated bold printing may cause an undesired shift in the printing of some DBCS characters.

To disable simulated bold printing set Print Overstrike to No Offset.

Print Proportional Chars per Inch

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

When this setting is enabled, the number of characters printed per line is always determined by dividing the width of the page (minus the left and right margins) by the width of a single character (the value of “Printer Chars per Inch” on page 606 is therefore ignored). Affects only 3812 printing.

Print Retain Host Format

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

Specify Yes to retain the format set by the host after a print job completes. If you specify No (default), the pre-existing format is restored after a print job completes.
NOTE: This setting is ignored if Print Override Host Format is enabled.

Print Suppress Blank Page

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting prevents blank pages from appearing in host print jobs.

Print Suppress Initial Form Feed

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

Select Yes to suppress the first form feed encountered in the data stream prior to any printable data.

Print Suppress Newlines

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting specifies how Reflection handles the suppression of extra blank lines in 3270 Printing (3287 Printer Emulation).

If a line of characters goes to the rightmost edge of the printable area, an automatic new line is generated. If a new-line character (0 x 15) occurs in the data stream after an automatic new line, two new lines occur, which creates a blank line in the printout. When this setting is Yes (default), Reflection ignores the data stream new-line character so that printed output does not include a blank line.

When this setting is No, the new line is not ignored and blank lines are printed. (This matches the behavior seen in the IBM PComm product.)

Print Suppress Null Lines

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting specifies whether lines of data that contain only null characters are suppressed in LU3 print jobs only.
Print to File

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting specifies whether Reflection directs screen prints and host print jobs to a file instead of a physical printer.

Print Transform

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

To enable the Print Transform option, select IBM 5250 Printer as Session Type in the Session Setup dialog box, and then click the Initialize button.

When Print Transform is enabled on a AS/400 print device, you can specify the following parameters for the printer device:

- Manufacturer type
- Paper source 1
- Paper source 2
- Envelope source

**NOTE:** If you set the Manufacturer Type to a printer that begins with *WSCST, you must specify the Workstation Customizing Object (WSCST) name and library that the AS/400 will use to print jobs.

Print Translate EBCDIC in TRN

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting specifies whether to print EBCDIC characters contained within the SCS TRN command.

Print Transparent

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

In transparent mode, all page format parameters (such as Characters Per Line and Lines Per Page) are ignored.
In 3812 printer sessions, select this option when the printer device is configured for **Host Print Transform** — that is, for documents (such as PCL files) that require no page formatting from Reflection or Windows.

In 3287 printer sessions, select this option for documents, such as PostScript files, that require no page formatting from Reflection.

**NOTE:** This setting is only relevant when “Bypass Windows Printing” on page 583 is set to Yes.

**Print Transverse Orientation**

This setting specifies whether to rotate a form (make transverse) compared to what the host is requesting before printing.

Applies only to 5250 printer sessions in which either the **Print Fit User Form to Page** or **Print Fit Form to Page** setting is set to Yes.

**Print Proportional Lines per Inch**

**Getting there**

1. Open a printer emulation session.
2. From the **Setup** menu, choose **View Settings**.

When this setting is enabled, the height of each print line is determined by the size of the selected font (the value of **Printer Lines Per Inch** on page 610 is therefore ignored). Affects both 3812 printing and 3287 printing.

**Printer Case**

**Getting there**

1. Open a printer emulation session.
2. From the **Setup** menu, choose **View Settings**.

This setting specifies how to handle cases in a print job. Select Dual Case (default) to print the host print job using a mixture of uppercase and lowercase letters; select Upper Case to force all text in the host print job to uppercase letters.

**Printer Chars per Inch**

**Getting there**

1. Open a printer emulation session.
2. From the **Setup** menu, choose **View Settings**.

This setting specifies the number of characters to print per inch.

If “**Print Proportional Chars per Inch**” on page 603 is set to Yes, **Printer Chars Per Inch** is disregarded. In this case, the number of characters printed per inch is determined by the current printer font.
As you change **Printer Chars Per Inch** in view 2.3, "Printer Chars per Line" on page 607 may change as well; more characters per inch means more characters on a line (assuming the left and right margins don't change).

**Printer Chars per Line**

**Getting there**

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting specifies the maximum number of characters that can be printed on a single line for 3812 and 3287 printing. If the host passes down a line that exceeds the maximum, Reflection automatically wraps the line.

Depending on your printer driver, font, and font size, the actual number of characters that can be printed on a line can vary. Use the Info button in the printer panel to find out the number of columns you can actually print.

As you change **Printer Chars Per Line**, "Printer Chars per Inch" on page 606 may change as well; more characters on a line means more characters per inch (assuming the left and right margins don't change).

**Printer DBCS Character Rotation Angle**

**Getting there**

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting specifies whether to rotate characters 270 degrees when printing host print jobs or terminal screens. Rotating characters 270 degrees presents host print jobs containing double-byte characters in traditional, up to down, left to right alignment.

Applies only to double-byte character sets in 5250 sessions.

**Printer DBCS Horizontal Font Size**

**Getting there**

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting specifies whether Reflection doubles the horizontal size of double-byte characters when it prints host screens or print jobs to make them more legible. Applies to 5250 sessions only.

**Printer DBCS Vertical Font Size**

**Getting there**

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.
This setting specifies whether Reflection doubles the vertical size of double-byte characters when it prints host screens or print jobs to make them more legible. Applies to 5250 sessions only.

**Printer Default Font**

**Getting there**

1. Open a printer emulation session.
2. From the *Setup* menu, choose *View Settings*.

This setting specifies font information to the Windows printer driver only when “Bypass Windows Printing” on page 583 is set to No.

Enter a string (up to 260 characters) that specifies valid font information for your current Windows printer driver. For example:

Courier, 10

**Printer Default Horizontal Tab**

**Getting there**

1. Open a printer emulation session.
2. From the *Setup* menu, choose *View Settings*.

This setting specifies the number of spaces to use for horizontal tabs. Applies to 3287 print jobs only.

**Printer Default Vertical Tab**

**Getting there**

1. Open a printer emulation session.
2. From the *Setup* menu, choose *View Settings*.

This setting specifies the number of lines to use for vertical tabs. Applies to 3287 print jobs only.

**Printer Emulate FF with LF**

**Getting there**

1. Open a printer emulation session.
2. From the *Setup* menu, choose *View Settings*.

This setting specifies whether Reflection should simulate a form feed by issuing line feeds until the end of the page is reached.

**Printer Flush on End of Job**

**Getting there**

1. Open a printer emulation session.
2. From the *Setup* menu, choose *View Settings*. 
This setting specifies whether an in-progress print job is closed if an end of job condition is sent from the host.

**Printer Flush on End of Media**

Getting there

1. Open a printer emulation session.
2. From the **Setup** menu, choose **View Settings**.

Select Yes to terminate LU3 print jobs if Reflection encounters an End of Media character.

**Printer Flush on Form Feed**

Getting there

1. Open a printer emulation session.
2. From the **Setup** menu, choose **View Settings**.

Select Yes to terminate LU3 print jobs if Reflection encounters a form feed.

**Printer Host LU Name**

Getting there

1. Open a printer emulation session.
2. From the **Setup** menu, choose **View Settings**.

Specify a name (up to 32 characters), if the host requires that you supply a host LU name when connecting as a 3287 printer.

**NOTE:** You cannot change this value while you're connected.

**Printer Line Spacing**

Getting there

1. Open a printer emulation session.
2. From the **Setup** menu, choose **View Settings**.

This setting specifies the amount of space between lines for 3812 and 3287 printer output.
Printer Lines Per Inch

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting specifies vertical spacing for printer output, measured in Lines Per Inch (LPI).

Printer Lines Per Page

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

Specifies the number of lines to print on a page for 3812 and 3287 printing.

Depending on your printer driver, font, and font size, the actual number of characters that can be printed on a line can vary. Use the Info button in the Reflection 3287 printer panel or 3812 printer panel to find out the number of lines per page your printer driver can accommodate for the current font and font size.

As you change this value for a 3812 printer session, the value for “Printer Lines Per Inch” on page 610 may change as well; more lines on a page means more lines per inch (assuming the top and bottom margins don’t change).

Printer Margin Bottom

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting specifies the size of the margin at the bottom of a page of printed output. The units of measure are twips. (A twip equals one twentieth of a point. There are 1440 twips to an inch.)

As you change your top or bottom margin, the value for “Printer Lines Per Page” on page 610 may change as well — larger margins mean fewer lines per page.
Printer Margin Left

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting specifies the size of the margin at the left side of a page of printed output. The units of measure are twips. (A twip equals one twentieth of a point. There are 1440 twips to an inch.)

As you change your left or right margin, the value for “Printer Chars per Line” on page 607 may change as well — larger margins mean fewer characters per line.

Printer Margin Right

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting specifies the size of the margin to be left at the right side of a page of printed output. The units of measure are twips. (A twip equals one twentieth of a point. There are 1440 twips to an inch.)

As you change your left or right margin, the value for “Printer Chars per Line” on page 607 may change as well — larger margins mean fewer characters per line.

Printer Margin Top

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting specifies the size of the margin at the top of a page of printed output. The units of measure are twips. (A twip equals one twentieth of a point. There are 1440 twips to an inch.)

As you change your top or bottom margin, the value for “Printer Lines Per Page” on page 610 may change as well — larger margins mean fewer lines per page.

Printer Maximum Chars per Line

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting specifies the value that Reflection provides to host applications that ask for the maximum number of printer characters per line.
Printer Maximum Lines per Page

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting specifies the value that Reflection provides to host applications that ask for the maximum number of printer lines per page.

Printer Orientation

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting specifies the default page orientation used to print both host print jobs in printer sessions, and host printing from terminal sessions.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Orientation</td>
<td>Uses the orientation defined by the currently selected Windows printer.</td>
</tr>
<tr>
<td>Landscape Orientation</td>
<td>Sets the page orientation to landscape mode (for example, 11&quot; x 8.5&quot;).</td>
</tr>
<tr>
<td>Portrait Orientation</td>
<td>Sets the page orientation to portrait mode (for example, 8.5&quot; x 11&quot;).</td>
</tr>
</tbody>
</table>

Printer Output Reduction

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

When enabled, this 3812 printing option does the following:

- Prints in landscape orientation — that is, with the longer (11 1/2 inch) edges of the paper as the top and bottom margins, and the shorter (8 inch) edge as the left and right margins
- Reduces the height of each line to 70 percent of the Lines Per Inch value
- Sets the top and left margins to 0.5 inches
- Increases the density of printed text to 125 percent of the Printer > Characters Per Inch value

Printer Paper Size

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting specifies the paper size to use for the current default Windows printer.
**Printer Paper Source**

**Getting there**

1. Open a printer emulation session.
2. From the **Setup** menu, choose **View Settings**.

This setting specifies the paper source to use for the current default Windows printer.

**Printer SO/SI Presentation**

**Getting there**

1. Open a printer emulation session.
2. From the **Setup** menu, choose **View Settings**.

This setting specifies the way Reflection treats shift-out and shift-in (SO/SI) characters, when printing host print jobs or terminal screens, in 5250 sessions only. Choose from the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SO/SI Rendered as Blanks (default)</td>
<td>Prints SO/SI characters as blank spaces. Select for WYSIWYG printing.</td>
</tr>
<tr>
<td>SO/SI Removed</td>
<td>Removes SO/SI characters and the cells they occupy, and condenses the remaining text.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Removing cells containing SO/SI characters changes the spacing of the text and may cause columns to go out of alignment.</td>
</tr>
<tr>
<td>SO Removed, SI Rendered as 2 Blanks</td>
<td>Removes SO characters, shifts double-byte characters one cell to the left, and prints SI characters as two blank spaces. This option preserves the alignment of columns in host print jobs.</td>
</tr>
</tbody>
</table>

**Representation of Unmapped DBCS Character**

**Getting there**

1. Open a printer emulation session.
2. From the **Setup** menu, choose **View Settings**.

In double-byte sessions, this setting determines how double-byte host characters not available in the Shift-JIS DBCS character translation table appear on the terminal screen, in file transfers using JISASCII translation, and in printed output.

**Save Changes on Exit**

**Getting there**

1. Open a printer emulation session.
2. From the **Setup** menu, choose **View Settings**.

This setting specifies the way to handle changes to settings and macros when you exit the current session or open a new session in the current window. Choose from the following options:
### Save Window State

**Getting there**

1. Open a printer emulation session.
2. From the **Setup** menu, choose **View Settings**.

This setting specifies whether to save the size and position of the terminal window when you save a settings file.

**NOTE:** When running in a browser, Reflection cannot save the terminal window's size and position.

### Settings Changed

**Getting there**

1. Open a printer emulation session.
2. From the **Setup** menu, choose **View Settings**.

This read-only setting indicates whether changes to Reflection macros or settings have not been saved.

### Settings File

**Getting there**

1. Open a printer emulation session.
2. From the **Setup** menu, choose **View Settings**.

This read-only setting returns the name of the open settings file. If no settings file is open, an empty string (""") is returned.

### Settings Update Type

**Getting there**

1. Open a printer emulation session.
2. From the **Setup** menu, choose **View Settings**.

This setting determines which settings Reflection includes when you save a settings update file.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ask</td>
<td>If settings or macros have been changed, Reflection opens a dialog box from which you can save the changes, exit without saving, or cancel and return to the Reflection session.</td>
</tr>
<tr>
<td>No</td>
<td>Reflection closes without saving any changes.</td>
</tr>
<tr>
<td>Yes</td>
<td>Reflection saves any changes without prompting.</td>
</tr>
</tbody>
</table>
When you create an update file, Reflection compares your current settings to a default configuration, and saves only those settings that have been changed from their default values. Because system administrators can customize Reflection, your site defaults may differ from the Reflection factory defaults.

This setting also determines whether the default settings used for this comparison are the Reflection factory defaults, or if they are defaults that have been customized (profiled) for your site by a system administrator.

**Shortcut Folder**

**Getting there**

1. Open a printer emulation session.
2. From the **Setup** menu, choose **View Settings**.

This setting specifies the location where Reflection creates the linked shortcut when you save a settings file.

**Show Status Bar**

**Getting there**

1. Open a printer emulation session.
2. From the **Setup** menu, choose **View Settings**.

This setting specifies whether to display or hide the Reflection status bar.

**NOTE:** When the status bar is hidden, you cannot use the Reflection command line.

**Show Title Bar**

**Getting there**

1. Open a printer emulation session.
2. From the **Setup** menu, choose **View Settings**.

This setting specifies whether the title bar appears in display sessions.

**Startup Settings**

**Getting there**

1. Open a printer emulation session.
2. From the **Setup** menu, choose **View Settings**.

This read-only setting specifies the name of the startup settings file.
**Startup Working Directory**

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose **View Settings**.

This read-only setting specifies the working directory for the current session.

**Status Bar Text**

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose **View Settings**.

This setting specifies the string that appears in the status bar. Type shortcuts or text in the text box, up to 260 characters.

**Shortcut** | **Option**
---|---
&w | Attachmate
&r | Reflection
&f | Settings file name (or **Untitled** if a settings file is not open)
&s | Session type
&t | Transport
&h | Host name
&d | Date
&c | Connection status (whether you are connected and over what transport)
&p | Printer status (relevant only if the session type is IBM 5250 Printer or IBM 3270 Printer)
&x | Transfer status (the percentage complete of file and data transfers)
&v | Assigned device name (relevant only for 5250 sessions that use an assigned device name)
&l | Assigned LU name (relevant only for 3270 sessions that use an assigned LU name)
&o | Profile name
&& | A single ampersand

**Support 3270 Partitions**

Getting there

1. Open a printer emulation session.
2. From the Setup menu, choose **View Settings**.

This setting specifies whether to send the partition-related information from the terminal to the host in response to a host query request. Use this setting in 3270 sessions for host applications that are not designed to handle terminals that support partitions.
When set to Yes, the terminal includes partition-related information in its response to a host query request; when set to No (default), the terminal does not include partition-related information in its response to a host query request.

**NOTE:** You cannot change this setting during a connection.

### Support Asian Double-byte Features

**Getting there**

1. Open a printer emulation session.
2. From the **Setup** menu, choose **View Settings**.

This setting specifies whether support for double-byte features is enabled. Applies only to double-byte 3270 sessions.

### Telnet Average Keep Alive Roundtrip

**Getting there**

1. Open a printer emulation session.
2. From the **Setup** menu, choose **View Settings**.

This read-only setting displays the average amount of time Reflection has waited for a response to a Timing Mark Command.

### Telnet Encryption

**Getting there**

1. Open a printer emulation session.
2. From the **Setup** menu, choose **View Settings**.

**Telnet Encryption** configures Reflection to use Secure Sockets Layer/Transport Layer Security (SSL/TLS).

If **Telnet Encryption** is enabled, but your host does not support TLS, Reflection will attempt to use SSL instead. If your host supports neither SSL nor TLS, an error message appears when you try to connect, and your connection attempt will fail.

**NOTE:** Reflection does not support TLS client authentication.

### Telnet Encryption Disable CRL Checking

**Getting there**

1. Open a printer emulation session.
2. From the **Setup** menu, choose **View Settings**.

This setting specifies whether Reflection checks for certificate revocation when validating host certificates in SSL/TLS Telnet sessions.
NOTE: Disabling CRL checking increases your security risk.

Telnet Encryption Strength

Getting there
1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting specifies the encryption strength for Secure Sockets Layer/Transport Layer Security (SSL/TLS) data stream encryption. To configure this setting, you must enable "Telnet Encryption" on page 617.

When set to Default, the encryption strength is established by the host and Reflection during handshaking. If you set encryption strength to a specific value, the server must support this encryption level. If the server does not support this level, the connection is not established. If you are running in FIPS mode and select Default, Reflection negotiates using only FIPS-compliant encryption levels.

Telnet Encryption Use OCSP

Getting there
1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

When this setting is enabled, an Online Certificate Status Protocol (OCSP) responder checks the revocation status of digital certificates any time you try to establish a secure connection.

Telnet Encryption Verify Host Name

Getting there
1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting specifies the way Reflection handles SSL/TLS Telnet connections when the host name in the certificate does not match the host being contacted. When this setting is Yes (the default and recommended value) the host name in the certificate must match the host you are contacting.

This setting is only relevant if "Telnet Encryption" on page 617 is enabled.

Telnet Environment

Getting there
1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.
When you establish a 5250 terminal or printer session, specific information is sent to the AS/400 to configure your session. When you connect over Telnet, you can pass additional information at connect time as input to an Exit program on the AS/400. Use the Telnet Environment setting to send this additional information. Enter a string of up to 260 characters, using the following format:

keyword=value; keyword=value; keyword=value

**Using Telnet Environment with Auto SignOn**

When Auto SignOn is set to Yes, Reflection automatically signs on to the host using the current user name and password. You can set Telnet Environment to specify additional, non-default sign-on options using any of the following keywords in the Exit program string:

<table>
<thead>
<tr>
<th>This keyword</th>
<th>Sets</th>
<th>Equivalent Sign-on Menu Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBMPROGRAM</td>
<td>The program to call.</td>
<td>Program/procedure</td>
</tr>
<tr>
<td>IBMIMENU</td>
<td>The initial menu.</td>
<td>Menu</td>
</tr>
<tr>
<td>IBMCURLIB</td>
<td>The current library.</td>
<td>Current library</td>
</tr>
</tbody>
</table>

**NOTE:** Because this information is sent at the time you connect, you cannot change this setting while you are connected.

**Telnet Keep Alive Packets**

**Getting there**

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

By sending Keep Alive packets, you can learn about Telnet connection problems as they occur and avoid losing entered data. If you select None, no packets are sent and connection problems are communicated only when Reflection attempts to send data to the host.

**Telnet Keep Alive Timeout**

**Getting there**

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting determines the interval (in seconds) between the Keep Alive packets (requests) sent by Reflection.

**Telnet Location**

**Getting there**

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting specifies where the connection originated. Use this optional setting to provide information to the host from the PC. Usage conventions vary by site.
NOTE: You cannot change this value while you're connected to a gateway.

Telnet Port

Getting there

1 Open a printer emulation session.
2 From the Setup menu, choose View Settings.

Specifies the host port that the Telnet session should use. The default is 23.

Telnet Protocol

Getting there

1 Open a printer emulation session.
2 From the Setup menu, choose View Settings.

This read-only setting specifies the Telnet protocol that Reflection uses to communicate with the host. The value of this setting can change during a session. Following is a list of Telnet protocols:

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NVT</td>
<td>The Network Virtual Terminal protocol is in use.</td>
</tr>
<tr>
<td>TN3270</td>
<td>Standard TN3270 protocol is in use.</td>
</tr>
<tr>
<td>TN3270E</td>
<td>Extended TN3270 protocol (RFC 1647) is in use.</td>
</tr>
<tr>
<td>OCS</td>
<td>OCS Printing protocol (RFC 1646) is in use.</td>
</tr>
<tr>
<td>TN5250</td>
<td>Standard TN5250 protocol is in use.</td>
</tr>
</tbody>
</table>

Telnet Response Mode

Getting there

1 Open a printer emulation session.
2 From the Setup menu, choose View Settings.

This setting specifies whether the PC returns a message after it receives a message from the host. For improved performance, set this to No.

Telnet Use Reflection Security Proxy

Getting there

1 Open a printer emulation session.
2 From the Setup menu, choose View Settings.

When SSL/TLS security is enabled and this setting is Yes, Reflection makes secure SSL connections via the Reflection Security Proxy.
Telnet Use SOCKS Proxy Server

Getting there
1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting specifies whether to connect to a host through a SOCKS proxy server.

TN3270 Primary Same as Alt

Getting there
1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

Select this setting to use the same model type for both primary and alternate screen sizes. When selected, you can use a model type other than model 2 for primary screens.

TN3287 Connect Type

Getting there
1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting determines whether the selected LU name is paired with a specific printer device in 3270 sessions only.

Select Associate if the selected LU name is paired with a specific printer device; otherwise, select Connect (default) if the selected LU name is not paired with a specific printer device.

TN Association

Getting there
1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting identifies a 3270 terminal session on the host. Use this option to associate a 3270 terminal session with a specific 3270 printer session.

Related Topics
- “Associate a 3270 Printer Session with a Terminal Session” on page 527

Toolbar Mode

Getting there
1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.
This setting specifies whether the toolbar is attached to one of the margins of the terminal window and, if so, to which margin it is attached.

Choose from the following:

<table>
<thead>
<tr>
<th>This option</th>
<th>Attaches the toolbar to</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bottom Bar</td>
<td>The bottom margin of the terminal window.</td>
</tr>
<tr>
<td>Floating</td>
<td>N/A — the toolbar is free floating.</td>
</tr>
<tr>
<td>Left Bar</td>
<td>The left margin of the terminal window.</td>
</tr>
<tr>
<td>Right Bar</td>
<td>The right margin of the terminal window.</td>
</tr>
<tr>
<td>Top Bar (default)</td>
<td>The top margin of the terminal window.</td>
</tr>
</tbody>
</table>

**Toolbar Tether**

**Getting there**

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting specifies whether the toolbar location is tied to the terminal window location. This setting is applicable only if “Toolbar Mode” on page 621 is set to Floating.

When you set **Toolbar Tether** to Yes (default), the toolbar tracks the nearest corner of the terminal window, and moves if you move or resize the terminal window.

**Toolbar Visible**

**Getting there**

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting specifies whether the toolbar is visible.

**Trace Buffer Size (KB)**

**Getting there**

1. Open a printer emulation session.
2. From the Setup menu, choose View Settings.

This setting specifies whether Reflection uses a buffer when writing to a trace file, and if so, the size of that buffer (in kilobytes). By creating a trace buffer, you can speed up the trace. However, if Reflection shuts down unexpectedly, some trace data may not be written to the trace file.

When set to 0 (default), no buffer is used during tracing. Reflection opens the trace file, appends the data, and then closes the trace file for each trace record. When set to greater than zero, trace data is written first to the trace buffer and then copied to the trace file on disk when the buffer is full. The trace file is closed only after the trace is stopped.
NOTE: The buffer size is calculated after compression. This means that if Trace Buffer Size is set to 100 and "Trace Compression Type" on page 623 is set to use Huffman compression (default), approximately 200 KB of data will be transmitted before the data is written to the trace file.

Trace Compression Type

Getting there

1 Open a printer emulation session.
2 From the Setup menu, choose View Settings.

This setting specifies which compression, if any, is used when Reflection creates a trace file. Choose from Huffman (default), None, or Runlength.

Transport Name

Getting there

1 Open a printer emulation session.
2 From the Setup menu, choose View Settings.

This read-only setting specifies the transport currently selected in the Session Setup dialog box.

Use Internet Protocol Version 6

Getting there

1 Open a printer emulation session.
2 From the Setup menu, choose View Settings.

This setting specifies whether Reflection uses version 6 of the Internet Protocol.

Use Printer Fonts Only

Getting there

1 Open a printer emulation session.
2 From the Setup menu, choose View Settings.

This setting specifies whether Reflection prints host jobs using only resident fonts on the host printer.

Use Windows Crypto API

Getting there

1 Open a printer emulation session.
2 From the Setup menu, choose View Settings.

This setting specifies which cryptographic routines Reflection uses for secure SSL/TLS connections. Prior to version 13.0, Reflection used the routines in the Windows cryptographic library. Starting with version 13.0, Reflection installs and uses its own integrated cryptographic library by default.
When **Use Windows Crypto API** is set to Yes, Reflection uses the Windows cryptographic library. You might find this setting useful if you are troubleshooting SSL/TLS connections.

**NOTE:** You cannot specify Yes for this setting if you are running Reflection in FIPS mode.

**User Data Directory**

**Getting there**

1. Open a printer emulation session.
2. From the **Setup** menu, choose **View Settings**.

This setting specifies the folder where user-created files, like settings files and trace files, are saved by default.

**Version String**

**Getting there**

1. Open a printer emulation session.
2. From the **Setup** menu, choose **View Settings**.

This read-only setting shows the version information for your copy of Reflection.

**Workstation Customizing Object Library**

**Getting there**

1. Open a printer emulation session.
2. From the **Setup** menu, choose **View Settings**.

This setting specifies the library on the AS/400 that contains the Workstation Customizing Object.

**Workstation Customizing Object Name**

**Getting there**

1. Open a printer emulation session.
2. From the **Setup** menu, choose **View Settings**.

This setting specifies the Workstation Customizing Object on the AS/400 that contains information about the ASCII printer you use.
10 File and Data Transfer

**InfoConnect** supports the following methods for transferring information between your Windows computer and a host computer:

For IBM hosts:
- Mainframe file transfer is supported in 3270 sessions.
- AS/400 data transfer is supported in 5250 sessions.
- FTP file transfer is supported in both 3270 and 5250 sessions.

For VT hosts:
- A **InfoConnect** proprietary protocol, which you can use to transfer files between your PC and an HP 3000 (including Classic, MPE/iX, and POSIX), VMS (including OpenVMS and Alpha computers), ULTRIX, Unisys, Linux Console or UNIX system.
- A variety of public domain protocols, including FTP.

**InfoConnect** also includes a separate, fully featured FTP client application available from any host session or from the Windows Start menu.

In this Chapter
- “IBM File and Data Transfer” on page 625
- “VT File Transfer” on page 688
- “Reflection FTP Client” on page 741

**IBM File and Data Transfer**

**Index Term**
*Primary: transfer*  
*Secondary: overview*

**Index Term**
*Primary: file transfer*  
*Secondary: overview*

**InfoConnect** supports the following methods for transferring information between your Windows computer and a host computer:

- Mainframe file transfer is supported in 3270 sessions.
- AS/400 data transfer is supported in 5250 sessions.
- FTP file transfer is supported in both 3270 and 5250 sessions.

In this Section
- “Mainframe File Transfer” on page 626
- “AS/400 Transfer” on page 638
- “Configure File Transfer” on page 647
From the Transfer Settings dialog box, you can configure global transfer setup for the current session document. Any configuration you perform is saved with your session document.

From the Transfer dialog box, you can configure and perform specific transfers. In 3270 sessions, you must be connected to a host to open the Transfer dialog box. If you frequently repeat the same transfers, use transfer request files to save specific transfer information, including which files to transfer.

**NOTE:** InfoConnect uses the IND$FILE host program by default for mainframe transfers, except on double-byte systems, when "APVUFILE" on page 892 is used.

**Related Topics**

- "Send Files to a Mainframe" on page 627
- "Receive Files from a Mainframe" on page 629
- "Mainframe Transfer Method Options" on page 630
- "Transfer Settings Dialog Box" on page 648
- "Transfer Request Files" on page 681
- "Batch Transfers" on page 683
- "Use File Transfer Naming Templates" on page 632
Send Files to a Mainframe

NOTE: If the transfer is one you'll be performing regularly, you can save your transfer settings in a transfer request file.

To transfer files to a mainframe from your PC

1 Open the File Transfer dialog box.
   1a Start Reflection and log on to the host computer as usual.
   1b The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Reflection Ribbon</td>
<td>On the Session tab, from the Transfer group, click File Transfer.</td>
</tr>
<tr>
<td>The Reflection Browser</td>
<td>On the Reflection menu, choose Tools and then File Transfer.</td>
</tr>
<tr>
<td>TouchUx</td>
<td>Tap the Wrench icon and then under Tools, select File Transfer.</td>
</tr>
</tbody>
</table>

2 Click the Settings button, and configure the file transfer settings.
   For most situations, you can configure for file transfers by selecting a preset configuration in the Protocol tab.

3 Click OK.
4 From the Transfer dialog box, under Local, do one of the following:
   - Browse under Local folders, and then select one or more files from the list.
   - or-
   - Type the path and filename into the File names box.

5 Select your preferences for Transfer method, If file exists, and Record format.

6 Specify the host file information:

   For this host system      Do this

   CICS       Type a filename in the File names box.
               It is not possible to perform transfers involving multiple files.
               If you don't type a filename, InfoConnect uses the PC filename, with the
               period and extension, if applicable, removed. To avoid overwriting files,
               do not send files with the same filename and different extensions.

   CMS        Click Show host files, and browse to select one or more host files.
               -or-
               Type the file information into the File names box.
               If you don't type a filename, InfoConnect uses the PC filename. If a PC
               file you are transferring does not have a file extension, the transfer fails.

   TSO        Click Show host files, and browse to select one or more host files.
               All datasets that have a high-level qualifier that equals your user ID are
               displayed.
               -or-
               Type the file information into the File names box.
               If you don't type a filename, InfoConnect uses the PC filename.

7 To initiate a file transfer, do one of the following:
   - Click a Transfer button to move the file in the indicated direction.
   - or-
   - Drag the source file, and then drop it on the desired destination file.

Related Topics
   - “Receive Files from a Mainframe” on page 629
   - “Mainframe Transfer Method Options” on page 630
   - “Use File Transfer Naming Templates” on page 632
   - “Transfer Dialog Box” on page 679
   - “Transfer Settings Dialog Box” on page 648
   - “Mainframe File Transfer” on page 626
Receive Files from a Mainframe

NOTE: If the transfer is one you'll be performing regularly, you can save your transfer settings in a transfer request file.

To transfer files from a mainframe to the PC

1 Open the Transfer dialog box.
   1a Start Reflection and log on to the host computer as usual.
   1b The steps depend on your user interface mode (page 120).

   User Interface Mode   Steps
   ----------------------- ---------------------------
   The Reflection Ribbon  On the Session tab, from the Transfer group, click File Transfer.
   The Reflection Browser On the Reflection menu, choose Tools and then File Transfer.
   TouchUX               Tap the Wrench icon and then under Tools, select File Transfer.

2 Click the Settings button, and configure the file transfer settings.
   For most situations, you can configure for file transfers by selecting a preset configuration in the Protocol tab.

3 Click OK.

4 Specify a host file:
6 Select your preferences for **Transfer method**, **If file exists**, and **Record format**.

From the **Transfer** dialog box, under **Local**, do one of the following:

- Browse under **Local folders**, and then select one or more files from the list.
- Type the path and filename into the **File names** box.

If you omit this step, InfoConnect uses the host filename.

7 To initiate a file transfer, do one of the following:

- Click a **Transfer** button to move the file in the indicated direction.
- Drag the source file, and then drop it on the desired destination file.

**Related Topics**

- “Send Files to a Mainframe” on page 627
- “Mainframe Transfer Method Options” on page 630
- “Use File Transfer Naming Templates” on page 632
- “Transfer Dialog Box” on page 679
- “Transfer Settings Dialog Box” on page 648
- “Mainframe File Transfer” on page 626

**Mainframe Transfer Method Options**

<table>
<thead>
<tr>
<th>For this host system</th>
<th>Do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>CICS</td>
<td>Type a filename in the <strong>File names</strong> box. It is not possible to perform transfers involving multiple files.</td>
</tr>
</tbody>
</table>
| CMS                  | Click **Show host files**, and browse to select one or more host files. To filter the list, you can enter partial filenames or wildcards; for example, to see all files that begin with the letter "d" of the mode "files" on the "a" disk, type the following: `d* files a`
- or-
Type the file information into the **File names** box. |
| TSO                  | Click **Show host files**, and browse to select one or more host files. All datasets that have a high-level qualifier that equals your user ID are displayed.
- or-
Type the file information into the **File names** box. |
Use the Transfer method setting in the Transfer dialog box to specify how files are converted. The options available depend on the file transfer protocol you have selected. For mainframe transfers the options are:

**Binary**
Use for program files and other types of files that should not be translated, such as files that have already been formatted for a particular type of printer or files with application-specific formatting. Binary files contain non-printable characters; using this method, a file is not converted or translated during the transfer.

**ASCII**
Use to transfer text files with no special formatting.
ASCII files on the PC are translated to the EBCDIC character set on the host.

**JISCII**
Use for files that contain any double-byte characters with no special formatting. JISCII files are translated to the double-byte IBM host character set during transfer to the host.

**Related Topics**
- “Send Files to a Mainframe” on page 627
- “Receive Files from a Mainframe” on page 629
- “Transfer Dialog Box” on page 679
- “Mainframe File Transfer” on page 626
Use File Transfer Naming Templates

A file transfer template defines a set of conditions that affects the way InfoConnect names files transferred between your PC and a host. Whereas transfer request files are used to transfer the same file or set of files between your PC and a host, file transfer templates affect how files transferred between your PC and a host are named.

When activated, InfoConnect checks transfer templates in the specified order, and tries to match the transferring filename to template conditions. When a match is found, the matching template is applied.

InfoConnect installs some default templates, but you can also add your own, and specify the sort order (using the Move up and Move down buttons).

To activate file transfer templates

1 Open a 3270 terminal session.

2 Open the Transfer Settings Dialog Box.
   The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ribbon</td>
<td>On the Session ribbon, from the Transfer group, click the Transfer Settings launcher.</td>
</tr>
<tr>
<td>Reflection Browser</td>
<td>On the Reflection menu, choose Tools and then File Transfer. In the Transfer dialog box, click the Settings button.</td>
</tr>
<tr>
<td>TouchUx</td>
<td>Tap the Wrench icon and then under Tools, select File Transfer. In the Transfer dialog box, click the Settings button.</td>
</tr>
</tbody>
</table>

3 With Mainframe selected under Protocol, click the Templates tab.

4 Select Activate Transfer Templates.

5 Click OK.

Related Topics

- “Default File Transfer Templates” on page 635
- “Template Properties Dialog Box” on page 659
- “File Transfer Template Syntax” on page 636
- “Create a File Transfer Template” on page 632
- “Translation Tab (Transfer Settings Dialog Box)” on page 655
- “Transfer Request Files” on page 681
- “Mainframe File Transfer” on page 626

Create a File Transfer Template

Index Term
   Primary: transfer
   Secondary: templates
InfoConnect installs some default templates, but you can also add your own, and specify the sort order (using the Move up and Move down buttons).

To create a file transfer template

1. Open a 3270 terminal session.
2. Open the Transfer Settings Dialog Box.

   The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ribbon</td>
<td>On the Session ribbon, from the Transfer group, click the Transfer Settings launcher.</td>
</tr>
<tr>
<td>Reflection Browser</td>
<td>On the Reflection menu, choose Tools and then File Transfer. In the Transfer dialog box, click the Settings button.</td>
</tr>
<tr>
<td>TouchUx</td>
<td>Tap the Wrench icon and then under Tools, select File Transfer. In the Transfer dialog box, click the Settings button.</td>
</tr>
</tbody>
</table>

3. With Mainframe selected under Protocol, click the Templates tab.
4. Select Activate Transfer Templates.
5. Click New.
6. From the New Transfer Template dialog box, type a PC filename condition and a host filename condition, using file transfer template syntax.
7. Select your preferences for Transfer method, If file exists, and Record format.
8. (Optional) To test your new template, click the Test button.
9. Click OK.

Related Topics

- “File Transfer Template Syntax” on page 636
- “New Transfer Template Dialog Box” on page 658
- “Default File Transfer Templates” on page 635
Test a File Transfer Template

Index Term
Primary: test
Secondary: mainframe file transfer templates

Index Term
Primary: templates
Secondary: testing (mainframe file transfer)

You can access the Test Template dialog box from the New Transfer Template dialog box, or from the Templates tab of the Transfer Settings dialog box (with a template selected).

To test a file transfer template

1. Open a 3270 terminal session.
2. Open the Transfer Settings Dialog Box. The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ribbon</td>
<td>On the Session ribbon, from the Transfer group, click the Transfer Settings launcher.</td>
</tr>
<tr>
<td>Reflection Browser</td>
<td>On the Reflection menu, choose Tools and then File Transfer. In the Transfer dialog box, click the Settings button.</td>
</tr>
<tr>
<td>TouchUx</td>
<td>Tap the Wrench icon and then under Tools, select File Transfer. In the Transfer dialog box, click the Settings button.</td>
</tr>
</tbody>
</table>

3. With Mainframe selected under Protocol, click the Templates tab.
4. Select Activate Transfer Templates.
5. From the Templates list, select a template.
6. Click the Test button.
7. Type either a PC filename or a host filename to test.
8. Click one of the directional Test buttons to see how the filename will be affected by the transfer.
9. (Optional) To test your filename against all of the templates for a given host type, select Test all templates, select a host type, and then click one of the Test buttons.

Related Topics

- “Use File Transfer Naming Templates” on page 632
- “Create a File Transfer Template” on page 632
- “Test Template Dialog Box” on page 660
- “Templates Tab (Transfer Settings Dialog Box)” on page 656
- “New Transfer Template Dialog Box” on page 658
- “Mainframe File Transfer” on page 626
Default File Transfer Templates

InfoConnect installs some default templates, but you can also add your own, and specify the sort order (using the Move up and Move down buttons).

Templates

CMS, *.exe, *exebin a

- All PC files with the .exe extension transferred to the host are given the extension "exebin" and stored on the A disk (the base name remains unchanged). For example, R8win.exe on the PC becomes R8win exebin on the host.

- All host files on the A disk with the extension "exebin" transferred to the PC are given the .exe extension (the base name remains unchanged). For example, R8win exebin becomes R8win.exe on the PC.

CMS, *.txt, *text a

- All PC files with the .txt extension transferred to the host are given the extension "text" and stored on the A disk (the base name remains unchanged). For example, Test.txt on the PC becomes Test text on the host.

- All host files on the A disk with the extension "text" transferred to the PC are given the .txt extension (the base name remains unchanged). For example, Test text becomes Test.txt on the PC.

CMS, *.*, * a

- All host files transferred to the PC keep their base name and extension (with a dot added) and are transferred from the A disk on the host. For example, Test test becomes Test.txt on the PC.

This condition is valid only for files transferred from a host.

TSO, *.exe, bin.*

- All PC files with the .exe extension transferred to the host are prefixed with "bin." on the host (the base name remains unchanged). For example, Test.exe on the PC becomes Bin.test on the host.

- All host files prefixed with "bin." transferred to the PC are given the extension ".exe" (the base name remains unchanged). For example, Bin.test becomes Test.exe on the PC.

TSO, *.txt, text.*

- All PC files with the .txt extension transferred to the host are prefixed with "text." on the host (the base name remains unchanged). For example, Filename.txt on the PC becomes Text.filename on the host.

- All host files prefixed with "text." transferred to the PC are given the extension ".txt" (the base name remains unchanged). For example, Text.filename becomes Filename.txt on the PC.

CICS, *.*, *

- All PC files transferred to the host are stripped of their extension and retain just their base name. For example, Test.txt on the PC becomes Test on the host.

- All host files transferred to the PC are given a dot extension (the base name remains unchanged). For example Test becomes Test. on the PC.

Related Topics

- "File Transfer Template Syntax" on page 636
- "Create a File Transfer Template" on page 632
File Transfer Template Syntax

Use the following syntax to create conditions for file transfer templates:

* (asterisk)  This works like a standard PC wildcard for one or more filename characters.
.
(dot)  As in standard PC file naming, use to separate filenames from extensions.
=  Use in conjunction with the asterisk and the numerals 1-9 to identify the part of a filename you want to keep or strip out when transferring it.

For example, if a host filename has three parts, such as 1.2.3, and you want to keep just the second and third components of the filename when transferring it to your PC, you would use this condition:

* = 1.* = 2.* = 3  (host file) ---* = 2.* = 3  (PC file)

1-9  Use the numerals 1 through 9 in conjunction with the asterisk (*) and the equal sign (=) to identify the part of a filename you want to keep or strip out when transferring it.

For example, if a host filename has three parts, such as Test.Text.Demo, and you want to keep just the second and third components of the file name when transferring it to your PC, you would use this condition:

* = 1.* = 2.* = 3  (host file) ---* = 2.* = 3  (PC file)

which in this example would yield Text.Demo.

If a host filename has six parts and you want to keep the second and fifth parts when transferring it to your PC, the condition would be:

* = 1.* = 2.* = 3.* = 4.* = 5.* = 6  ---* = 2.* = 5

You can use up to eight numerals in a condition.

Related Topics

- “New Transfer Template Dialog Box” on page 658
- “Create a File Transfer Template” on page 632
- “Use File Transfer Naming Templates” on page 632
Send.exe and Receive.exe

Send.exe to send a file to your mainframe host from a DOS prompt. The syntax for Send.exe is identical to the syntax of the HLLAPI function Send File (90).

Before sending a file, you must be connected to the host and at a ready prompt.

To send a file to the host using Send.exe, type the following from the DOS prompt:

```
send pc_filename PresentationSpace_shortname: host_filename [IND$FILE options]
```

Receive.exe

Use Receive.exe to receive a file from your mainframe host from a DOS prompt. The syntax for Receive.exe is identical to the syntax of the HLLAPI function Receive File (91).

Before receiving a file you must be connected to the host and at a ready prompt.

To receive a file from the host using Receive.exe, type the following from the DOS prompt:

```
receive pc_filename PresentationSpace_shortname: host_filename [IND$FILE options]
```

Related Topics

- “Send Files to a Mainframe” on page 627
- “Receive Files from a Mainframe” on page 629
- “Mainframe File Transfer” on page 626

DBCS File Transfer Settings

DBCS File Transfer Settings with double-byte characters (DBCS) for User Mode (IBM) and SO.
The following table shows the effects that the DBCS file transfer settings NOSO, SO, and User Mode have on the characters SO (hex 0E), SI (hex 0F), RS (hex 1E) and US (hex 1F) when they appear in files sent to or received from the host.

<table>
<thead>
<tr>
<th>NOSO (Sending)</th>
<th>SO (Receiving)</th>
<th>User Mode (Receiving)</th>
<th>Effects on File</th>
</tr>
</thead>
<tbody>
<tr>
<td>Selected</td>
<td>n/a</td>
<td>n/a</td>
<td>RS/US (hex 1E and hex 1F) characters are removed when the PC file is sent to the host. SO/SI (hex 0E and hex 0F) characters are not sent to the host when a transition to or from single-byte to double-byte format is detected.</td>
</tr>
<tr>
<td>Cleared</td>
<td>n/a</td>
<td>n/a</td>
<td>RS/US (hex 1E and hex 1F) characters are converted to SO/SI (hex 0E and hex 0F), respectively when the file is sent to the host. SO/SI (hex 0E and hex 0F) characters are converted to NUL when the file is sent to the host. Note: This character translation can be edited using the 3270 Single-byte Translation Table Editor (Edit3270.exe).</td>
</tr>
<tr>
<td>n/a</td>
<td>Selected</td>
<td>Cleared</td>
<td>SO/SI (hex 0E and hex 0F) characters are converted to RS/US (hex 1E and hex 1F), respectively, when the host file is received.</td>
</tr>
<tr>
<td>n/a</td>
<td>Selected</td>
<td>Selected</td>
<td>SO/SI (hex 0E and hex 0F) characters are kept intact when the host file is received.</td>
</tr>
<tr>
<td>n/a</td>
<td>Cleared</td>
<td>Cleared</td>
<td>The host file is received from the host as is, with no changes.</td>
</tr>
<tr>
<td>n/a</td>
<td>Cleared</td>
<td>Selected</td>
<td>The host file is received from the host as is, with no changes.</td>
</tr>
</tbody>
</table>

Related Topics

- “CMS Advanced Options Dialog Box” on page 652
- “TSO Advanced Options Dialog Box” on page 653
- “CICS Advanced Options Dialog Box” on page 654

AS/400 Transfer

Index Term
Primary: transfer
Secondary: AS/400 transfer

Index Term
Primary: data transfer (AS/400)
Secondary: overview
From the **Transfer Settings** dialog box, you can configure global transfer setup for the current session document. For AS/400 transfer, InfoConnect creates a new connection to the host. If you don't want to be prompted each time you transfer files, you can save your user name and password information on the **AS/400** tab. Any configuration you perform is saved with your session document.

From the **Transfer** dialog box, you can configure and perform specific transfers. In 5250 sessions you don't need to be connected to a host to open this dialog box. If you frequently repeat the same transfers, use transfer request files to save specific transfer information, including which files to transfer.

A common way to receive data from an AS/400 is to collect only the data you need from one or more files in the host database. To do this you can create an SQL query. Query information can also be saved to a transfer request file.

**Related Topics**
- “Send Data to an AS/400” on page 639
- “Receive Data from an AS/400” on page 642
- “AS/400 Field Description Files” on page 641
- “Create an SQL Query” on page 644
- “Transfer Request Files” on page 681
- “Batch Transfers” on page 683

**Send Data to an AS/400**

**NOTE:** If the transfer is one you'll be performing regularly, you can save your transfer settings in a transfer request file.
To send data to an AS/400

1 Open the File Transfer dialog box.
   1a Start Reflection and log on to the host computer as usual.
   1b The steps depend on your user interface mode (page 120).

   **User Interface Mode** | **Steps**
   ------------------------|------------------
   The Reflection Ribbon   | On the Session tab, from the Transfer group, click File Transfer.
   The Reflection Browser  | On the Reflection menu, choose Tools and then File Transfer.
   TouchUX                | Tap the Wrench icon and then under Tools, select File Transfer.

2 Click the Settings button, and configure the file transfer settings.
3 From the AS/400, Options, and Translation tabs, specify the way you want InfoConnect to handle AS/400 transfers.
4 Click OK.
5 From the Transfer dialog box, under Local, do one of the following:
   - Browse under Local folders, and then select one or more files from the list.
   -or-
   - Type the path and filename into the File names box.
6 Under Host specify which host file should receive the data using one of the following techniques:
   - Click Show Host Files and browse to select a host file.
   -or-
   - Type the file information using this syntax: LIBRARY/FILE(MEMBER).

   **NOTE:** If InfoConnect is configured to use a character set that is not supported by your host, you cannot display host files using the Show host files button.

7 To initiate a file transfer, do one of the following:
   - Click a Transfer button to move the file in the indicated direction.
   -or-
   - Drag the source file, and then drop it on the desired destination file.

**Related Topics**
- “Drag-and-Drop Options for Sending to an AS/400” on page 641
- “AS/400 Field Description Files” on page 641
- “Transfer Dialog Box” on page 679
- “Transfer Settings Dialog Box” on page 648
- “Receive Data from an AS/400” on page 642
- “AS/400 Transfer” on page 638
Drag-and-Drop Options for Sending to an AS/400

From the Transfer dialog box, you can drag a PC file to a host library, a file, or a member (by clicking Settings, then from the Options tab, under To host, making sure that the value for Objects is appropriate).

Following are the possible scenarios:

- PC file to host library

<table>
<thead>
<tr>
<th>In the Objects box</th>
<th>This occurs</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you select Create File and Member</td>
<td>A new host file is created.</td>
</tr>
<tr>
<td>If you don't select Create File and Member, and a host file with the same name as the PC file already exists</td>
<td>You are asked whether you would like to overwrite the file.</td>
</tr>
<tr>
<td>If you don't select Create File and Member, and no host file of the same name as the PC file exists</td>
<td>You receive an error message, and the transfer fails.</td>
</tr>
</tbody>
</table>

- PC file to host file

<table>
<thead>
<tr>
<th>When you select, in the Objects box</th>
<th>This occurs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Member</td>
<td>A new member is created.</td>
</tr>
<tr>
<td>Replace Member (Confirm) or Replace Member (Don't Confirm)</td>
<td>The existing member of the same name as the PC file is overwritten.</td>
</tr>
<tr>
<td>If no member of the same name exists, you receive an error message, and the transfer fails.</td>
<td></td>
</tr>
</tbody>
</table>

- PC file to host member

<table>
<thead>
<tr>
<th>When you select, in the Objects box</th>
<th>This occurs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Replace Member (Confirm)</td>
<td>You are asked whether you would like to overwrite the existing member.</td>
</tr>
<tr>
<td>Replace Member (Don't Confirm)</td>
<td>The existing member is overwritten, without asking you to confirm the overwrite action.</td>
</tr>
</tbody>
</table>

Related Topics

- “Send Data to an AS/400” on page 639
- “Transfer Dialog Box” on page 679
- “AS/400 Transfer” on page 638

AS/400 Field Description Files

Index Term
Primary: field description file (AS/400)
A description file is a text file in ASCII format that contains descriptions of each field in a corresponding data file, which allows you to keep data in the intended format when sending data to the host. Field description files are created by default during data transfers to your PC.

The description file has the same name as the data file, except for the extension, which is `.FDF`. You’ll see its name in the Local file names box in the Transfer dialog box.

If the file you’re sending did not originate on the host, and has never been transferred to the host, you must create a description file before you can send a PC file to the host.

Your system administrator may have created a generic description file that resides on the host and can be downloaded, modified, and saved with a new name. (Check with your system administrator to see if this option is available.) Or, you can create your own description file. Refer to your AS/400 documentation for more information.

**Related Topics**

- “Send Data to an AS/400” on page 639
- “AS/400 Transfer” on page 638

### Receive Data from an AS/400

**NOTE:** If the transfer is one you’ll be performing regularly, you can save your transfer settings in a transfer request file.
To receive data from an AS/400

1 Open the File Transfer dialog box.
   1a Start Reflection and log on to the host computer as usual.
   1b The steps depend on your user interface mode (page 120).

   User Interface Mode          Steps
   The Reflection Ribbon         On the Session tab, from the Transfer group, click File Transfer.
   The Reflection Browser       On the Reflection menu, choose Tools and then File Transfer.
   TouchUx                       Tap the Wrench icon and then under Tools, select File Transfer.

2 Click the Settings button, and configure the file transfer settings.

3 From the AS/400, Options, and Translation tabs, specify the way you want InfoConnect to handle AS/400 transfers.

4 Click OK.

5 From the Transfer dialog box, under Host, specify the host file from which to receive data using one of the following techniques:
   • Click Show host files, and browse to select one or more host files. You can right-click on a file or member to view a brief description, if available. If the library containing the host file you need is not shown, click Add library and type the library name in the Add Library dialog box.
   -or-
   • Type the file information using this syntax: LIBRARY/FILE(MEMBER).

   NOTE: If InfoConnect is configured to use a character set that is not supported by your host, you cannot display host files using the Show host files button.

6 (Optional) To configure an SQL query, click Settings and from the SQL tab, build your query. Field information about the host file you selected becomes available when you select this tab.

7 From the Transfer dialog box, specify a local destination for the data.

   To send data to          Do this
   A file                  Specify a filename under Local.
                           If you don't specify a filename, InfoConnect uses the host filename.
   A display window        Click Settings, and then from the Options tab, set Output to to Display.
   A spreadsheet           Click Settings, and then from the Options tab, set Output to to Spreadsheet.
                           Data is saved to a .DIF file.

8 To initiate a file transfer, do one of the following:
   • Click a Transfer button to move the file in the indicated direction.
Drag-and-Drop Options for Receiving from an AS/400

From the Transfer dialog box, you can drag AS/400 host files to a listed PC file or to an item in Local folders. (First, make sure that the value for the If File Exists is appropriate.)

Following are the possible scenarios:

- Host file to Local folders box
  The first member of the selected host file is copied to the local folder on which it is dropped.
- Host file to PC file
  The first member of the selected host file is copied to the PC file on which it was dropped.
- Host member to Local folders box
  The selected member is copied to the folder on which it was dropped.
- Host member to PC file
  The selected member is copied to the selected PC file.

Related Topics

- “Receive Data from an AS/400” on page 642
- “Send Data to an AS/400” on page 639
- “AS/400 Transfer” on page 638

Create an SQL Query
A common way to receive data from an AS/400 is to collect only the data you need from one or more files in the host database; for example, to assemble a list of employee addresses and payroll information, you can collect and transfer only that information to a PC file or to your display, even if the information resides in different host files. You can also specify how to sort data or set conditions that determine which records are transferred. To do this, you would create an SQL query. If you need help building your SQL query, consult your SQL documentation.

To create an SQL query

1 Open the File Transfer dialog box.
   1a Start Reflection and log on to the host computer as usual.
   1b The steps depend on your user interface mode (page 120).

2 Click Show Host Files. (It may be necessary to enter your user name and password.)

3 Select one or more host files from which to transfer data.

4 Click Settings, and then click the SQL tab.
   The database options Select, Where, Order by, Group by, Having, and Join by appear as text boxes.

5 Do one of the following:
   - If you already know the syntax for the statement or clause, type it in the text box.
   - Or-
   - If you don't know how to create the statement or clause, click the arrow button to the right of the option, and then in the dialog box that opens, specify the field names, functions, operators, options and so on.
   The statement is automatically created from your selections.

   **NOTE:** If the transfer is one you'll be performing regularly, you can save your transfer settings in a transfer request file.

Related Topics

- “SQL Tab (Transfer Settings Dialog Box)” on page 668
- “Receive Data from an AS/400” on page 642
AS/400 Transfer Method Options

Index Term
Primary: transfer  
Secondary: AS/400 options

Index Term
Primary: Microsoft  
Secondary: Excel (file transfer)

Index Term
Primary: DOS random (AS/400 transfer method)

Index Term
Primary: DIF (AS/400 data conversion)

Index Term
Primary: data transfer (AS/400)  
Secondary: transfer methods

Index Term
Primary: CSV

Index Term
Primary: basic sequential transfer method

Index Term
Primary: ASCII  
Secondary: AS/400 data conversion

Index Term
Primary: AS/400 transfer  
Secondary: transfer methods

Index Term
Primary: AS/400 data conversion  
Secondary: tab delimited

Index Term
Primary: AS/400 data conversion  
Secondary: DOS random

Index Term
Primary: AS/400 data conversion  
Secondary: DIF

Index Term
Primary: AS/400 data conversion  
Secondary: CSV

Index Term
Primary: AS/400 data conversion  
Secondary: basic sequential
Use the **Transfer method** setting in the **Transfer** dialog box to specify how data in files is processed during transfers.

**NOTE:** This setting does not affect transfers to the host when you are using a description file to keep data in the intended format. InfoConnect uses description files by default. You can change this configuration from the **Options** tab of the **Transfer Settings** dialog box.

The options available depend on the file transfer protocol you have selected. For AS/400 transfers, the options are:

- **ASCII**
  - Use for files with no special formatting, and fixed record widths.

- **Basic Sequential**
  - Use to separate all fields with commas, and insert quotation marks around character and hexadecimal fields.

- **CSV**
  - Use to separate fields with commas, and insert quotation marks only around character fields that contain a comma or quotation mark.

- **DIF**
  - Use for files transferred to and from Microsoft Excel — DIF files contain the field names.

- **DOS Random**
  - Use for data transferred to and from the host from host database applications that require data to be in DOS Random format.

- **No Conversion**
  - Use for files that should not be translated — files transferred as No Conversion are not translated to the EBCDIC character set during a transfer to the host.

- **Tab Delimited**
  - Use to separate all fields with tabs, and insert quotation marks only around character fields that contain a quotation mark.

**Related Topics**

- “Receive Data from an AS/400” on page 642
- “AS/400 Transfer” on page 638

**Configure File Transfer**

You can manually configure file transfer settings in the **Transfer Settings** dialog box. Any configuration you perform is saved with your session document.

However, using the automated preset configurations is recommended.
To configure file transfer

1 Open the File Transfer dialog box.
   
   1a Start Reflection and log on to the host computer as usual.
   
   1b The steps depend on your user interface mode (page 120).

   User Interface Mode                      Steps
   The Reflection Ribbon                    On the Session tab, from the Transfer group, click File Transfer.
   The Reflection Browser                   On the Reflection menu, choose Tools and then File Transfer.
   TouchUx                                  Tap the Wrench icon and then under Tools, select File Transfer.

2 Click the Settings button, and configure the file transfer settings.
   For most situations, you can configure for file transfers by selecting a preset configuration in the Protocol tab.

Related Topics

- “Transfer Settings Dialog Box” on page 648

Transfer Settings Dialog Box

Configure transfer protocol and translation options for file and data transfers. Any configuration you perform is saved with your session document. The tabs displayed depend on your current configuration, and the way you accessed this dialog box.
Protocol (page 649)
Available in all session types. Use this tab to select a transfer protocol.

Mainframe (page 650)
Available in 3270 sessions when Mainframe is the selected protocol. Use this tab to configure transfer protocol options when you're transferring to or from an IBM mainframe.

Translation (page 655)
Available in all sessions when Mainframe or AS/400 is the selected protocol. Use this tab to specify how filenames are handled during transfers.

Templates (page 656)
Available in 3270 sessions when Mainframe is the selected protocol. Use this tab to map PC filename patterns to filename patterns on the mainframe.

AS/400 (page 661)
Available in all sessions when AS/400 is the selected protocol. Use this tab to configure transfer protocol connection options for transfers to and from an AS/400.

Options (page 666)
Available in all sessions when AS/400 is the selected protocol. Use this tab to configure the way InfoConnect handles data transfer.

SQL (page 668)
Available when AS/400 is the selected protocol, and you open the Transfer Settings dialog box by clicking the Settings button in the Transfer dialog box. Use this tab to create SQL queries for extracting data from AS/400 files.

FTP (page 676)
Available in both 3270 and 5250 sessions.

Related Topics
- “IBM File and Data Transfer” on page 625
- “Transfer Dialog Box” on page 679

Protocol Tab (Transfer Settings Dialog Box)

Index Term
Primary: transfer settings
Secondary: Protocol tab

Index Term
Primary: Protocol tab (Transfer Settings, IBM)

Index Term
Primary: preset configurations
Secondary: IBM file transfer

Getting there
1. Open the Transfer Settings dialog box.
The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ribbon</td>
<td>On the Session ribbon, from the Transfer group, click the Transfer Settings launcher.</td>
</tr>
<tr>
<td>Reflection Browser</td>
<td>On the Reflection menu, choose Tools and then File Transfer. In the Transfer dialog box, click the Settings button.</td>
</tr>
<tr>
<td>TouchUx</td>
<td>Tap the Wrench icon and then under Tools, select File Transfer. In the Transfer dialog box, click the Settings button.</td>
</tr>
</tbody>
</table>

The protocol you select determines which preset configurations are available. Also, the tabs available from the Transfer Settings dialog box change to enable you to configure transfers using the selected protocol.

**Protocol**

Select the file transfer protocol you want to use.

**Preset configurations**

Selecting an item from this list adjusts the appropriate values automatically in the Transfer Settings dialog box for that specific environment.

**Related Topics**

- “Transfer Settings Dialog Box” on page 648

**Mainframe Tab (Transfer Settings Dialog Box)**

**Index Term**

Primary: transfer settings
Secondary: Mainframe tab

**Index Term**

Primary: timeout
Secondary: mainframe transfer settings

**Index Term**

Primary: structured field transfer

**Index Term**

Primary: startup command (mainframe transfer)

**Index Term**

Primary: mainframe file transfer
Secondary: transfer settings

**Index Term**

Primary: IND$FILE transfer
Secondary: transfer settings

**Getting there**

1. Open a 3270 terminal session.
   
The steps depend on your user interface mode (page 120).
With Mainframe selected under Protocol, click the Mainframe tab. The options are:

**Host**

- **System**
  - Select the operating system the host is running.

- **Startup command**
  - Type the name of the host program to be issued by InfoConnect to initiate a file transfer. The default value, IND$FILE, is appropriate for CMS and TSO hosts.

  For CICS hosts, IND$FILE may be appropriate, or you may need to specify your site’s CICS transaction (for example, CFTR).

  When working with double-byte characters, use “APVUFILE” on page 892.

- **Advanced**
  - Configure advanced options for the selected host system type (CICS, CMS, or TSO).

**Structured field transfer**

- **Max field size**
  - Select a buffer value (other than Disabled) to have InfoConnect use the Write Structured Field protocol. As a rule, the larger the buffer size, the faster the transfer. However, if you select a value that is too large for your host, it will disconnect your session when you first attempt to send a file big enough to fill the buffer.

  This option is relevant for IND$FILE, “APVUFILE” on page 892 and DISOSS transfers.

**Timeout (in seconds)**

- **Startup**
  - Set the amount of time InfoConnect should wait for a host response when attempting to connect. Select a value between 1-9999.

- **Response**
  - Set the amount of time InfoConnect should wait for a host response. Select a value between 1-9999.

**Related Topics**

- “Mainframe File Transfer” on page 626
CMS Advanced Options Dialog Box

Index Term
Primary: CMS
Secondary: CMS Advanced Options dialog box

Getting there
1 Open a 3270 terminal session.
   The steps depend on your user interface mode (page 120).

   User Interface Mode        Steps
   Ribbon                       On the Session ribbon, from the Transfer group, click the Transfer Settings launcher:
   InfoConnect Browser         On the InfoConnect menu, choose Tools and then File Transfer. In the Transfer dialog box, click the Settings button.
   TouchUx                      Tap the Wrench icon and then under Tools, select File Transfer. In the Transfer dialog box, click the Settings button.

2 With Mainframe selected under Protocol, click the Mainframe tab.
3 Under Host, from the System list, select CMS.
4 Click the Advanced button.

The options are:

  Logical record length       Type the record size (in bytes) for the file being created on the host. If you leave this box blank, the record size is determined by the host. Use a value between 0 and 32768 to accommodate the range accepted by your host.

  For ASCII files, set this value to accommodate the longest line in your file. When you leave this box blank, the host typically accepts lines of up to 80 characters.

  CR/LF processing
  When you select one of these options, a carriage return character and a linefeed character are stripped from the end of each line of the file you are sending.
  CR/LF processing is typically appropriate for ASCII and JISCII files but not for binary files; the defaults for these options are set up accordingly.

  Additional IND$FILE parameters
  Use this text box for any parameters specific to the IND$FILE (or APVUFILE) program on your host system. The contents of this text box are appended to the end of the transfer command generated by InfoConnect. InfoConnect does not check the contents of this text box for validity.

  For a description of the NOSO, SO, and User Mode settings, see the "DBCS File Transfer Settings" on page 637 topic.

Related Topics
* "DBCS File Transfer Settings" on page 637
• “Mainframe Tab (Transfer Settings Dialog Box)” on page 650
• “Mainframe File Transfer” on page 626

**TSO Advanced Options Dialog Box**

**Index Term**
Primary: TSO
Secondary: TSO Advanced Options dialog box

**Index Term**
Primary: block allocation
Secondary: TSO advanced options

**Getting there**

1. Open a 3270 terminal session.
   The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ribbon</td>
<td>On the <strong>Session</strong> ribbon, from the <strong>Transfer</strong> group, click the <strong>Transfer Settings</strong> launcher:</td>
</tr>
<tr>
<td><strong>InfoConnect</strong> Browser</td>
<td>On the <strong>InfoConnect</strong> menu, choose <strong>Tools</strong> and then <strong>File Transfer</strong>. In the Transfer dialog box, click the <strong>Settings</strong> button.</td>
</tr>
<tr>
<td><strong>TouchUx</strong></td>
<td>Tap the Wrench icon and then under <strong>Tools</strong>, select <strong>File Transfer</strong>. In the Transfer dialog box, click the <strong>Settings</strong> button.</td>
</tr>
</tbody>
</table>

2. With **Mainframe** selected under **Protocol**, click the **Mainframe** tab.
3. Under **Host**, from the **System** list, select **TSO**.
4. Click the **Advanced** button.

The options are:

**Dataset options**

**Logical record length**
Type the record size (in bytes) for the file being created on the host. If you leave this box blank, the record size is determined by the host. Use a value between 0 and 32768 to accommodate the range accepted by your host.

For ASCII files, set this value to accommodate the longest line in your file. When you leave this box blank, the host typically accepts lines of up to 80 characters.

**Block size**
Type the block size (in bytes) for the file being created on the host. For files with fixed-length records, this value must be a multiple of the **Logical record length** (because blocks are divided into logical records).

Use a value between 0 and 32768 to accommodate the range accepted by your host.
Space allocation

**Allocation units**  Select the disk subdivisions for your primary and secondary space allocations. If you select Default, the unit is determined by the host. If you select Block, use the Average block box to set the size for an average block.

**Average block**  Type the size (in bytes) for an average block. This value is only relevant if you are using blocks as your allocation unit.

**Primary**  Type the size (in allocation units) of the primary allocation for the host file being created.

**Secondary**  Type the size of any additional allocations (in allocation units) in the event that the primary allocation is not sufficient. Multiple secondary allocations (known as "extents") are allowed, up to a host-specified limit (generally 15).

CR/LF processing

When you select one of these options, a carriage return character and a linefeed character are stripped from the end of each line of the file you are sending.

CR/LF processing is typically appropriate for ASCII and JISCII files but not for binary files; the defaults for these options are set up accordingly.

**Additional IND$FILE parameters**  Use this text box for any parameters specific to the IND$FILE (or APVUFILE) program on your host system. The contents of this text box are appended to the end of the transfer command generated by InfoConnect. InfoConnect does not check the contents of this text box for validity.

For a description of the NOSO, SO, and User Mode settings, see the "DBCS File Transfer Settings" on page 637 topic.

Related Topics

- "DBCS File Transfer Settings" on page 637
- "Mainframe Tab (Transfer Settings Dialog Box)" on page 650
- "Mainframe File Transfer" on page 626

CICS Advanced Options Dialog Box

Index Term
Primary: CICS
Secondary: CICS Advanced Options dialog box

Getting there

1. Open a 3270 terminal session.
   The steps depend on your user interface mode (page 120).
2 With **Mainframe** selected under **Protocol**, click the **Mainframe** tab.
3 Under **Host**, from the **System** list, select **CICS**.
4 Click the **Advanced** button.

The options are:

**CR/LF processing**

When you select one of these options, a carriage return character and a linefeed character are stripped from the end of each line of the file you are sending.

CR/LF processing is typically appropriate for ASCII and JISCII files but not for binary files; the defaults for these options are set up accordingly.

**Additional IND$FILE parameters**

Use this text box for any parameters specific to the IND$FILE (or APVUFILE) program on your host system. The contents of this text box are appended to the end of the transfer command generated by InfoConnect. InfoConnect does not check the contents of this text box for validity.

For a description of the **NOSO**, **SO**, and **User Mode** settings, see the "**DBCS File Transfer Settings**" on page 637 topic.

**Related Topics**

- "**DBCS File Transfer Settings**" on page 637
- "**Mainframe Tab (Transfer Settings Dialog Box)**" on page 650
- "**Mainframe File Transfer**" on page 626

**Translation Tab (Transfer Settings Dialog Box)**
The steps depend on your user interface mode (page 120).

### User Interface Mode

#### Ribbon
- On the Session ribbon, from the Transfer group, click the Transfer Settings launcher.

#### Reflection Browser
- On the Reflection menu, choose Tools and then File Transfer.
- In the Transfer dialog box, click the Settings button.

#### TouchUx
- Tap the Wrench icon and then under Tools, select File Transfer. In the Transfer dialog box, click the Settings button.

The options are:

### Filename translation options

- **Change spaces to underscores when sending**
  - Select to convert spaces in filenames to underscores in files sent to the host. If your host does not support spaces in filenames, this prevents the host from modifying the filename or rejecting the transfer.

- **Change underscores to spaces when receiving**
  - Select to convert underscores in filenames to spaces in files received from the host.
  - By selecting this option in conjunction with the Change spaces to underscores when sending option, you satisfy the conventions of both the PC and the host, yet maintain the appearance of an unchanged file name: The name change occurs, but is transparent to both the PC and the host.

- **Truncate received filenames to 8.3 format**
  - Select to receive host files in the DOS 8.3 filename format.
  - For example, a file with the name `Longfilename.Document` will be converted automatically to `Longfile.doc` when transferred to your PC.

- **Display 8.3 filenames as**
  - Select how you want filenames conforming to the DOS 8.3 file naming convention to display under Local in the Transfer dialog box.

### Related Topics
- “IBM File and Data Transfer” on page 625

### Templates Tab (Transfer Settings Dialog Box)

#### Index Term
- Primary: templates
- Secondary: Templates Tab (Transfer Settings)

#### Getting there
- 1. Open a 3270 terminal session.
   - The steps depend on your user interface mode (page 120).
With **Mainframe** selected under **Protocol**, click the **Templates** tab.

File transfer templates are available when the transfer protocol is set to Mainframe. These templates define a set of conditions that affect the way **InfoConnect** names files transferred between your Windows computer and a host. Unlike transfer request files, which are used to transfer the same file or set of files between your computer and a host, file transfer templates affect the how all files transferred between your computer and the host are named. You can create multiple conditions for **InfoConnect** to step through until it finds the first one that is applicable.

With file transfer templates, for example, you can send all local files with the extension .EXE to the host, and give them the extension .EXEC.

**Activate transfer templates**
Select to enable file transfer templates for all files transferred to or received from the host. When selected, **InfoConnect** steps through the list of file transfer templates to find a matching condition each time you transfer a file to or from the host.

**Templates**
Lists the templates that have been defined.

**New**
Add a new template to the list.

**Remove**
Remove the selected template.

**Properties**
View and edit the properties of the selected template.

**Test**
Open the **Test Template** dialog box, from which you can test how **InfoConnect** handles sample filename conditions without actually having to transfer a file.

**Move up**
Move the selected item in the list.

**Move down**
Move the selected item in the list.

**Related Topics**
- “Default File Transfer Templates” on page 635
- “Use File Transfer Naming Templates” on page 632
- “Mainframe File Transfer” on page 626
- “Transfer Request Files” on page 681
New Transfer Template Dialog Box

Getting there

1 Open a 3270 terminal session.
2 Open the Transfer Settings Dialog Box.
   The steps depend on your user interface mode (page 120)
   
<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ribbon</td>
<td>On the Session ribbon, from the Transfer group, click the Transfer Settings launcher.</td>
</tr>
<tr>
<td>Reflection Browser</td>
<td>On the Reflection menu, choose Tools and then File Transfer. In the Transfer dialog box, click the Settings button.</td>
</tr>
<tr>
<td>TouchUX</td>
<td>Tap the Wrench icon and then under Tools, select File Transfer. In the Transfer dialog box, click the Settings button.</td>
</tr>
</tbody>
</table>

3 With Mainframe selected under Protocol, click the Templates tab.
4 Select Activate Transfer Templates.
5 Click New.

The options are:

PC file name Type the PC filename parameters. This condition is used for files transferred to and from the host.

Host file name Type the host filename parameters. This condition is used for files transferred to and from the host.

Host type Select the operating system the host is running.

Transfer type When you perform a file transfer, it defaults to the transfer type you select from this list.

If file exists Select what to do when the transferred file already exists in the target location.

Record format Select the record format to use for transfers to the host:

<table>
<thead>
<tr>
<th>Select</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fixed</td>
<td>Force the host to create fixed-length records.</td>
</tr>
<tr>
<td>Undefined</td>
<td>Force the host to create files without a specific record format (this value is only relevant for TSO systems).</td>
</tr>
<tr>
<td>Variable</td>
<td>Force the host to create variable-length records and preserve the format of a binary file.</td>
</tr>
</tbody>
</table>
Template Properties Dialog Box

Getting there

1 Open a 3270 terminal session.

2 Open the Transfer Settings Dialog Box.
   The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ribbon</td>
<td>On the Session ribbon, from the Transfer group, click the Transfer Settings launcher.</td>
</tr>
<tr>
<td>Reflection Browser</td>
<td>On the Reflection menu, choose Tools and then File Transfer. In the Transfer dialog box, click the Settings button.</td>
</tr>
<tr>
<td>TouchUx</td>
<td>Tap the Wrench icon and then under Tools, select File Transfer. In the Transfer dialog box, click the Settings button.</td>
</tr>
</tbody>
</table>

3 With Mainframe selected under Protocol, click the Templates tab.

4 Select Activate Transfer Templates.

5 From the Templates list, select a template.

6 Click the Properties button.

The options are:

- **PC file name**: Type the PC filename parameters. This condition is used for files transferred to and from the host.

- **Host file name**: Type the host filename parameters. This condition is used for files transferred to and from the host.

- **Host type**: Select the operating system the host is running.

Related Topics

- “File Transfer Template Syntax” on page 636
- “Create a File Transfer Template” on page 632
- “Test a File Transfer Template” on page 634
- “Use File Transfer Naming Templates” on page 632
- “Templates Tab (Transfer Settings Dialog Box)” on page 656
- “Mainframe File Transfer” on page 626
## Test Template Dialog Box

### Getting there

1. Open a 3270 terminal session.

2. Open the Transfer Settings Dialog Box.

   The steps depend on your user interface mode (page 120).

### Transfer type

When you perform a file transfer, it defaults to the transfer type you select from this list.

### If file exists

Select what to do when the transferred file already exists in the target location.

### Record format

Select the record format to use for transfers to the host:

<table>
<thead>
<tr>
<th>Select</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fixed</td>
<td>Force the host to create fixed-length records.</td>
</tr>
<tr>
<td>Undefined</td>
<td>Force the host to create files without a specific record format (this value is only relevant for TSO systems).</td>
</tr>
<tr>
<td>Variable</td>
<td>Force the host to create variable-length records and preserve the format of a binary file.</td>
</tr>
<tr>
<td>Default</td>
<td>Let the host determine the record format.</td>
</tr>
</tbody>
</table>

### Advanced

Configure advanced options for the selected host system type (CICS, CMS, or TSO).

### Test

Open the Test Template dialog box, from which you can test how InfoConnect handles sample filename conditions without actually having to transfer a file.

### Related Topics

- “File Transfer Template Syntax” on page 636
- “Create a File Transfer Template” on page 632
- “Test a File Transfer Template” on page 634
- “Use File Transfer Naming Templates” on page 632
- “Templates Tab (Transfer Settings Dialog Box)” on page 656
- “Mainframe File Transfer” on page 626
With **Mainframe** selected under **Protocol**, click the **Templates** tab.

Select **Activate Transfer Templates**.

From the **Templates** list, select a template.

Click the **Test** button.

The options are:

- **PC file name**: Type the PC filename parameters. This condition is used for files transferred to and from the host.
- **Host file name**: Type the host filename parameters. This condition is used for files transferred to and from the host.
- **Test all templates**: Select to perform a test using all the currently defined conditions for the selected host type. When more than one condition is defined, **InfoConnect** steps through them in the order they appear in the **Templates** list.
- **Host Type**: Select the host type for which you want to test all templates.

**Related Topics**

- “Test a File Transfer Template” on page 634
- “File Transfer Template Syntax” on page 636
- “Create a File Transfer Template” on page 632
- “Use File Transfer Naming Templates” on page 632
- “Mainframe File Transfer” on page 626

**AS/400 Tab (Transfer Settings Dialog Box)**
Getting there

1. Open a 3270 or 5250 terminal session.
   The steps depend on your user interface mode (page 120).

   **User Interface Mode**  
   **Steps**
   
   **Ribbon**
   On the Session ribbon, from the Transfer group, click the Transfer Settings launcher.

   **InfoConnect Browser**
   On the InfoConnect menu, choose Tools and then File Transfer. In the Transfer dialog box, click the Settings button.

   **TouchUx**
   Tap the Wrench icon and then under Tools, select File Transfer. In the Transfer dialog box, click the Settings button.

   2. From the Protocol list, select **AS/400**.

   3. Click the **AS/400** tab.
The options are:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transport</td>
<td>TCP/IP is the only supported transfer type.</td>
</tr>
<tr>
<td>Host TP</td>
<td>Select an AS/400 data transfer transaction program to use. <strong>LIPI</strong> supports more complex SQL statements.</td>
</tr>
<tr>
<td>National character set</td>
<td>Select a character set to use for character translations during AS/400 data transfers.</td>
</tr>
<tr>
<td>PC characters</td>
<td>Select a character set. This option is relevant for data that contains characters with decimal values above 127. (ANSI and ASCII character sets have the same values for characters with decimal values from 32 – 126.)</td>
</tr>
<tr>
<td>System name</td>
<td>Type the host name to use for AS/400 data transfers. If you are connected to a host, this value identifies that host and can’t be changed. To transfer files to and from a different host, use an unconnected session.</td>
</tr>
<tr>
<td>Username</td>
<td>Type your username for the AS/400 Sign On screen, to bypass being prompted for it before performing a data transfer.</td>
</tr>
<tr>
<td>Password</td>
<td>Type your password for the AS/400 Sign On screen, to bypass being prompted for it before performing a data transfer.</td>
</tr>
<tr>
<td>Advanced</td>
<td>Configure advanced TCP/IP options.</td>
</tr>
<tr>
<td>Fields</td>
<td>Set format options for the database fields you receive from the host.  Adam Adam.</td>
</tr>
<tr>
<td>Security</td>
<td>Secure data communications with SOCKS or SSL/TLS.</td>
</tr>
</tbody>
</table>

**Timeout (in seconds)**

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Startup</td>
<td>Set the amount of time <strong>InfoConnect</strong> should wait for a host response when attempting to connect. Select a value between 1-9999.</td>
</tr>
<tr>
<td>Response</td>
<td>Set the amount of time <strong>InfoConnect</strong> should wait for a host response. Select a value between 1-9999.</td>
</tr>
</tbody>
</table>

**Related Topics**

- “AS/400 Transfer” on page 638
- “Database Field Options Dialog Box” on page 664

**Advanced TCP/IP Dialog Box**

**Getting there**

1. Open a 3270 or 5250 terminal session. The steps depend on your user interface mode (page 120).
From the Protocol list, select AS/400.

3 Click the AS/400 tab.

4 Click the Advanced button.

The options are:

- **IP address**: Type the host system address here if you do not have a Hosts file, and your system name does not have an IP address entry in the Domain Name Server for which your TCP/IP stack is configured.

- **Use default ports**: Clear this check box to allow InfoConnect to communicate with host transaction programs using non-standard port numbers.

## Related Topics

- “AS/400 Tab (Transfer Settings Dialog Box)” on page 661
- “AS/400 Transfer” on page 638

## Database Field Options Dialog Box

Index Term
Primary: time format (AS/400 transfer)

Index Term
Primary: sort sequence (AS/400 transfer)

Index Term
Primary: date format (AS/400 transfer)

Index Term
Primary: Database Field Options (AS/400 transfer)

Index Term
Primary: data transfer (AS/400)
Secondary: database field options

Index Term
Primary: AS/400 transfer
Secondary: database field options

### Getting there

1 Open a 3270 or 5250 terminal session.
   
   The steps depend on your user interface mode (page 120).
<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ribbon</td>
<td>On the <strong>Session</strong> ribbon, from the <strong>Transfer</strong> group, click the <strong>Transfer Settings</strong> launcher: <img src="image" alt="Transfer Settings" /></td>
</tr>
<tr>
<td>InfoConnect Browser</td>
<td>On the <strong>InfoConnect</strong> menu, choose <strong>Tools</strong> and then <strong>File Transfer</strong>. In the Transfer dialog box, click the <strong>Settings</strong> button.</td>
</tr>
<tr>
<td>TouchUx</td>
<td>Tap the Wrench icon and then under <strong>Tools</strong>, select <strong>File Transfer</strong>. In the Transfer dialog box, click the <strong>Settings</strong> button.</td>
</tr>
</tbody>
</table>

2. From the **Protocol** list, select **AS/400**.
3. Click the **AS/400** tab.
4. Click the **Fields** button.

Set format options for the database fields you receive from the host.

**Time**

<table>
<thead>
<tr>
<th>Time Format</th>
<th>Select the time format for selected fields with an AS/400 field type of Time. The options are:</th>
</tr>
</thead>
<tbody>
<tr>
<td>DDS</td>
<td>Format given by AS/400 file attribute.</td>
</tr>
<tr>
<td>DFT</td>
<td>AS/400 job default (default).</td>
</tr>
<tr>
<td>EUR</td>
<td>IBM European standard (hh.mm.ss).</td>
</tr>
<tr>
<td>HMS</td>
<td>Hour, minute, second (hh:mm:ss).</td>
</tr>
<tr>
<td>ISO</td>
<td>International Standards Organization (hh.mm.ss).</td>
</tr>
<tr>
<td>JIS</td>
<td>Japanese Industrial Standard (hh:mm:ss).</td>
</tr>
<tr>
<td>USA</td>
<td>USA standard (hh:mm AM or PM).</td>
</tr>
</tbody>
</table>

**Time Separator**

Select a character to use as a time separator in selected fields having an AS/400 field type of Time.

**Date**

<table>
<thead>
<tr>
<th>Date Format</th>
<th>Select the date format for selected fields having an AS/400 field type of Date. The options are:</th>
</tr>
</thead>
<tbody>
<tr>
<td>DDS</td>
<td>Format given by AS/400 file attribute.</td>
</tr>
<tr>
<td>DFT</td>
<td>AS/400 job default (default).</td>
</tr>
<tr>
<td>DMY</td>
<td>Day, month, year (dd/mm/yy)</td>
</tr>
<tr>
<td>EUR</td>
<td>IBM European standard (dd.mm.yyyy).</td>
</tr>
<tr>
<td>ISO</td>
<td>International Standards Organization (yyyy/mm/dd).</td>
</tr>
<tr>
<td>JIS</td>
<td>Japanese Industrial Standard (yyyy-mm-dd).</td>
</tr>
<tr>
<td>JULIAN</td>
<td>(yy/ddd)</td>
</tr>
<tr>
<td>MDY</td>
<td>Month, day, year (mm/dd/yy).</td>
</tr>
</tbody>
</table>
USA standard (mm/dd/yyyy).
YMD Year, month, day (yy/mm/dd).

**Date Separator**
Select a character to use as a date separator in selected fields having an AS/400 field type of Date.

**Ignore decimal data errors**
Select to ignore any decimal data errors found in a packed or zoned field during the transfer from the AS/400. Ignoring these errors speeds up the transfer process.

**Decimal separator**
Select the character to use as a decimal separator in selected fields that have an AS/400 field type of packed decimal or zoned decimal.

**Sort sequence**
Select a sort sequence for the data being transferred. This sequence determines the order of characters in the alphabet when fields are alphabetized. The sort sequence also affects any comparisons based on characters in the fields. The options are:

- *HEX Uses the EBCDIC hexadecimal sort sequence.
- *JOB Uses the AS/400 job default.
- *LANGIDSHR Uses a shared weight table.
- *LANGIDUNQ Uses a unique weight table.

**Related Topics**
- “AS/400 Tab (Transfer Settings Dialog Box)” on page 661
- “AS/400 Transfer” on page 638

## Options Tab (Transfer Settings Dialog Box)

### Index Term
Primary: transfer settings
Secondary: Options tab

### Index Term
Primary: reference file (AS/400 transfer)

### Getting there

1. Open a 3270 or 5250 terminal session.
   The steps depend on your user interface mode (page 120).

   **User Interface Mode**
   **Steps**
   - **Ribbon**
     On the Session ribbon, from the Transfer group, click the Transfer Settings launcher:
   - **InfoConnect Browser**
     On the InfoConnect menu, choose Tools and then File Transfer. In the Transfer dialog box, click the Settings button.
   - **TouchUx**
     Tap the Wrench icon and then under Tools, select File Transfer. In the Transfer dialog box, click the Settings button.

2. From the Protocol list, select **AS/400**.
3. Click the **Options** tab.
From host

Save description
Select to save description files associated with files you receive from the host. Description files are only relevant when you are receiving data output to a file, rather than to your display.

Description file
Type a description filename. By default, InfoConnect creates a description file that has the same name as its corresponding data file, but with an .FDF extension.

Show transfer progress
Select to display a progress bar during transfers from the host. Transfers take less time when this check box is cleared because the AS/400 does not have to count the number of selected records before transferring them.

Delete trailing spaces (ASCII only)
Select to remove extra spaces at the end of a record when the data is received.

Output to
Select where to direct received data. Use Display to display data in the Query Results window. Use Spreadsheet to save data to a .DIF file.

To host

Use description file
Select to use description files with files you receive from the host.

Description file
Type a description filename. By default, InfoConnect creates a description file that has the same name as its corresponding data file, but with an .FDF extension.

Objects
Select whether data is transferred to a new or existing member on the AS/400.

Select  To
Create File And Member  Create a new member within a new host file. To use this option, specify a host library in the Transfer dialog box.

Create Member  Create a new member within an existing host file.

Replace Member (Confirm)  Send data to an existing member in an existing file and prompt for confirmation of the overwrite action.

Replace Member (Don’t Confirm)  Send data to an existing member in an existing file without being prompted to confirm the overwrite action.

File type
If you are creating a file on the host, select the type of file to create.

If you aren't using a description file, this setting will be determined by host defaults.

Authority
Set permissions for the new host file.

File text
Describe the new host file.

Member text
Describe the new member.

Record length
Select the record size (in bytes) for the new host file. This setting is unavailable if you are using a description file.
Reference file

Specify a reference file to use for the file you are sending. The new host file is created using the field names in the description file and the definitions of the fields in the reference file.

The syntax for specifying a reference file is:

\[\text{library_name/}\text{filename}\]

Related Topics

- “AS/400 Field Description Files” on page 641
- “AS/400 Transfer” on page 638

SQL Tab (Transfer Settings Dialog Box)

Index Term
Primary: Where (AS/400 transfer)

Index Term
Primary: transfer settings
Secondary: SQL tab

Index Term
Primary: SQL transfer settings (AS/400)

Index Term
Primary: Select (AS/400 transfer)

Index Term
Primary: Order by (AS/400 transfer)

Index Term
Primary: Join by (AS/400 transfer)

Index Term
Primary: Having (AS/400 transfer)

Index Term
Primary: Group by (AS/400 transfer)

Index Term
Primary: AS/400 transfer
Secondary: SQL tab (Transfer Settings)

Getting there

1 Open the Transfer Dialog box.
   The steps depend on your user interface mode (page 120).

User Interface Mode | Steps
--- | ---
The Reflection Ribbon | On the Session tab, from the Transfer group, click File Transfer.
The Reflection Browser | On the Reflection menu, choose Tools and then File Transfer.
TouchUx | Tap the Wrench icon and then under Tools, select File Transfer.
If you are running a 3270 session, change the protocol to AS/400.

2a Click Settings.
2b From the Protocol list, select AS/400.
2c Click OK.

3 Click Show Host Files. (It may be necessary to enter your user name and password.)

4 Select one or more host files from which to transfer data.

5 Click Settings.
6 From the Transfer Settings dialog box, click the SQL tab.

7 Open the dialog box by clicking the arrow next to the field (for example, to open the Select dialog box, click the arrow button for the Select box).

Use this tab to create SQL queries for extracting data from AS/400 files. Type text directly into the text boxes, or click any of the buttons on the right to open a dialog box to build a query.

**NOTE:** From the Transfer dialog box, select at least one host file before you build your query. InfoConnect displays field information from the specified file to help you build the query.

If you need help building your SQL query, consult your SQL documentation.

- **Select**
  - Start building your SELECT statement by specifying fields (or columns) to transfer.

- **Where**
  - In this box, add a WHERE clause to your SELECT statement. Specify one or more conditions that must be met for a record to be transferred.

- **Order by**
  - In this box, add an ORDER BY clause to your SELECT statement to sort the records resulting from the query. You can sort only by fields specified in your SELECT statement.

- **Group by**
  - In this box, add a GROUP BY clause to your SELECT statement to specify how to group the resulting data after the requested calculation (function) is performed.
    - This clause is necessary when a function and multiple fields are specified in your SELECT statement.

- **Having**
  - In this box, add a HAVING clause to apply a condition to a function of the SELECT statement.
    - To enable the Having box and dialog box, you must first add a GROUP BY clause.

- **Join by**
  - In this box, add a JOIN clause to your SELECT statement to specify how you want data from multiple files or members combined.
    - To enable the Join by box and dialog box, you must have selected multiple files or members on the Host side of the Transfer dialog box.

- **Return records with missing fields**
  - When joining records from more than one file, there may be cases where a record cannot be found to complete the join.

**Related Topics**

- “Create an SQL Query” on page 644
Select Dialog Box

Getting there

1. Open the Transfer Dialog box.
   The steps depend on your user interface mode (page 120).

   **User Interface Mode** | **Steps**
   -------------------------|-----------------------------------------------
   The Reflection Ribbon   | On the **Session** tab, from the **Transfer** group, click File Transfer.
   The Reflection Browser  | On the Reflection menu, choose **Tools** and then File Transfer.
   TouchUX                 | Tap the Wrench icon and then under **Tools**, select File Transfer.

2. If you are running a 3270 session, change the protocol to AS/400:
   2a Click **Settings**.
   2b From the **Protocol** list, select AS/400.
   2c Click **OK**.

3. Click **Show Host Files**. (It may be necessary to enter your user name and password.)

4. Select one or more host files from which to transfer data.

5. Click **Settings**.

6. From the **Transfer Settings** dialog box, click the **SQL** tab.

7. Open the dialog box by clicking the arrow next to the field (for example, to open the Select dialog box, click the arrow button for the **Select** box).

Type directly into the statement box, or use the lists and buttons to build your SQL query.

**Finished statement**
Start building your **SELECT** statement by specifying fields (or columns) to transfer.

If you don't enter anything, all fields will be transferred.

**Functions**
Use these SQL functions to perform calculations on fields.

**Fields**
This box displays the fields in the selected file(s). For more information about a field, hover your mouse over the field name.

**Related Topics**

- “Create an SQL Query” on page 644
- “SQL Tab (Transfer Settings Dialog Box)” on page 668

Where Dialog Box

Getting there

1. Open the Transfer Dialog box
The steps depend on your user interface mode (page 120).

### User Interface Mode

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Reflection Ribbon</td>
<td>On the Session tab, from the Transfer group, click File Transfer.</td>
</tr>
<tr>
<td>The Reflection Browser</td>
<td>On the Reflection menu, choose Tools and then File Transfer.</td>
</tr>
<tr>
<td>TouchUX</td>
<td>Tap the Wrench icon and then under Tools, select File Transfer.</td>
</tr>
</tbody>
</table>

2 If you are running a 3270 session, change the protocol to AS/400.
   2a Click **Settings**.
   2b From the **Protocol** list, select **AS/400**.
   2c Click **OK**.

3 Click **Show Host Files**. (It may be necessary to enter your user name and password.)

4 Select one or more host files from which to transfer data.

5 Click **Settings**.

6 From the **Transfer Settings** dialog box, click the **SQL** tab.

7 Open the dialog box by clicking the arrow next to the field (for example, to open the Select dialog box, click the arrow button for the **Select** box).

Type directly into the statement box, or use the lists and buttons to build your SQL query.

- **Finished statement**
  - In this box, add a **WHERE** clause to your **SELECT** statement. Specify one or more conditions that must be met for a record to be transferred.

- **Fields**
  - This box displays the fields in the selected file(s). For more information about a field, hover your mouse over the field name.

- **Value**
  - Type a value to test against as part of your condition.

### Related Topics

- “Create an SQL Query” on page 644
- “SQL Tab (Transfer Settings Dialog Box)” on page 668

### Order By Dialog Box

#### Getting there

1 Open the Transfer Dialog box.
   The steps depend on your user interface mode (page 120).
If you are running a 3270 session, change the protocol to AS/400:

2a Click **Settings**.
2b From the **Protocol** list, select **AS/400**.
2c Click **OK**.

3 Click **Show Host Files**. (It may be necessary to enter your user name and password.)

4 Select one or more host files from which to transfer data.

5 Click **Settings**.

6 From the **Transfer Settings** dialog box, click the **SQL** tab.

7 Open the dialog box by clicking the arrow next to the field (for example, to open the *Select* dialog box, click the arrow button for the *Select* box).

Type directly into the statement box, or use the lists and buttons to build your SQL query.

**Finished statement**

In this box, add an `ORDER BY` clause to your `SELECT` statement to sort the records resulting from the query. You can sort only by fields specified in your `SELECT` statement.

**Functions**

Use these SQL functions to perform calculations on fields.

**Fields**

This box displays the fields in the selected file(s). For more information about a field, hover your mouse over the field name.

**Related Topics**

- “Create an SQL Query” on page 644
- “SQL Tab (Transfer Settings Dialog Box)” on page 668

**Group By Dialog Box**

**Getting there**

1 Open the Transfer Dialog box.

   The steps depend on your **user interface mode** (page 120).
If you are running a 3270 session, change the protocol to AS/400:

2a Click **Settings**.

2b From the **Protocol** list, select **AS/400**.

2c Click **OK**.

3 Click **Show Host Files**. (It may be necessary to enter your user name and password.)

4 Select one or more host files from which to transfer data.

5 Click **Settings**.

6 From the **Transfer Settings** dialog box, click the **SQL** tab.

7 Open the dialog box by clicking the arrow next to the field (for example, to open the Select dialog box, click the arrow button for the **Select** box).

Type directly into the statement box, or use the lists and buttons to build your SQL query.

**Finished statement**

In this box, add a `GROUP BY` clause to your `SELECT` statement to specify how to group the resulting data after the requested calculation (function) is performed.

This clause is necessary when a function and multiple fields are specified in your `SELECT` statement.

**Fields**

This box displays the fields in the selected file(s). For more information about a field, hover your mouse over the field name.

**Related Topics**

- “Create an SQL Query” on page 644
- “SQL Tab (Transfer Settings Dialog Box)” on page 668

**Having Dialog Box**

**Getting there**

1 Open the Transfer Dialog box.

The steps depend on your user interface mode (page 120).
### User Interface Mode

<table>
<thead>
<tr>
<th>The Reflection Ribbon</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>On the Session tab, from the Transfer group, click File Transfer.</td>
</tr>
<tr>
<td>The Reflection Browser</td>
<td>On the Reflection menu, choose Tools and then File Transfer.</td>
</tr>
<tr>
<td>TouchUX</td>
<td>Tap the Wrench icon and then under Tools, select File Transfer.</td>
</tr>
</tbody>
</table>

2 If you are running a 3270 session, change the protocol to AS/400.
   2a Click Settings.
   2b From the Protocol list, select AS/400.
   2c Click OK.

3 Click Show Host Files. (It may be necessary to enter your user name and password.)

4 Select one or more host files from which to transfer data.

5 Click Settings.

6 From the Transfer Settings dialog box, click the SQL tab.

7 Open the dialog box by clicking the arrow next to the field (for example, to open the Select dialog box, click the arrow button for the Select box).

Type directly into the statement box, or use the lists and buttons to build your SQL query.

**Finished statement**

In this box, add a HAVING clause to apply a condition to a function of the SELECT statement.

**Functions**

Use these SQL functions to perform calculations on fields.

**Fields**

This box displays the fields in the selected file(s). For more information about a field, hover your mouse over the field name.

**Value**

Type a value to test against as part of your condition.

**Related Topics**

- “Create an SQL Query” on page 644
- “SQL Tab (Transfer Settings Dialog Box)” on page 668

### Join By Dialog Box

**Getting there**

1 Open the Transfer Dialog box.
   The steps depend on your user interface mode (page 120).
If you are running a 3270 session, change the protocol to AS/400.

2a Click Settings.
2b From the Protocol list, select AS/400.
2c Click OK.

3 Click Show Host Files. (It may be necessary to enter your user name and password.)

4 Select one or more host files from which to transfer data.

5 Click Settings.

6 From the Transfer Settings dialog box, click the SQL tab.

7 Open the dialog box by clicking the arrow next to the field (for example, to open the Select dialog box, click the arrow button for the Select box).

Type directly into the Joins box, or use the lists and buttons to build your SQL query.

Joins
In this box, add a JOIN clause to your SELECT statement to specify how you want data from multiple files or members combined.

Fields
This box displays the fields in the selected file(s). For more information about a field, hover your mouse over the field name.

Tables
This box displays the files or members selected on the Host side of the Transfer dialog box.

Related Topics
- “Create an SQL Query” on page 644
- “SQL Tab (Transfer Settings Dialog Box)” on page 668

FTP Tab (Transfer Settings Dialog Box)

Index Term
Primary: passwords
Secondary: integrated FTP (IBM)

Index Term
Primary: anonymous logins
Secondary: IBM file transfer setting

Getting there
1 Open a 3270 or 5250 terminal session.
   The steps depend on your user interface mode (page 120).
2. From the **Protocol** list, select **FTP**.

3. Click the **FTP** tab.

   The options are:

<table>
<thead>
<tr>
<th><strong>Host name or IP address</strong></th>
<th>Type the name or IP address of the FTP server to log on to.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Anonymous</strong></td>
<td>Log on to the FTP server as a guest, with the user name <em>anonymous</em>.</td>
</tr>
<tr>
<td><strong>Save password</strong></td>
<td>Select to save your password in encrypted form in your session document file. (Passwords for anonymous connections are not encrypted). If you prefer not to store information about your password in your session file, clear this check box. If the password was previously saved, it is removed.</td>
</tr>
<tr>
<td><strong>User name</strong></td>
<td>Type your user name on the FTP server.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Type the password the FTP server associates with the user name. When the <strong>Anonymous</strong> check box is selected, a password appears in plain text, instead of asterisks (*), as you type it. If no password is expected, click <strong>OK</strong> to continue.</td>
</tr>
</tbody>
</table>

   Advanced
   Click to open the **FTP Properties** dialog box, from which you can configure additional FTP transfer features.

   Defaults
   Sets all FTP settings to the defaults, including the settings you configure using the **Advanced** button.

**Related Topics**

- “Use Integrated FTP Transfer” on page 677
- “Transferring Files with FTP” on page 676

**Transferring Files with FTP**
You can perform FTP file transfer from a terminal session using InfoConnect integrated FTP support, or you can launch the FTP Client.

With InfoConnect FTP, you can connect to an FTP server running on any supported host. Once connected, FTP is used to transfer files between your PC and the FTP server.

Related Topics

- “Use Integrated FTP Transfer” on page 677
- “Launch the FTP Client from a Terminal Session” on page 678
- “Introducing Reflection FTP Client” on page 741

Use Integrated FTP Transfer

Index Term
Primary: FTP
Secondary: within a terminal session

Integrated FTP transfer is available when you want to use the FTP protocol from within a terminal session.

NOTE: If the transfer is one you'll be performing regularly, you can save your transfer settings in a transfer request file.

To transfer files using the FTP protocol from within a terminal session

1 Open the File Transfer dialog box.
   1a Start Reflection and log on to the host computer as usual.
   1b The steps depend on your user interface mode (page 120).

   User Interface Mode | Steps
   ---------------------|-----------------------------------------------
   The Reflection Ribbon| On the Session tab, from the Transfer group, click File Transfer.
   The Reflection Browser| On the Reflection menu, choose Tools and then File Transfer.
   TouchUx              | Tap the Wrench icon and then under Tools, select File Transfer.

2 Click the Settings button, and configure the file transfer settings.
   For most situations, you can configure for file transfers by selecting a preset configuration in the Protocol tab.
3 From the Protocol list, select FTP.
4 Click the FTP tab, and configure the host and user name information.
   This doesn't have to be the host you're logged on to.
5 (Optional) Click Advanced to configure additional FTP settings.
6 Click OK.
7 From the Transfer dialog box, under Local, do one of the following:
   - Browse under Local folders, and then select one or more files from the list.
-or-
  - Type the path and filename into the **File names** box.

8 Under **Host** specify a host file using one of the following techniques:
  - Click **Show host files**, and browse to select one or more host files.
- or-
  - Type the file information into the **File names** box.

**NOTE:** If InfoConnect is configured to use a character set that is not supported by your host, you cannot display host files using the **Show host files** button.

9 To initiate a file transfer, do one of the following:
  - Click a **Transfer** button to move the file in the indicated direction.
- or-
  - Drag the source file, and then drop it on the desired destination file.

Related Topics
  - “Transferring Files with FTP” on page 676
  - “Launch the FTP Client from a Terminal Session” on page 678

**Launch the FTP Client from a Terminal Session**

You can launch the FTP Client from the Windows Start menu or from an InfoConnect terminal session.

To launch the FTP Client from a terminal session
  - Open FTP Client as follows:
    - The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ribbon</td>
<td>On the <strong>Session</strong> tab, from the <strong>Transfer</strong> group, click <strong>FTP Client</strong>.</td>
</tr>
<tr>
<td>InfoConnect Browser</td>
<td>On the <strong>InfoConnect</strong> menu, choose <strong>Tools</strong> and then <strong>FTP Client</strong>.</td>
</tr>
<tr>
<td>TouchUx</td>
<td>On the <strong>InfoConnect</strong> menu, tap the Wrench icon, and then select <strong>FTP Client</strong>.</td>
</tr>
</tbody>
</table>

Related Topics
  - “Introducing Reflection FTP Client” on page 741
  - “Transferring Files with FTP” on page 676
  - “Use Integrated FTP Transfer” on page 677
Transfer Dialog Box

Index Term
Primary: TSO
Secondary: dataset level

Index Term
Primary: transfer
Secondary: Transfer dialog box (IBM sessions)

Index Term
Primary: record format
Secondary: IBM hosts

Index Term
Primary: IND$FILE transfer
Secondary: Transfer dialog box (IBM sessions)

Index Term
Primary: file transfer
Secondary: Transfer dialog box (IBM sessions)

Index Term
Primary: dataset level, TSO

Getting there
Start Reflection and log on to the host computer as usual.
The steps depend on your user interface mode (page 120).

User Interface Mode         Steps
The Reflection Ribbon        On the Session tab, from the Transfer group, click File Transfer.
The Reflection Browser       On the Reflection menu, choose Tools and then File Transfer.
TouchUX                      Tap the Wrench icon and then under Tools, select File Transfer.

The options are:
Local

File names
Type the path and filename of the file you want to transfer. Separate multiple filenames with commas. Standard PC wildcard characters are supported.

Local Folders
Browse for the folder containing the file or files you want to transfer.

Transfer

Transfer
Click a transfer button to move the file(s) in the indicated direction.

Transfer method
Select how data conversion should be handled. The options available depend on the file transfer protocol. For additional information, see "AS/400 Transfer Method Options" on page 646 and "Mainframe Transfer Method Options" on page 630.
If file exists  
Select what to do when the transferred file already exists in the target location.

Record format  
Select the record format to use for transfers to the host:
- **Select** To
  - **Fixed**  
    Force the host to create fixed-length records.
  - **Undefined**  
    Force the host to create files without a specific record format (this value is only relevant for TSO systems).
  - **Variable**  
    Force the host to create variable-length records and preserve the format of a binary file.
  - **Default**  
    Let the host determine the record format.

Settings
Click the **Settings** button, and configure the file transfer settings.

Transfer Request
Choose one of the following:
- **Select** To
  - **Open**  
    Load transfer settings that you have saved to a transfer request file.
  - **Save**  
    Save your current transfer configuration to a transfer request file.

Host

File names
Type or select one or more host files for the transfer. Separate multiple filenames with commas.

Show Host Files
Click to display host files in a tree view. The display you see depends on the protocol you have selected. InfoConnect displays only those files that can be transferred using the currently selected transfer protocol.

In 5250 sessions, when you click **Show Host Files** you are prompted for user name and password, unless you have configured these values from the AS/400 tab of the Transfer Settings dialog box.

**Show Host Files** is not available if you are transferring to and from a CICS host.

Refresh
Click to refresh the file list. This button appears in place of the **Show host files** button after you have displayed the host files.

Add Library
Click to view an additional library (you will need to provide the library name). This button appears only if you are connected to an AS/400 host, and you have displayed the host files.

Level
Click to open the New Level dialog box, where you can specify the high-level qualifier or qualifications (or filter) of the host files to display.

**NOTE:** This button appears only if you have configured File Transfer for a TSO host and you have displayed the host files.

If you enter a filter that is a subset of the files in the current view, only the files matching the filter are displayed. If the filter is not a subset of the files in the current view, the files matching the filter are added to the view.
Related Topics
- “AS/400 Transfer” on page 638
- “Mainframe File Transfer” on page 626
- “Transfer Dialog Box (VT)” on page 702
- “Transferring Files with FTP” on page 676

Saving and Repeating Transfers

If you perform the same transfers frequently, you can use transfer request files to save your transfer information. You can save information about single transfers or batch transfers.

Related Topics
- “Transfer Request Files” on page 681
- “Create a Transfer Request File” on page 681
- “Open a Transfer Request File” on page 682
- “Batch Transfers” on page 683
- “Save a Batch Transfer” on page 684

Transfer Request Files

Using transfer request files, you can perform the same transfer (or transfers) again later, without having to specify files and options each time. You can save transfer request files using either the Single or Batch tab of the Transfer dialog box.

NOTE: When you save a transfer request file from the Batch tab, InfoConnect stores the direction of transfer for each saved transfer. Therefore, you might want to use the Batch tab to save your transfer configuration, even if you have transferred only one file. When you save transfer request files from the Single tab, the direction of transfer is not included in the transfer request file.

Related Topics
- “Create a Transfer Request File” on page 681
- “Open a Transfer Request File” on page 682
- “Batch Transfers” on page 683

Create a Transfer Request File
To create a transfer request file

1 Open the File Transfer dialog box.
   1a Start Reflection and log on to the host computer as usual.
   1b The steps depend on your user interface mode (page 120).

2 From the Transfer dialog box, configure and perform the transfer you want to save.

3 Under Transfer request, click Save.

4 In the File name box, type a filename.

5 In the Transfer list, specify whether data is being sent to the PC from the host, or from the host to the PC.
   This setting is not saved with the transfer request file.

6 Click Save.
   In 5250 sessions, transfer request files use the extension .XTO; in 3270 sessions, transfer request files use the extension .MTO.

**NOTE:** When you save a transfer request file from the Batch tab, InfoConnect stores the direction of transfer for each saved transfer. Therefore, you might want to use the Batch tab to save your transfer configuration, even if you have transferred only one file. When you save transfer request files from the Single tab, the direction of transfer is not included in the transfer request file.

**Related Topics**

- “Open a Transfer Request File” on page 682
- "Batch Transfers" on page 683

**Open a Transfer Request File**
When you open a transfer request file, you load the options previously saved to that file. To use saved transfer request files, first open the Transfer dialog box. You can load transfer requests from either the Single tab or the Batch tab.

**NOTE:** In 5250 sessions, transfer request files use the extension .XTO; in 3270 sessions, transfer request files use the extension .MTO.

---

### To open a transfer request file

1. **Open the Transfer dialog box.**
   1a. Start Reflection and log on to the host computer as usual.
   1b. The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Reflection Ribbon</td>
<td>On the Session tab, from the Transfer group, click File Transfer.</td>
</tr>
<tr>
<td>The Reflection Browser</td>
<td>On the Reflection menu, choose Tools and then File Transfer.</td>
</tr>
<tr>
<td>TouchUx</td>
<td>Tap the Wrench icon and then under Tools, select File Transfer.</td>
</tr>
</tbody>
</table>

2. From the Transfer dialog box (either tab), under Transfer request, click Open.
3. Select the transfer request file you want to open.
4. Click Open.
5. To initiate a file transfer, do one of the following:
   - Click a Transfer button to move the file in the indicated direction.
   - Drag the source file, and then drop it on the desired destination file.

---

### Related Topics

- “Create a Transfer Request File” on page 681

---

### Batch Transfers

**Index Term**
- Primary: transfer
- Secondary: batch transfers

**Index Term**
- Primary: batch transfers
- Secondary: overview

**Index Term**
- Primary: batch transfers
- Secondary: data transfer (AS/400)

**Index Term**
- Primary: batch transfers
- Secondary: AS/400 transfer
If you routinely perform a group of transfer operations, you can create and save a list of transfers from the Batch tab of the Transfer dialog box. Your transfer information is saved to a transfer request file. You can then use the transfer request file to perform multiple transfers in a single operation.

Related Topics

- “Save a Batch Transfer” on page 684
- “Run a Batch Transfer” on page 685
- “Batch Tab (Transfer Dialog Box)” on page 686
- “Batch Wizard” on page 687
- “Transfer Request Files” on page 681

Save a Batch Transfer

Using batch transfers, you can save a series of transfer operations to a single transfer request file. You can use this file later to repeat the same set of transfers.

**NOTE:** When you add an item to a batch, all aspects of the file transfer configuration are saved independently for each item, including file names, transfer direction, SQL query information, and any other transfer settings you have configured.
To create a batch transfer request file

1 Open the File Transfer dialog box.
   1a Start Reflection and log on to the host computer as usual.
   1b The steps depend on your user interface mode (page 120).

2 Click the Settings button, and configure the file transfer settings.

3 Perform the series of transfers that you want to save to the batch.
   Successful transfers are automatically added to the batch list on the Batch tab.

   **NOTE:** If you prefer to configure transfers to be saved without actually transferring data, you can use the Batch wizard to add transfers to the batch list.

4 Click the Batch tab.

   You can use this tab to modify individual items on the list, to add or delete items, and to change the order in which transfers occur when you run the saved file.

5 Click Save.

6 In the File name box, type a filename.

7 Click Save.

Related Topics

- “Batch Transfers” on page 683
- “Run a Batch Transfer” on page 685
- “Batch Wizard” on page 687

Run a Batch Transfer

Index Term
Primary: running
Secondary: batch transfer (IBM)

Index Term
Primary: batch transfers
Secondary: running in 5250 sessions
Open the File Transfer dialog box.

1a Start Reflection and log on to the host computer as usual.
1b The steps depend on your user interface mode (page 120).

2 Click the Batch tab.

3 Click Open, select a transfer request file and click Open.

In 5250 sessions, transfer request files use the extension .XTO; in 3270 sessions, transfer request files use the extension .MTO.

NOTE: By default, all items are transferred each time you run a batch request. If there are individual items you don’t want to transfer this time, clear the check box to the left of the filename.

4 Click Run.

Batch Tab (Transfer Dialog Box)

Getting there

Start InfoConnect and log on to the host computer as usual.

The steps depend on your user interface mode (page 120).

User Interface Mode | Steps
---|---
The Reflection Ribbon | On the Session tab, from the Transfer group, click File Transfer.
The Reflection Browser | On the Reflection menu, choose Tools and then File Transfer.
touchUx | Tap the Wrench icon and then under Tools, select File Transfer.

From the Batch tab, you can save file transfers for future use. InfoConnect saves batch transfers to transfer request files, and automatically adds successful transfers to the Transfer list on the Batch tab. You can also add file transfers using the Batch wizard.
Run
Perform all of the selected transfers in the list, starting at the top.

Add
Use the Batch wizard to add items to the list.

Remove
Delete the selected transfer.

Properties
Use the Batch wizard to view or modify the selected transfer. Changes you make using the Batch wizard affect the currently selected transfer only.

Move up
Move the selected item in the list.

Move down
Move the selected item in the list.

Open
Use the Open Transfer Request File dialog box to import transfers from an existing file.

NOTE: Opening a transfer request file will replace any items currently in your list of transfers. Use the Add button to append additional items and keep the items in your current list.

Save
Save the items in your transfer list to a transfer request file.

Related Topics
- “Batch Transfers” on page 683

Batch Wizard

Index Term
Primary: test
Secondary: batch transfers

Index Term
Primary: Batch wizard (IBM data transfer)

Index Term
Primary: batch transfers
Secondary: Batch wizard (IBM data transfer)

Getting there

1 Open a 3270 or 5250 terminal session.
   The steps depend on your user interface mode (page 120).

   User Interface Mode
   Steps
   The InfoConnect Ribbon
   On the Session tab, from the Transfer group, click File Transfer.
   The InfoConnect Browser
   On the InfoConnect menu, choose Tools and then File Transfer.

   TouchUx
   Tap the Wrench icon and then under Tools, select File Transfer.

2 Click the Batch tab.
3 Click the Add button.

Use the Batch wizard to add new items to a batch transfer.
NOTE: InfoConnect automatically adds file transfers to your batch list when you transfer files from the Single tab of the Transfer dialog box. Adding items this way may suit your needs better than using the Batch wizard. The Batch wizard is useful when you want to add transfers to a batch without actually performing the transfer.

Add a new single transfer to batch
Use this option to configure a new transfer for the batch list. Click Next to configure the transfer using the Batch Wizard transfer panel (described below).

Host name
Specify the host to use for this transfer. If you are connected, this must be the host to which you are currently connected.

Transfer type
Select the file transfer protocol you want to use.

Add transfers from an existing batch file
Use this option to import transfers that you have already saved to a transfer request file. Transfers in the saved file are appended to the end of the current list.

Batch file name
Type path and filename of the transfer request file containing the transfer(s) you want to add to the batch.

Batch Wizard Transfer Panel
Use this panel to configure a transfer in your batch list. The Batch Wizard panel is similar to the Single tab of the Transfer dialog box, but has the following differences:

- Changes you make using the Batch Wizard panel affect only the item you are adding or modifying in the batch list; these changes have no affect on subsequent transfers and are not saved when you save your settings file.
- In the Batch wizard, you set the transfer direction by clicking Send or Receive. Your choice is indicated by the direction of the blue arrow at the top of the panel. No transfer actually occurs.
- The Batch Wizard panel includes a Test button that performs the currently configured transfer.

Related Topics
- “Batch Transfers” on page 683
- “Transfer Dialog Box” on page 679

VT File Transfer

Index Term
Primary: VT
Secondary: file transfer

Index Term
Primary: transfer
Secondary: VT

Index Term
Primary: file transfer
Secondary: VT

You can transfer files in InfoConnect using the File Transfer command from the Transfer group on the Session ribbon. You can transfer any type of file to and from a host computer. Use InfoConnect to transfer files between your PC and an HP 3000 (including Classic, MPE/iX, and POSIX), VMS
(including OpenVMS and Alpha computers), ULTRIX, Unisys, Linux Console or UNIX system. Or, transfer files to any host or electronic service that supports the FTP, Zmodem, Xmodem, Kermit, or SuperKermit protocols.

**InfoConnect** includes its own proprietary protocol, called the WRQ/Reflection protocol. Before you can transfer a file for the first time, your administrator must upload the host file transfer program. Host programs are provided for HP 3000, VAX/VMS (DEC), AXP machines, and UNIX operating systems. A system administrator may have already uploaded the host program; if so, you can skip this step.

### In this Section

- “Transfer a File” on page 689
- “Transfer Protocols” on page 691
- “Transferring Existing Files” on page 693
- “Transfer a File with Kermit” on page 696
- “Transfer Types” on page 697
- “Filenaming and Wildcards” on page 699
- “OpenVMS Host Filename Switches” on page 699
- “Transferring Files with FTP” on page 701
- “Launch the FTP Client from a Terminal Session” on page 701
- “Transfer Dialog Box (VT)” on page 702
- “FTP Log In Dialog Box” on page 704
- “Confirm File Replace Dialog Box” on page 704
- “Select Transfer Type Dialog Box” on page 705
- “Auto-Detect Ask User Dialog Box” on page 705
- “Add Auto-detect Extension Dialog Box” on page 706
- “Configure File Transfer” on page 706

## Transfer a File

The **Transfer** dialog box supports two "drag-and-drop" methods for transferring files, in addition to specifying files and using the directional **Transfer** buttons.

Before you can transfer a file for the first time, your administrator must upload the host file transfer program.
To transfer a file

1 Open the File Transfer dialog box.
   1a Start Reflection and log on to the host computer as usual.
   1b The steps depend on your user interface mode (page 120).

2 From the Transfer dialog box, select a Protocol.

3 Select a Transfer type.

4 Select the action you want to occur if the transferred file exists in the target location.
   For more information about the options available, see the “Transferring Existing Files” on page 693 topic.

5 Click the Settings button, and configure the file transfer settings.
   For most situations, you can configure for file transfers by selecting a preset configuration in the Protocol tab.

6 Click OK.

7 Perform the file transfer using one of the following methods:
   • Drag one or more files directly from Windows Explorer to the Host icon in the Transfer dialog box (or from the Host file names list to Windows Explorer).
   -or-
   • Drag one or more files between the Local and Host boxes in the Transfer dialog box.
   -or-
   • Type one or more filename(s) in the text boxes, and then click one of the Transfer buttons.
   For more information about the filenaming options available, see the “Filenaming and Wildcards” on page 699 topic.

When the transfer begins, the File Transfer in Progress window opens. When transferring multiple files, this window displays the name of each file as it is being transferred; when the If file exists option is set to Cancel or there is some other error that stops the transfer, any remaining files matching a wildcard specification are not transferred. To cancel a file transfer in progress, click the Cancel button, press ESC, or press SPACEBAR.

Related Topics
• “Transfer Protocols” on page 691
• “Transfer Types” on page 697
• “Transferring Existing Files” on page 693
• “Filenaming and Wildcards” on page 699
• “Transfer Dialog Box (VT)” on page 702
• “Configure File Transfer” on page 706
Transfer Protocols

A file transfer protocol is a set of rules that two computers follow for transferring files between them. Files can be transferred only when both computers use the same protocol. Protocols can specify error-checking and correction rules to ensure that the information you’re transferring is accurately sent and received. InfoConnect supports several file transfer protocols:

- InfoConnect 7-bit and 8-bit WRQ/Reflection protocol to HP 3000 hosts (PCLINK2), VMS hosts (VAXLINK2), and to UNIX hosts (UNXLINK2)
- The FTP public domain protocol
If you use SuperKermit, Kermit, Zmodem, or Xmodem, that protocol must be available on the host, and you must start the host side of the process to transfer files.

On bulletin boards, you must issue a download or upload command before starting the transfer in InfoConnect.

**WRQ/Reflection**

The WRQ/Reflection protocol requires that the appropriate host program be on the host. These host programs include PCLINK2 on an HP 3000, VAXLINK2 on a VMS host, (including OpenVMS and Alpha computers), or UNXLINK2 for a UNIX host. The WRQ/Reflection protocol offers the following features:

- Wildcard transfers can be performed in either direction.
- CRC-CCITT error checking is used to ensure error-free transmission. Using this method, blocks are retransmitted, if necessary, to ensure completely accurate transmission.
- When you transfer a host file, all the file parameters of the host can be kept on the PC copy. This information can later be used to create an exact copy of the original file on the host.
- You can specify data translation parameters and many file transfer settings in the **Transfer Settings** dialog box.
- Data compression techniques produce faster transfers.

When InfoConnect is using the fast file transfer capability, data compression is not used because it usually slows down the file transfer.

- ASCII files can be sent from the PC to a host printer.
- When you click the **Attributes** button on the WRQ tab in the **Transfer Settings** dialog box or on the **Filter** tab, you can specify date/time filters (which limit the selection of files transferred using wildcards) or the file attributes for sending PC files and receiving host files.

**FTP**

File Transfer Protocol (FTP) is a public domain file transfer protocol used for file transfers to and from an FTP server. Because you can connect to an FTP server without an account, FTP servers can be useful to exchange a variety of files, including software upgrades and utilities.

Use FTP when you need network-speed file transfer across a terminal connection to a UNIX, HP 3000, VMS, or Unisys host.

If you will be using FTP exclusively for transferring files, use the InfoConnect FTP Client shipped with InfoConnect products. This application provides quick FTP transfers with a full complement of features.

**Zmodem**

Zmodem is a public domain file transfer protocol that uses a 32-bit CRC (cyclic redundancy check) to detect transmission errors. It also allows for the batch transfer of more than one file, time and date stamping, and automatic downloading. The Zmodem protocol is often used for downloading and uploading files from bulletin boards.
Kermit

Kermit is a public domain file transfer protocol available for many types of computers. You can transfer files between a PC and a host running Kermit protocol. If the Kermit program on your host has a server mode, you can also use this mode to transfer files.

SuperKermit

The SuperKermit protocol offers the following enhanced features over the standard Kermit protocol:

- You can set packet sizes greater than 94 bytes; the new default value is 512, which results in faster transfers. You can set a packet size of up to 2,048 bytes.
- The SuperKermit file transfer protocol is a sliding-window, or full-duplex protocol, which means that it sends data continuously while receiving occasional acknowledgments from the host.

In InfoConnect, you can set the number of packets that one side can receive before sending an acknowledgment. This value is 0-based, which means that the default setting of 1 (one) configures InfoConnect for a two-packet sliding-window under Kermit.

Xmodem

Xmodem is a public domain program used for file transfers, and is available for a variety of computers. The Xmodem binary transfer protocol transfers data in 128-byte data blocks. InfoConnect can receive a file in either 128-byte or 1K blocks, depending on the configuration of the remote system.

Most versions of Xmodem can perform CRC (cyclic redundancy check) error checking, which is accomplished when, from the Transfer Settings dialog box Xmodem tab, Xmodem-CRC is selected as the extension. This causes a 2-byte CRC and sets the packet size to 128-byte packets (not including overhead). The other two extension options are:

Xmodem 1-byte checksum, 128-byte packets
Xmodem-1K 2-byte CRC, 1024-byte packets

With the default Extensions option selected (Xmodem-CRC), on receives, InfoConnect automatically switches between Xmodem-CRC and Xmodem-1K, to match what the other end is sending.

Related Topics

- “Transfer a File” on page 689
- “Configure File Transfer” on page 706
- “Reflection FTP Client” on page 741

Transferring Existing Files

Index Term

Primary: use remote (VT file transfer)

Index Term

Primary: purge (VT file transfer)

Index Term

Primary: file transfer
Secondary: existing files (VT)
By default, InfoConnect asks you what to do if the local or host file being transferred already exists at the file transfer destination. If you don’t want to be prompted for each existing file, you can change the **If file exists** option in the Transfer dialog box. The options provided by this feature will change depending on which protocol you are using.

The **If file exists** options apply to both sending and receiving files when you are using the WRQ/Reflection or FTP protocol. For all other protocols, the options only apply when you are receiving files from the host and the label of the option changes to **If local file exists**. When you are transferring files to the host, what happens to duplicate files depends on the operating system or protocol rules of the host.

**NOTE:** When you are transferring mixed or uppercase file names, keep in mind that some hosts recognize case as a distinguishing feature. Same-name files, such as Myfile.doc and MYFILE.DOC, can exist side-by-side in a folder on the host simply because they are capitalized differently.

When configuring InfoConnect file transfer in the Transfer Settings dialog box, you can select from several options to change the default behavior. If you select an option that is not available for all protocols, and then transfer a file using a protocol that does not support the default option, InfoConnect reverts to the **Ask User** setting.

The options are:

- **Append**
  - Add the source file contents to the end of the destination file.

- **Ask User**
  - Open a dialog box when the file already exists. The dialog box options change depending on the type of host to which you are connected and the protocol you are using.

- **Cancel**
  - A transfer to the host is canceled only if a file with the specified name (and version number for VMS hosts) already exists. For VMS hosts, however, if you specify an existing filename without a version number, a new file with the same name is created, but with a version number one greater than the highest version number of the existing file. This applies to transfers from a PC to a VMS host, not to transfers from a host to a PC.
  
  If you send a file or files with the same name as an existing file to an HP 3000 or UNIX system, the transfer is canceled. If the file is part of a wildcard set (files being transferred using wildcards or a string of file names), no other files are transferred after a duplicate is found.

  When transferring a file to the PC, the file transfer is canceled when a file with the specified name already exists. If the file is part of a wildcard set (files being transferred using wildcards or a string of file names), no other files are transferred to the PC after a duplicate is found.

- **Delete**
  - When transferring to the PC, the existing file on the PC is deleted and a new file is created.

  When sending to a UNIX host (this option only applies to sending files to a UNIX host with the WRQ/Reflection protocol), a host file matching the local filename is deleted and a new file is created.
**Overwrite**

For transfers to this host type

**This option**

**HP**

Replaces the data in the destination file but does not replace the attributes (characteristics) of the file.

This can be a problem when overwriting a smaller file with a larger one; new records are not allocated to accommodate additional data, which means that only part of the file data is transferred.

**VMS**

Replaces the most recent instance of the destination file.

**UNIX**

Preserves existing symbolic links to the host file.

---

**Purge**

This option is available when you're using the WRQ/Reflection protocol, and when you're connected to a VMS host or an HP 3000 host. (With an HP 3000 host, this option is equivalent to deleting a file).

If you send a PC file to a VMS host using the Purge option, existing versions of the file on the host are purged following the transfer. For example, if you send Notes.txt to the host, and Notes.txt;2 and Notes.txt;3 already exist, a successful transfer results in a single file on the host called Notes.txt;4.

When transferring to the PC, the existing file on the PC is deleted and a new file is created.

**Rename**

Automatically make a copy of the existing file (you are not prompted). If you’re connected to an HP 3000, the newly created file is renamed by inserting or appending three zeros, and then incrementing the numerical characters until a unique filename is created.

If 999 is reached and a unique filename is still not found, an error is returned.

For example, with a file named filename:

<table>
<thead>
<tr>
<th>For MPE</th>
<th>For POSIX</th>
</tr>
</thead>
<tbody>
<tr>
<td>filenam0</td>
<td>filename000</td>
</tr>
<tr>
<td>filenam1</td>
<td>filename001</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>filenam9</td>
<td>filename009</td>
</tr>
<tr>
<td>filena10</td>
<td>filename010</td>
</tr>
<tr>
<td>filena11</td>
<td>filename011</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>filena99</td>
<td>filename099</td>
</tr>
<tr>
<td>filen100</td>
<td>filename100</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>filen999</td>
<td>filename999</td>
</tr>
</tbody>
</table>

**NOTE:** For POSIX, the incremented numerical characters added to a filename will be inserted before any file extension, like this: filename000.txt.

---

**Resume**

Resume a cancelled transfer when InfoConnect encounters a file with the same name as that which you are transferring.

This option is available only when you are using the Zmodem protocol, and works only when a previous attempt to receive the same file was interrupted and the **Delete cancelled receives** check box had been cleared.
You can transfer files between a PC and a host running Kermit protocol. If the Kermit program on your host has a server mode, you can also use this mode to transfer files.

To transfer a file with Kermit protocol

1. Log in to the host and invoke the host Kermit program by typing `KERMIT` (or type in the string used by your particular version of Kermit) at the host prompt.

2. Prepare to transfer the file by typing either `RECEIVE` or `SEND <filename>` at the host's Kermit prompt. (These commands are from the host's point of view, so be sure to use `RECEIVE` when sending files to the host, and `SEND` when receiving files from the host.)

3. Open the File Transfer dialog box.
   
   3a Start Reflection and log on to the host computer as usual.
   
   3b The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Reflection Ribbon</td>
<td>On the Session tab, from the Transfer group, click File Transfer.</td>
</tr>
<tr>
<td>The Reflection Browser</td>
<td>On the Reflection menu, choose Tools and then File Transfer.</td>
</tr>
<tr>
<td>touchUx</td>
<td>Tap the Wrench icon and then under Tools, select File Transfer.</td>
</tr>
</tbody>
</table>

Related Topics

- “Confirm File Replace Dialog Box” on page 704
4 From the Protocol list, choose Kermit.
5 Click the Settings button, and configure the file transfer settings.
6 From the Preset configurations list, select the type of host to which you're transferring, and then click OK.
7 Perform the file transfer.

To use Kermit server mode

1 Verify that the Kermit program on your host has a server mode.
2 After invoking Kermit on your host computer, put it in server mode by typing `SERVER` and pressing Enter.
3 Open the File Transfer dialog box.
   3a Start Reflection and log on to the host computer as usual.
   3b The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Reflection Ribbon</td>
<td>On the Session tab, from the Transfer group, click File Transfer.</td>
</tr>
<tr>
<td>The Reflection Browser</td>
<td>On the Reflection menu, choose Tools and then File Transfer.</td>
</tr>
<tr>
<td>touchUX</td>
<td>Tap the Wrench icon and then under Tools, select File Transfer.</td>
</tr>
</tbody>
</table>

4 From the Protocol list, choose Kermit.
5 Click the Settings button, and configure the file transfer settings.
6 From the Preset configurations list, select To Kermit Server, and then click OK.
7 Perform the file transfer.

Related Topics

- “Transfer a File” on page 689
- “Kermit Tab (Transfer Settings Dialog Box)” on page 735
- “Transfer Protocols” on page 691

Transfer Types

Index Term
Primary: text files

Index Term
Primary: image transfer type

Index Term
Primary: binary
Secondary: VT file transfer type

Index Term
Primary: Auto-detect
Secondary: transfer type
The file transfer type determines the way the file is saved and any data manipulation that should be performed during the transfer. You can select from the following file transfer types: ASCII, Binary, Labels (HP 3000 host only), Auto-Detect, or Image (VMS host only). For protocols other than WRQ/Reflection, you can only select from Binary (the default), ASCII, or Auto-Detect.

**NOTE:** If you are transferring a file that contains double-byte characters, select ASCII or Binary, not Auto-Detect.

---

**ASCII**

Use to transfer text files with no special formatting.

Data is transferred according to parameters set on the Translation tab in the Transfer Settings dialog box.

**Binary**

Use for program files and other types of files that should not be translated, such as files that have already been formatted for a particular type of printer or files with application-specific formatting. Binary files contain non-printable characters; using this method, a file is not converted or translated during the transfer.

**Auto-detect**

Use to cause InfoConnect to determine the file type and select the transfer type for you automatically (or to use your explicit association; see below).

This option is especially useful when transferring mixed file types. InfoConnect uses the Auto-detect tab from the Transfer Settings dialog box to detect your preferred associations between file type (by its extension) and transfer method. The Transfer Settings dialog box contains common file type associations, any of which you can delete or move to another transfer type list.

**Image**

Use to transfer a VMS or UNIX program file between two hosts via the PC. When receiving files, attribute information is appended to the file stored on the PC; this information is then used to create the file when it is transferred back to the host. Therefore, when sending files, the file must first have been received on the PC from the host using the Image transfer type.

In the case of VMS, the Image transfer type preserves the file's Record Management Services (RMS) attributes, such as the file's organization and record type. VMS files that are re-created correctly when transferred as image files include:

- .obj files
- .exe files
- .mai files
- Indexed files

For UNIX, this preserves the UNIX file's user, group, and mode information.

---

**Related Topics**

- “Transfer a File” on page 689
- “Transfer Protocols” on page 691
- “Transfer Dialog Box (VT)” on page 702
Filenaming and Wildcards

Index Term
Primary: wildcards
Secondary: VT file transfer

The list below describes the rules and behavior of filenames and wildcards in the Transfer dialog box for VT sessions.

- In the Local file names box, you can include a drive specifier, path name, and extension. However, the combination with filename (the path) cannot exceed 260 characters total. Local filenames are optional if you are receiving files from the host. Using the WRQ/Reflection protocol, wildcards can specify a group of PC files to send to the host.

- In the Host file names box, names must satisfy host system rules. For transfers to a VMS host, you can enter logical names. Host filenames are optional if you are sending files to the host.

- Specifying a filename supersedes any settings under File name translation options on the Translation tab of the Transfer Settings dialog box. Using the WRQ/Reflection protocol, host wildcard characters can specify a group of host files to send to the PC.

- You can also put wildcard entries in the text box. The receiving-side text box must be empty (or you can specify a path); host filename switches are allowed for VMS hosts. Then, click a Transfer button. The files are given the same names as they have on the sending end. All files transferred using wildcards use the specified values in the Transfer dialog box. Sets of ASCII and binary files should be transferred separately, or using auto-detect.

- The wildcard characters you use must be recognized as such by the computer that is transferring the files. The following table lists a few of the most common wildcard characters:

<table>
<thead>
<tr>
<th>This computer</th>
<th>Recognizes these wildcards</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC, UNIX, VMS</td>
<td>* ?</td>
</tr>
<tr>
<td>HP 3000</td>
<td>@ ?</td>
</tr>
</tbody>
</table>

- When the transfer begins, the File Transfer in Progress window opens. When transferring multiple files, this window displays the name of each file as it is being transferred; when the If file exists option is set to Cancel or there is some other error that stops the transfer, any remaining files matching a wildcard specification are not transferred. To cancel a file transfer in progress, click the Cancel button, press ESC, or press SPACEBAR.

OpenVMS Host Filename Switches

Index Term
Primary: filename
Secondary: switches (OpenVMS host)

Index Term
Primary: file transfer
Secondary: switches (OpenVMS host)

Using the WRQ/Reflection protocol, you can specify various qualifiers, or switches, to modify the way the file is saved on the VAX, and how it is handled when the transfer is complete.
To use the file transfer switches, append the switch you want to the name of the host file when transferring it; for example to submit the file Harriet.dat to the print spooler after sending it to the VAX, from the Transfer dialog box, in the Host file name box, you would enter the following:

Harriet.dat/S

**CAUTION:** Do not type a space before appending a switch to a filename. Doing so results in an error — InfoConnect considers this as two separate filenames. For example, Filename /A is valid, whereas Filename /A will cause the transfer to fail.

The following switches are available:

<table>
<thead>
<tr>
<th>Switch</th>
<th>Description</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>/A</td>
<td>ASCII transfer: Set maximum record length</td>
<td>When transferring ASCII files with Fast file transfer, you can specify that the maximum record length be set in the file header of the resulting host file.</td>
</tr>
<tr>
<td>/B</td>
<td>Block mode</td>
<td>For binary transfers from the host only. Forces VAXLINK2 to read the host file in block mode rather than record mode. For certain files in non-standard formats, this gives you every byte that is actually contained in the file, including record separators, without regard to record lengths or carriage control. In other words, if you do a binary receive of a file that does not have fixed record lengths, record separators will be discarded unless you use /B. You must use this switch when the file was put onto the OpenVMS system using the Pathworks COPY command.</td>
</tr>
<tr>
<td>/C</td>
<td>Submit files to batch queue</td>
<td>File transfer to the host only. Submits the file or files to the batch queue (SYS$BATCH) upon completion of the transfer. Files are deleted on the host after they have been submitted; use /K to retain the file(s).</td>
</tr>
<tr>
<td>/D</td>
<td>DECDx format files</td>
<td>Binary file transfer only. Transfers files in DECDx format between the VAX and PC.</td>
</tr>
<tr>
<td>/F</td>
<td>Fixed length records</td>
<td>Formerly used with VAXLINK to specify fixed length binary files. VAXLINK2 creates this file format by default (this switch is offered only for backward compatibility with the older protocol).</td>
</tr>
<tr>
<td>/I</td>
<td>Image transfer method</td>
<td>Formerly used with VAXLINK to specify a file transfer type of image; the image method should be specified in the Transfer dialog box (this switch is offered only for backward compatibility with the older protocol).</td>
</tr>
<tr>
<td>/K</td>
<td>Keep submitted files</td>
<td>Valid only in conjunction with the /C or /S switch, both of which submit files to a queue on the host. Once the files are in the queue, they are typically deleted. To retain a copy of the file on the host, use the /K (keep) switch.</td>
</tr>
<tr>
<td>/L</td>
<td>Add linefeed</td>
<td>Binary file transfers from the host only. Appends a linefeed character to each record when receiving a file that has carriage control. The linefeed character is added even if the carriage control is not stream- if.</td>
</tr>
<tr>
<td>/P</td>
<td>Translate carriage control characters</td>
<td>ASCII or binary file transfers from the host only. This switch translates FORTRAN or PRINT carriage control characters in OpenVMS files. When carriage control characters are not translated, they become part of the file’s records. To discard these characters, use the /T switch.</td>
</tr>
</tbody>
</table>
Transferring Files with FTP

Index Term  
Primary: FTP  
Secondary: within a terminal session (VT)

You can perform FTP file transfer from a terminal session using InfoConnect integrated FTP support, or you can launch the FTP Client.

With InfoConnect FTP, you can connect to an FTP server running on any supported host. Once connected, FTP is used to transfer files between your PC and the FTP server.

Related Topics

- “Transfer a File” on page 689
- “Configure File Transfer” on page 706
- “FTP Tab (Transfer Settings Dialog Box)” on page 738
- “Reflection FTP Client” on page 741

Launch the FTP Client from a Terminal Session

You can launch the FTP Client from the Windows Start menu or from a InfoConnect terminal session.

To launch the FTP Client from a terminal session

- Open FTP Client as follows:

  The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ribbon</td>
<td>On the Session tab, from the Transfer group, click FTP Client.</td>
</tr>
<tr>
<td>InfoConnect Browser</td>
<td>On the InfoConnect menu, choose Tools and then FTP Client.</td>
</tr>
<tr>
<td>TouchUx</td>
<td>On the InfoConnect menu, tap the Wrench icon, and then select FTP Client.</td>
</tr>
</tbody>
</table>

Switch Description Remarks

/S Spool files to printer ASCII file transfers to the host only. Submits the file or files to the print queue (SYS$PRINT) upon completion of the transfer. Files are deleted on the host after they have been submitted; use /K to retain the file after it is submitted.

/T Discard carriage control characters ASCII or binary file transfers from the host only. Discards FORTRAN or PRINT carriage control characters in OpenVMS files. To translate these characters, use /P.

/V Variable host record size Binary file transfers to the host only. Creates the host file with variable-length records (the default is fixed).

/W Block mode binary Binary file transfers from the host only. Supports the block mode binary transfer required for files created by applications, such as the DOS and OpenVMS versions of Lotus 1-2-3 and WordPerfect.
Related Topics

- “Transferring Files with FTP” on page 701
- “Reflection FTP Client” on page 741

Transfer Dialog Box (VT)

Index Term
Primary: transfer
Secondary: Transfer dialog box (VT sessions)

Index Term
Primary: record size
Secondary: VT Transfer dialog box

Index Term
Primary: logging
Secondary: VT file transfer, view

Index Term
Primary: host record size
Secondary: VT Transfer dialog box

Getting there

Start Reflection and log on to the host computer as usual.
The steps depend on your user interface mode (page 120).

User Interface Mode | Steps
---|---
The Reflection Ribbon | On the Session tab, from the Transfer group, click File Transfer.
The Reflection Browser | On the Reflection menu, choose Tools and then File Transfer.
TouchUx | Tap the Wrench icon and then under Tools, select File Transfer.

The options are:

Local

File names | Type the path and filename of the file you want to transfer. Separate multiple filenames with commas. Standard PC wildcard characters are supported.
Local Folders | Browse for the folder containing the file or files you want to transfer.
Transfer | Click a transfer button to move the file(s) in the indicated direction.
Protocol | Select the file transfer protocol you want to use.
Transfer type | Select the desired transfer type. The file transfer type determines the way the file is saved and any data manipulation that should be performed during the transfer.

For more information, see the “Transfer Protocols” on page 691 topic.

For more information, see the “Transfer Types” on page 697 topic.
If file exists
Select what to do when the transferred file already exists in the target location.

For more information, see the “Transferring Existing Files” on page 693 topic.

Host record size
**NOTE:** This box is only visible when you select, from the General tab of the Transfer Settings dialog box, Show record size on > File Transfer dialog box.

Type a value between 0 and 32767 (default: 0).

This value serves as an upper limit for the amount of data to be placed in the records of a file; records that exceed the maximum record size are split into multiple records. A value of 0 indicates that the host should determine the record size based on the transfer method selected (there is no maximum for ASCII transfers; 512-byte records are used for binary transfers). If you are in doubt as to a file's size, review other host files used by the same program.

If you're using InfoConnect for HP with NS/VT to perform transfers to an HP host, ASCII transfers default to 80 bytes, and binary transfers default to 244 bytes (122 words on the host).

Settings
Click to configure the file transfer settings.

For more information, see the “Configure File Transfer” on page 706 topic.

View Log
Click to open the log file specified on the Logging tab of the Transfer Settings dialog box.

Host

File names
Type or select one or more host files for the transfer. Separate multiple filenames with commas.

When transferring a file to a VMS host, the filename does not have to be unique. However, only the latest version of the file is displayed in the file list (the one with the highest version number).

If you want to transfer an earlier version of the file, you must type the name and version number in the Host file names box.

Show Host Files
(Appplies to WRQ/Reflection and FTP protocols only.) Click to display a list of the files in the current directory on the host.

InfoConnect first checks for a host connection, and then performs a file transfer to download a current listing of the files on the host.

After you have clicked Show Host Files, the button changes to Refresh Host Files.

If you add a new directory to the host, it will not display in the listing until you log on again.

Refresh Host Files
Click to confirm receipt of any files you transferred from the PC to the host, and to update the host file list.

By default, the host file list is not updated automatically after a file transfer. However, you can change this behavior by selecting, from the Transfer Settings dialog box General tab, Auto refresh host directory.
Host directories

(Applies to WRQ/Reflection and FTP protocols only). Click to display a list of the host directories.

To change to a different host directory, double-click its name. The list of files under File Names is updated appropriately.

NOTE: You can choose the same view of your files as you would in Windows Explorer by right-clicking either the Local file names or Host file names list, and choosing one of the options from the View menu: Large Icons, Small Icons, List, or Details.

Related Topics

- “Transfer Protocols” on page 691
- “Transfer Types” on page 697
- “Transferring Existing Files” on page 693
- “Configure File Transfer” on page 706

FTP Log In Dialog Box

This dialog box opens when you have logged on to an FTP server without specifying a user name or password.

Enter Host (or System) Name or IP Address

Type the name or IP address of the FTP server to log on to.

User name

Enter your user name as it is registered on the FTP server. If you are logging in for the first time, try to log in as Guest, or log in by selecting the Anonymous check box.

Password

Enter the password the FTP server associates with the user name. When a password is expected and the Anonymous check box is selected, the password appears in plain text, instead of asterisks (*), as you type it. If no password is expected, click OK to continue.

For added security, the number of asterisks that show do NOT match the number of characters in your password.

Often, FTP servers expect an e-mail address as a password when you log in as an Anonymous user.

Anonymous

Log on to the FTP server as a guest, with the user name anonymous.

Confirm File Replace Dialog Box

This dialog box opens when the file you're receiving already exists. You are prompted because the If local file exists option is set to its default value of Ask User.

NOTE: Different protocols will have different text on this dialog box, and different file resolution options.
<table>
<thead>
<tr>
<th>What would you like to do?</th>
<th>Select an option, and then click OK.</th>
</tr>
</thead>
<tbody>
<tr>
<td>- or - Select Transfer Type Dialog Box</td>
<td>The options are described in the topic “Transferring Existing Files” on page 693.</td>
</tr>
<tr>
<td>File resolution</td>
<td>Auto-Detect Ask User Dialog Box</td>
</tr>
<tr>
<td>Apply to all</td>
<td>Select an option, and then click <strong>Apply to all</strong> (or select the <strong>Apply to all</strong> check box and click OK). The existing file resolution option is applied to all of the files being transferred.</td>
</tr>
<tr>
<td>Cancel</td>
<td>Click to stop the transfer.</td>
</tr>
</tbody>
</table>

Related Topics
- “Transferring Existing Files” on page 693

Select Transfer Type Dialog Box

This dialog box opens when you receive a file with **Auto-Detect** as the transfer type, and **Scan** or **Ask user** are selected under **Transfer type for undefined extensions** from the **Auto-Detect** tab.

<table>
<thead>
<tr>
<th>Transfer type</th>
<th>To continue the file transfer, select a transfer type and click OK.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add extension to list</td>
<td>Select to transfer every file with this extension using the transfer type you selected from the <strong>Transfer type</strong> box. The selection is automatically updated from the <strong>Auto-detect</strong> tab. If you select this option for a file with no extension, you are adding an association between files with no extensions and the selected transfer type or method. Files with no extensions are listed on the <strong>Auto-detect</strong> tab as <code>&lt; &gt;</code>.</td>
</tr>
</tbody>
</table>

Auto-Detect Ask User Dialog Box

<table>
<thead>
<tr>
<th>Transfer type</th>
<th>To continue the file transfer, select a transfer type and click OK.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add extension to list</td>
<td>Select to transfer every file with this extension using the transfer type you selected from the <strong>Transfer type</strong> box. The selection is automatically updated from the <strong>Auto-detect</strong> tab. If you select this option for a file with no extension, you are adding an association between files with no extensions and the selected transfer type or method. Files with no extensions are listed on the <strong>Auto-detect</strong> tab as <code>&lt; &gt;</code>.</td>
</tr>
</tbody>
</table>
Related Topics

- “Auto-Detect Tab (Transfer Settings Dialog Box)” on page 713
- “Transfer Types” on page 697

Add Auto-detect Extension Dialog Box

Index Term
Primary: Auto-detect
Secondary: add extension

Index Term
Primary: Auto-detect
Secondary: add extension

Getting there

1. Open a VT terminal session.
   The steps depend on your user interface mode (page 120).

   **User Interface Mode** | **Steps**
   --- | ---
   Ribbon | On the Session ribbon, from the Transfer group, click the Transfer Settings launcher.
   InfoConnect Browser | On the InfoConnect menu, choose Tools and then File Transfer. In the Transfer dialog box, click the Settings button.
   TouchUx | Tap the Wrench icon and then under Tools, select File Transfer. In the Transfer dialog box, click the Settings button.

2. From the Transfer Settings dialog box, click the Auto-detect tab.
3. Under Auto-detect options, click the Add button.

Type an extension, and then choose a transfer type to associate with that extension.

**Extension**
Type the extension for the transfer method. The limit is five characters, or type "<" to associate a file with no extension to a transfer type.

**Transfer type**
Select a transfer type to associate with the extension in the Extension box.

   If you are unsure which transfer type to associate with an extension, use Scan. InfoConnect uses the proper transfer type after "scanning" the file being transferred.

Related Topics

- “Auto-Detect Tab (Transfer Settings Dialog Box)” on page 713

Configure File Transfer

Index Term
Primary: transfer
Secondary: configuring (VT)
You can manually configure file transfer settings by moving amongst the tabs in the Transfer Settings dialog box. Any configuration you perform is saved with your session document.

However, using the automated preset configurations is recommended.

**To configure file transfer**

1. **Open the File Transfer dialog box.**
   1a. Start Reflection and log on to the host computer as usual.
   1b. The steps depend on your user interface mode (page 120).

2. Click the **Settings** button, and configure the file transfer settings.
   
   For most situations, you can configure for file transfers by selecting a preset configuration in the Protocol tab.
   
   To see the contents of the predefined configuration, click the **View** button.

**Related Topics**

- “Transfer Dialog Box (VT)” on page 702

**Protocol Tab (Transfer Settings Dialog Box)**

Index Term
Primary: transfer
Secondary: Transfer Settings dialog box (VT)

Index Term
Primary: preset configurations
Secondary: VT file transfer

Index Term
Primary: file transfer
Secondary: preset configurations (VT)

**Getting there**

1. Open the Transfer Settings dialog box.
The steps depend on your user interface mode (page 120).

### User Interface Mode

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ribbon</td>
<td>On the Session ribbon, from the Transfer group, click the Transfer Settings launcher.</td>
</tr>
<tr>
<td>Reflection Browser</td>
<td>On the Reflection menu, choose Tools and then File Transfer. In the Transfer dialog box, click the Settings button.</td>
</tr>
<tr>
<td>TouchUx</td>
<td>Tap the Wrench icon and then under Tools, select File Transfer. In the Transfer dialog box, click the Settings button.</td>
</tr>
</tbody>
</table>

The protocol you select determines which preset configurations are available. Also, the tabs available from the Transfer Settings dialog box change to enable you to configure transfers using the selected protocol.

#### Protocol

Select the file transfer protocol you want to use. For information about the protocols, see the “Transfer Protocols” on page 691 topic.

#### Preset configurations

Selecting an item from this list adjusts the appropriate values automatically in the Transfer Settings dialog box for that specific environment. To see which values will change, select a preset configuration name and click View.

To use the values you already have defined in InfoConnect (in the Transfer Settings dialog box and elsewhere), click Current Configuration. After doing so, the View button becomes unavailable.

#### View

Click to open the View File Transfer Presets dialog box, from which you can see the predefined settings for the currently selected preset configuration.

#### Related Topics

- “Configure File Transfer” on page 706
- “Transfer Protocols” on page 691

### General Tab (Transfer Settings Dialog Box)

Index Term
Primary: timeout
Secondary: error retry limit

Index Term
Primary: timeout
Secondary: display settings (VT transfer)

Index Term
Primary: retry limit (VT file transfer)

Index Term
Primary: record size
Secondary: show in Transfer dialog box (VT)
Index Term
Primary: host record size
Secondary: show in Transfer dialog box (VT)

Index Term
Primary: filenames (8.3)
Secondary: display settings (VT transfer)

Index Term
Primary: error retry limit

Index Term
Primary: download folder

Index Term
Primary: auto refresh host directory

Getting there

1 Open the Transfer Settings dialog box.
   The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ribbon</strong></td>
<td>On the Session ribbon, from the Transfer group, click the Transfer Settings launcher: <img src="image" alt="Ribbon Launcher" /></td>
</tr>
<tr>
<td><strong>Reflection Browser</strong></td>
<td>On the Reflection menu, choose Tools and then File Transfer. In the Transfer dialog box, click the Settings button.</td>
</tr>
<tr>
<td><strong>TouchUx</strong></td>
<td>Tap the Wrench icon and then under Tools, select File Transfer. In the Transfer dialog box, click the Settings button.</td>
</tr>
</tbody>
</table>

The options are:

**General options**

- **If file exists**
  Select a default for the If file exists setting on the Transfer dialog box. For more information, see the “Transferring Existing Files” on page 693 topic.

- **Start timeout**
  Set the maximum amount of time that InfoConnect should wait for a response from the host when starting a file transfer. If there is no response within the timeout period, an error message is displayed.

- **Receive timeout**
  Set the maximum amount of time that InfoConnect should wait for a block of data or an acknowledgment from the host when transferring a file. If there is no response within the timeout period, it is assumed that the data is lost and InfoConnect requests that it be sent again. Consecutive timeouts can cause termination of the file transfer (see Error retry limit).

- **Error retry limit**
  Set the number of times InfoConnect should try to transfer a block of data before abandoning the transfer.
Transfer dialog options

Show record size on File Transfer dialog box
(Appplies only to the WRQ/Reflection protocol.) Select to display the Host record size box (located on the WRQ tab of the Transfer Settings dialog box, where it is labelled Record size) on the Transfer dialog box. This is convenient if you change the host record size often, and don’t want to go to the Transfer Settings dialog box every time you need to change it.

Auto refresh host directory
Update the host directory display in the Transfer dialog box after you’ve sent a file. If you perform a large number of transfers, keeping this check box selected is not recommended because of the time it may require (depending on the number of files in the host directory) to query the host and then update this listing.

Display 8.3 filenames as
Select how you want filenames conforming to the DOS 8.3 file naming convention to display under Local in the Transfer dialog box.

This option applies at all times when you use the WRQ/Reflection protocol, and also to Zmodem, XModem, Kermit, and FTP when the File name translation check box is selected on those protocol tabs in the Transfer Settings dialog box.

Download folder

The default folder in which received files should be placed
By default, InfoConnect specifies a folder associated with the current user. However, you can choose a different location. Type the full path, or use the Browse button.

Related Topics
• “Configure File Transfer” on page 706
• “Transferring Existing Files” on page 693

Translation Tab (Transfer Settings Dialog Box)

Index Term
Primary: translation
Secondary: translation (VT file transfer)

Index Term
Primary: translation
Secondary: options (VT file transfer)

Index Term
Primary: filenames (8.3)
Secondary: truncate received files to (VT transfer)

Index Term
Primary: filename
Secondary: translation (VT file transfer)

Index Term
Primary: ASCII
Secondary: options (VT file transfer)
Getting there

1. Open the Transfer Settings dialog box.
   The steps depend on your user interface mode (page 120).

   **User Interface Mode** | **Steps**
   --- | ---
   Ribbon | On the Session ribbon, from the Transfer group, click the Transfer Settings launcher.
   Reflection Browser | On the Reflection menu, choose Tools and then File Transfer. In the Transfer dialog box, click the Settings button.
   TouchUX | Tap the Wrench icon and then under Tools, select File Transfer. In the Transfer dialog box, click the Settings button.

The options are:

**Translation options for ASCII transfers**

**Translation to host**

- **Change tabs to spaces**
  When selected, tab characters are expanded to spaces in the host file. InfoConnect replaces each tab character with the number of spaces necessary to fill out to the next tab stop, as specified in the Spaces per tab box.

  **NOTE:** This option is not related to the Tabs tab in the Terminal Setup dialog box.

- **Read CTRL-Z as end of file**
  When selected, file transfer uses Ctrl-Z as the end-of-file marker, and strips it from the file being sent. Otherwise, the character count in the file directory is used to determine the file length.
Translation from host

**Change spaces to tabs**  
Select to use tab characters to replace consecutive spaces in the host file, and save local disk space. InfoConnect replaces consecutive spaces that fill out to the next tab stop, as specified by the **Spaces per tab** box, with a tab character.

Many PC applications interpret embedded tabs as standard, 8-column tab stops. Clear this check box if your PC program cannot interpret embedded tabs to indicate column tab stops.

**Write CTRL-Z at end of file**  
Select to add a Ctrl-Z (^Z) character to the end of a file when it is received. On the PC, ASCII text files normally end with ^Z, and many PC applications require this marker.

This setting also affects whether an end-of-file marker is added in InfoConnect macros that use the Open, PrintFile, and FlushPrinter methods.

**Delete trailing spaces**  
Select to save local disk space. Some host text files use fixed-length records to delimit lines; they pad the end of each record with blanks. Most PC text processing programs use a carriage return and linefeed sequence to delimit lines and paragraphs, and thus do not need blanks preceding a delimiter.

**Spaces per tab**  
Set the number of tab stops used if you convert tabs to spaces.

Filename translation options

**Change spaces to underscores when sending**  
Select to convert spaces in filenames to underscores in files sent to the host. If your host does not support spaces in filenames, this prevents the host from modifying the filename or rejecting the transfer.

**NOTE:** This option is ignored if, from the Transfer dialog box, in the **Host file names** box, you type a new filename: the file is transferred and stored as you type it.

**Change underscores to spaces when receiving**  
Select to convert underscores in filenames to spaces in files received from the host.

By selecting this option in conjunction with the **Change spaces to underscores when sending** option, you satisfy the conventions of both the PC and the host, yet maintain the appearance of an unchanged file name: The name change occurs, but is transparent to both the PC and the host.

This option applies at all times when you use the WRQ/Reflection protocol, and also applies to Kermit and Zmodem transfers when the **File name translation** check box is selected on the corresponding protocol tabs in the Transfer Settings dialog box.

**NOTE:** This option is ignored if, from the Transfer dialog box, in the **Local file names** box, you type a new filename: the file is transferred and stored as you type it.
Truncate received filenames to 8.3 format

Select to receive host files in the DOS 8.3 filename format.

For example, a file with the name Longfilename.Document will be converted automatically to Longfile.doc when transferred to your PC.

This option applies at all times when you use the WRQ/Reflection protocol, and also applies to Kermit and Zmodem transfers when the File name translation check box is selected on the corresponding protocol tabs in the Transfer Settings dialog box.

NOTE: This option is ignored if, from the Transfer dialog box, in the Local file names box, you type a new filename: the file is transferred and stored as you type it.

Related Topics

- “Configure File Transfer” on page 706

Auto-Detect Tab (Transfer Settings Dialog Box)

Index Term
Primary: Auto-detect
Secondary: configure

Index Term
Primary: Auto-detect
Secondary: Auto-detect Tab (Transfer Settings Dialog Box)

Getting there

1. Open the Transfer Settings dialog box.
   The steps depend on your user interface mode (page 120).

User Interface Mode

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ribbon</td>
<td>On the Session ribbon, from the Transfer group, click the Transfer Settings launcher.</td>
</tr>
<tr>
<td>Reflection Browser</td>
<td>On the Reflection menu, choose Tools and then File Transfer. In the Transfer dialog box, click the Settings button.</td>
</tr>
<tr>
<td>TouchUX</td>
<td>Tap the Wrench icon and then under Tools, select File Transfer. In the Transfer dialog box, click the Settings button.</td>
</tr>
</tbody>
</table>

Use the Auto-detect tab to associate a filename extension (five characters or less) with a transfer type. When you send a file, it is transferred using the transfer type you specify.

InfoConnect comes with default extension associations. For example, the extension .txt is associated with the ASCII file type — when a .txt file is transferred, it is transferred as an ASCII file.

You can associate additional filename extensions with a file transfer type by clicking Add.
Auto-detect options

Add
Click to show the Add Auto-detect Extension dialog box, from which you can add filename extensions to a selected transfer type.

Remove
Click to remove the selected extension.

Transfer type for undefined extensions
To associate all files to this transfer method by default, select ASCII, Binary, Image, Scan or Ask user. Only those files that are already associated with a file transfer type are exempted.

If you are unsure about which transfer method to associate to the files you transfer, you have two choices:

- Select Scan to have InfoConnect determine the file transfer type without your input.

  -or-

- Select Ask User, and then from the Ask User dialog box, select the transfer method you want.

  NOTE: If you are transferring a file that contains double-byte characters, select ASCII or Binary, not Scan.

Related Topics

- "Add Auto-detect Extension Dialog Box" on page 706
- "Auto-Detect Ask User Dialog Box" on page 705
- "Transfer Types" on page 697
- "Configure File Transfer" on page 706

Logging Tab (Transfer Settings Dialog Box)

Index Term
Primary: logging
Secondary: VT file transfer

Getting there

1. Open the Transfer Settings dialog box.

   The steps depend on your user interface mode (page 120).

User Interface Mode  Steps

Ribbon
On the Session ribbon, from the Transfer group, click the Transfer Settings launcher.

Reflection Browser
On the Reflection menu, choose Tools and then File Transfer. In the Transfer dialog box, click the Settings button.

TouchUx
Tap the Wrench icon and then under Tools, select File Transfer. In the Transfer dialog box, click the Settings button.
From this tab, you can enable logging for file transfer actions and specify the folder where the logging file should be created and updated. The logging file is named "Transfer.log" and will automatically rename itself by appending a number to the filename; for example, when the file exceeds 64K in size, it is renamed Transfer1.log. The older transfer information is retained in this now-renamed file and the file Transfer.log continues the process of adding transfer information.

<table>
<thead>
<tr>
<th>Enable file transfer logging</th>
<th>Select to log file transfer information in a text file. The file includes information such as the transferred filename, the date and time, the protocol used, and whether the transfer was successful.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log file name</td>
<td>Type the path and filename where the log file should be saved and updated.</td>
</tr>
</tbody>
</table>

Related Topics

- "Configure File Transfer" on page 706
- “Transfer Dialog Box (VT)” on page 702

**Filter Tab (Transfer Settings Dialog Box)**

**Index Term**
Primary: filter by creation date (VT file transfer)

**Index Term**
Primary: exclude files (VT file transfer)

**Getting there**

1. Open a VT terminal session. The steps depend on your user interface mode (page 120).
2. From the Transfer Settings dialog box, select either the WRQ/Reflection protocol or the FTP protocol.
3. Click the Filter tab.

From this tab, you can restrict which files are transferred, based on the date and time of their last modification. For example, to transfer only those files created after 5:00 p.m. on October 2nd, 2008, you would select the Transfer files created after check box, then enter:

Date: 10/02/08
Time: 17:00:00

The notation for the time and date depends on how you have the time set under the Regional Options in Windows Control Panel.
Transfer files created before
Select to specify a date and time, so that only files created before this time period are transferred.

Transfer files created after
Select to specify a date and time, so that only files created after this time period are transferred.

Exclude files
Exclude files from a file transfer by typing the filename(s) in this box. You can use wildcard characters; for example, to exclude HTML and GIF files, type the following:

*.htm, *.html, *.gif

Related Topics

- “Configure File Transfer” on page 706

WRQ Tab (Transfer Settings Dialog Box)

Index Term
Primary: WRQ/Reflection transfer protocol
Secondary: configuration

Index Term
Primary: window
Secondary: size (VT file transfer)

Index Term
Primary: saving
Secondary: file attributes (VT file transfer)

Index Term
Primary: run length compression

Index Term
Primary: record size
Secondary: set default (VT file transfer)

Index Term
Primary: preserve file date

Index Term
Primary: Huffman compression

Index Term
Primary: host record size
Secondary: set default (VT file transfer)

Index Term
Primary: frame size

Index Term
Primary: file attributes
Secondary: saving (VT file transfer)

Index Term
Primary: fast file transfer
Getting there

1. Open a VT terminal session.
   The steps depend on your user interface mode (page 120).

   **User Interface Mode** | **Steps**
   --- | ---
   Ribbon | On the Session ribbon, from the Transfer group, click the Transfer Settings launcher: 🔄
   InfoConnect Browser | On the InfoConnect menu, choose Tools and then File Transfer. In the Transfer dialog box, click the Settings button.
   TouchUx | Tap the Wrench icon and then under Tools, select File Transfer. In the Transfer dialog box, click the Settings button.

2. From the Transfer Settings dialog box, select the WRQ/Reflection protocol.

3. Click the WRQ tab.

   The WRQ/Reflection protocol is proprietary to InfoConnect. Before you can transfer a file for the first time, your administrator must upload the host file transfer program.

**WRQ/Reflection Protocol Options**

**Transfer type** | When you perform a file transfer, it defaults to the transfer type you select from this list.
--- | ---
Select | To do this
ASCII | Apply the items under Translation options for ASCII transfers (set from the Translation tab) to be applied to the file contents, as well as any character set translation that you have opted to perform.
Binary | Transfer the file contents unchanged.
Image | Transfer between two host computers and preserve OpenVMS-specific information.
Auto-Detect | Have InfoConnect select the transfer type for you.
Transfer link  

**NOTE:** If you're using **Fast file transfer**, this value is ignored.

Unless you're having trouble transferring files, keep this option set to its default value of **8-Bit** (this results in the fastest file transfer). In some environments, however, you may need to use one of the slower methods that convert non-printable ASCII characters to printable (and more reliably transferred) ASCII characters. Any conversion that takes place is reversed at the other end, so the contents of the file are unaffected.

For more information, see the "Transfer Link Options" on page 720 topic.

Frame size  

**NOTE:** If you're using **Fast file transfer**, this value is ignored.

Set the number of bytes of data to transfer at a time. The transfer program breaks a file into packets, or frames, that are sent one at a time until the entire file has been transmitted. There is no correlation between this box and the size of the records or blocks on the host computer.

A large frame size is more efficient when there are few transmission errors. This is especially important if you're communicating to the host over a modem, which has a greater chance of error. Use the default value in most situations.

Too small a frame results in long transmission times because of the overhead that occurs for each frame. Conversely, too large a frame can increase the elapsed time; when an error occurs, retransmitting a large frame takes longer.

For UNIX file transfers, the Window size multiplied by the Frame size cannot exceed the system-imposed limit on the number of characters that can be stored in the input queue. This limit is dependent on the particular implementation, but is typically at least 256.

Window size  

**NOTE:** If you're using **Fast file transfer**, this value is ignored.

The WRQ/Reflection file transfer protocol is a sliding-window protocol, which means that you can set the number of packets that one side sends before receiving an acknowledgment.

For UNIX file transfers, the Window size multiplied by the Frame size cannot exceed the system-imposed limit on the number of characters that can be stored in the input queue. This limit is dependent on the particular implementation, but is typically at least 256.

Because of host limitations, sliding windows are not supported by the HP 3000. For HP 3000 hosts, a window size of 1 is always used, regardless of the actual setting here.

Preserve file date  

Select to specify that, whenever a file is transferred, it should receive the source file's date and time, rather than the current date and time.

The date used is the source file's last modification date, not the creation date.
Host System Options

Fast file transfer

NOTE: This option is not available when you have UNIX selected as the System type. It is only available when your host connection is through a network using the TELNET, LAT, or NS/VT protocols.

When set to Negotiate, InfoConnect uses fast file transfer whenever possible, but reverts back to the standard protocol if fast file transfer is unsuccessful.

When Fast file transfer is set to Always (or Negotiate, and it has been determined that fast file transfers can be performed), the following settings are ignored:

WRQEndCharacter
WRQExtraCharacters
WRQFrameSize
WRQTransferLink
WRQStartCharacter
WRQWindowSize

It may be necessary to set this list to Never when sending ASCII files with records larger than 32,764 bytes.

Compress fast file transfer

If you have a fast network but comparatively slow CPU, clear this option to prevent Fast file transfer from using compression. However, if you have one of the faster CPUs currently available in today's market (for both PCs and hosts), select this option to speed up fast file transfer.

Compression

NOTE: If you're using Fast file transfer, this value is ignored.

File compression typically speeds up file transfers. Huffman compression uses more processing power on the host and the local computer, but compresses data most effectively. Users with less computing power might prefer to select Run Length or None to bypass compression completely.

Record Separator

Opens the Configure Record Separator dialog box, from which you can set the line terminator characters to use on the host and on the PC.

NOTE: Record separator options apply only to ASCII transfers.

A record separator is a character string that signifies the end of a data stream, or record. Which character string serves as a record separator can vary according to the computer.

Startup command

Each time you start a file transfer using the WRQ/Reflection protocol, InfoConnect transmits the startup command to the host computer. This tells the host to run the InfoConnect file transfer program, using the name given when it was uploaded to the host.

If you select a preset configuration (from the Protocol tab), the default command for the selected host type is inserted here.

System type

Select the type of host you will be sending files to or receiving files from.
Transfer link options can be set on the **WRQ** tab when configuring file transfer settings. In some environments, the default setting of 8-bit will not work, so you may need to use one of the slower methods that convert non-printable ASCII characters to printable (and more reliably transferred) ASCII characters.

**7-bit**

Some host environments require translation of a wider variety of non-printable ASCII characters than those that are converted by the **8-Bit** option. If you have trouble with file transfers using *InfoConnect* and an intermediary system exists between your PC and the host computer (such as a gateway or router), using the **7-Bit** option may solve the problem.

When **7-Bit** is selected, each data character, including binary data, is examined and, if necessary, modified to ensure that it is a non-control (printable) ASCII character. This data modification is reversed by the recipient (the host computer or PC), so that the data being transferred is not affected. Each packet starts with an opening parenthesis — "(" — and ends with a closing parenthesis — ")".
8-bit

This value provides the fastest file transfers, because it converts only a small number of non-printable ASCII characters during a transfer. The following characters are translated:

<table>
<thead>
<tr>
<th>Description</th>
<th>Character</th>
<th>Hex Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start of text</td>
<td>^B</td>
<td>02</td>
</tr>
<tr>
<td>End of text</td>
<td>^C</td>
<td>03</td>
</tr>
<tr>
<td>Carriage return</td>
<td>^M</td>
<td>0D</td>
</tr>
<tr>
<td>XON</td>
<td>^Q</td>
<td>11</td>
</tr>
<tr>
<td>XOFF</td>
<td>^S</td>
<td>13</td>
</tr>
<tr>
<td>End of medium</td>
<td>^Y</td>
<td>19</td>
</tr>
<tr>
<td>Number sign</td>
<td>#</td>
<td>23</td>
</tr>
<tr>
<td>Ampersand</td>
<td>&amp;</td>
<td>26</td>
</tr>
</tbody>
</table>

UNIX file transfer translates the following additional characters:

<table>
<thead>
<tr>
<th>Description</th>
<th>Character</th>
<th>Hex Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Substitute</td>
<td>^Z</td>
<td>1A</td>
</tr>
<tr>
<td>Null</td>
<td>^@</td>
<td>00</td>
</tr>
<tr>
<td>Linefeed</td>
<td>^J</td>
<td>0A</td>
</tr>
<tr>
<td>Decimal 17</td>
<td>^Q</td>
<td>11</td>
</tr>
<tr>
<td>Decimal 19</td>
<td>^S</td>
<td>13</td>
</tr>
<tr>
<td>Decimal 128</td>
<td></td>
<td>80</td>
</tr>
<tr>
<td>Decimal 255</td>
<td></td>
<td>FF</td>
</tr>
</tbody>
</table>

If you need additional character translation beyond the default set of characters that is translated, select a different value from the Transfer link list.

Setting the Transfer link value to 8-Bit requires an 8-bit data path. However, if you change Parity (in Document Settings, under Configure Connection Settings, click the More Settings button) to a value other than 8/None, you no longer have an 8-bit data path and a Transfer link of 8-Bit is ignored. All characters except those for the start and end of frame are converted.

User Defined

Some intermediate devices or drivers filter out a wider variety of non-printable ASCII characters than the default set of characters that are converted by the 8-Bit option; this also applies to certain host applications and network environments.

If you create a macro for transfer presentation or start and end of frame characters using the command WRQExtraCharacters, and the properties you use do not correspond to the values for 8-Bit or 7-Bit, the Transfer link value automatically changes to User Defined.
Related Topics
- “WRQ Tab (Transfer Settings Dialog Box)” on page 716
- “Configure File Transfer” on page 706

Configure Record Separator Dialog Box

Getting there
1. Open a VT terminal session.
   The steps depend on your user interface mode (page 120).
2. From the Transfer Settings dialog box, select the WRQ/Reflection protocol.
3. Click the WRQ tab.
4. Under WRQ/Reflection protocol options, click Record Separator.

A record separator is a character string that signifies the end of a data stream, or record. Which character string serves as a record separator can vary according to the computer.

To host

Translate record separator
Select to remove the record separators listed in the PC record separator box from the file, and replace them with the record separator appropriate for the host.

PC record separator
By default, the most common record separator for PCs, carriage return/line feed (CR/LF), is specified.

Insert special characters
Select to type the character string you want InfoConnect to interpret as your PC’s record separator. The characters you type on your keyboard will appear in the PC record separator box.
From host

**Translate record separator**  Select to remove the record separators for the host from the file and replace them with the record separator in the **Host record separator** box.

**Host record separator**  By default, the most common record separator for PCs, carriage return/line feed (CR/LF), is specified.

**Insert special characters**  Select to type the character string you want InfoConnect to interpret as your PC’s record separator. The characters you type on your keyboard will appear in the **Host record separator** box.

Related Topics

- “WRQ Tab (Transfer Settings Dialog Box)” on page 716
- “Configure File Transfer” on page 706

**HP Advanced File Transfer Options Dialog Box**

Index Term
Primary: spooled device (send to on MPE/iX)

Index Term
Primary: record format
Secondary: stream (POSIX)

Index Term
Primary: QEdit format

Index Term
Primary: POSIX
Secondary: stream record format

**Getting there**

1. Open a VT terminal session.
   The steps depend on your user interface mode (page 120).

   **User Interface Mode**  
   **Steps**
   
   **Ribbon**  
   On the **Session** ribbon, from the **Transfer** group, click the **Transfer Settings** launcher.

   **InfoConnect Browser**  
   On the **InfoConnect** menu, choose **Tools** and then **File Transfer**. In the Transfer dialog box, click the **Settings** button.

   **TouchUx**  
   Tap the Wrench icon and then under **Tools**, select **File Transfer**. In the Transfer dialog box, click the **Settings** button.

2. From the **Transfer Settings** dialog box, select the WRQ/Reflection protocol.
3. Click the **WRQ** tab.
4. Under **Host system options**, from the **System type** list, choose an HP host.
5. Click the **Advanced** button.
The options are:

**MPE file names**
Select a naming format. For more information, see the "MPE File Names, WRQ protocol" on page 727 topic.

**Send as stream**
Native POSIX files under version 5.0 of the MPE operating system support a new record format known as "stream," which is just a stream of bytes. Files created under the POSIX shell or by POSIX programs have this format by default. Files created from the MPE command interpreter or by MPE programs can be stream files.

Interoperability between stream files and other record formats is automatic. This means an MPE program can read from a stream file and it will appear to be a traditional variable length record file, and a POSIX program will see all files as stream files. MPE does the translation automatically.

If you want all files that you send to the host to have the stream format, select **Send as stream** (when you receive files from the host, the WRQ/Reflection protocol automatically detects the record format of the host file and the correct translation is performed). When this option is cleared, PCLINK2 defaults to a **Fixed** record format for ASCII files and a **Variable** record format for binary files.

**QEdit format on send**
Select to create a host file with the QEdit format.

**Send to spooled device**
Select to send output to a spooled device on MPE/iX machines.

**Remove file extension on send**
Select to strip the filename extension automatically from the files you are sending to an HP 3000.

**Related Topics**
- “MPE File Names, WRQ protocol” on page 727
- “HP File Attributes Dialog Box” on page 724

**HP File Attributes Dialog Box**

**Index Term**
Primary: variable record format (HP host)

**Index Term**
Primary: user labels (HP file attributes)

**Index Term**
Primary: undefined record format (HP host)

**Index Term**
Primary: stream record format (HP host)

**Index Term**
Primary: standard file type (HP host)

**Index Term**
Primary: relative I/O file type (HP host)

**Index Term**
Primary: record type (HP file attributes)
Index Term
Primary: record format
Secondary: file attributes (HP)

Index Term
Primary: message file type (HP host)

Index Term
Primary: HP
Secondary: file attributes

Index Term
Primary: fixed record format (HP host)

Index Term
Primary: file size (HP file attributes)

Index Term
Primary: file extent (HP file attributes)

Index Term
Primary: file code (HP file attributes)

Index Term
Primary: file attributes
Secondary: HP

Index Term
Primary: domain (HP file attributes)

Index Term
Primary: default record format (HP host)

Index Term
Primary: circular file type (HP host)

Index Term
Primary: carriage control
Secondary: HP file attribute

Index Term
Primary: blocking factor (HP file attributes)

**Getting there**

1. Open a VT terminal session.

   The steps depend on your user interface mode (page 120).

   **User Interface Mode**
   
   **Ribbon**
   
   On the **Session** ribbon, from the **Transfer** group, click the **Transfer Settings** launcher:

   **InfoConnect Browser**
   
   On the **InfoConnect** menu, choose **Tools** and then **File Transfer**. In the Transfer dialog box, click the **Settings** button.

   **TouchUx**
   
   Tap the Wrench icon and then under **Tools**, select **File Transfer**. In the Transfer dialog box, click the **Settings** button.
2 From the Transfer Settings dialog box, select the WRQ/Reflection protocol.
3 Click the WRQ tab.
4 Under Host system options, from the System type list, choose an HP host.
5 Click the Attributes button.

NOTE: With the exception of Carriage control and Domain, HP file attributes affect only the transfer of new files to the host. When you send a file that already exists on the host, these specifications are ignored.

Specifying HP attributes is an alternative to explicitly creating a file equation for a new file on the host prior to the actual transfer. The HP file attributes are used to define the physical characteristics of the file when it is created on the host. If you specify invalid file attributes, the host will refuse the file transfer; and InfoConnect will display an error message.

File attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blocking factor</td>
<td>Set the number of logical records to be contained in one physical block.</td>
</tr>
<tr>
<td>File code</td>
<td>Set the file code that identifies the file's purpose or format.</td>
</tr>
<tr>
<td>File extent</td>
<td>Set the maximum number of extents for the file.</td>
</tr>
<tr>
<td>Number of user labels</td>
<td>Set the number of user labels to be written for the file.</td>
</tr>
<tr>
<td>File size (in records)</td>
<td>Set the maximum file size.</td>
</tr>
</tbody>
</table>

Domain

Select the domain where the file resides. The domain specification determines which location, the system domain or the temporary file domain, the host uses during the transfer. For existing files, your specification should match the current domain specification for the file. If the specification does not match, a send results in a new file in the domain specified; the existing file remains unchanged in its domain.

<table>
<thead>
<tr>
<th>Domain</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temporary</td>
<td>Select when transferring a temporary job file, which is retained in the temporary file domain for use during the current session.</td>
</tr>
<tr>
<td>Permanent</td>
<td>By default, the domain is set to Permanent; the file is located in the system domain.</td>
</tr>
<tr>
<td>Carriage control</td>
<td>When selected, carriage control characters are maintained in the first column of each line in the file. The first character of each line is assumed to be a carriage control, and it is retained as such. When cleared, it is assumed that no carriage control exists in the local file (and therefore nothing is discarded).</td>
</tr>
</tbody>
</table>

Record type

Select the type of file you're transferring.

<table>
<thead>
<tr>
<th>Record type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASCII</td>
<td>Create an ASCII file.</td>
</tr>
<tr>
<td>Binary</td>
<td>Create a binary file</td>
</tr>
<tr>
<td>Default</td>
<td>Use the value selected in the Transfer type list on the WRQ tab.</td>
</tr>
</tbody>
</table>
File type

Select the type of file to create on the host. **Standard** indicates that a regular file is always created on the host. The other types are created only if they are specified explicitly from this dialog box or in the file header of a labels transfer.

Record format

The setting **Default** creates a record format based on the **Send as Stream** setting from the **HP Advanced File Transfer Options** dialog box.

<table>
<thead>
<tr>
<th>When</th>
<th>This occurs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send as Stream is selected</td>
<td>A byte-stream file is created on the host (regardless of the transfer method).</td>
</tr>
<tr>
<td>Send as Stream is cleared</td>
<td>If the <strong>Transfer</strong> type is <strong>ASCII</strong>, a fixed-length ASCII file is created.</td>
</tr>
<tr>
<td></td>
<td>-or-</td>
</tr>
<tr>
<td></td>
<td>If the <strong>Transfer</strong> type is <strong>Binary</strong>, a variable-length binary file is created.</td>
</tr>
</tbody>
</table>

Related Topics

- “**WRQ Tab (Transfer Settings Dialog Box)**” on page 716
- “**Configure File Transfer**” on page 706

MPE File Names, WRQ protocol

**Index Term**

Primary: WRQ/Reflection transfer protocol  
Secondary: MPE file names

**Index Term**

Primary: POSIX  
Secondary: filenames

**Index Term**

Primary: MPE file names

This filename structure is used for host filenames during file transfers, and it also determines how the filenames display in the **Transfer** dialog box after clicking the **Show Host Files** button.

**InfoConnect** supports four name spaces for filenames:

- **Traditional MPE filenames**. The names are assumed to be all uppercase (regardless of how they are entered in the **Host file names** box), and each name is a maximum of eight characters in the format directory structure FILENAME.GROUP.ACCOUNT. When this list is set to **MPE**, files beginning with a period or a forward slash (., /) are interpreted as POSIX files.

- **MPE/IX 5.x POSIX filenames**. For example, the names can be mixed case up to 32 characters in length, using a fully hierarchical directory structure.

MPE filenames are a subset of the POSIX names. All MPE filenames are visible from within **POSIX** (for example, PCLINK2.PUB.SYS appears as /SYS/PUB/PCLINK2), but only POSIX files whose names are also valid as MPE filenames are visible from **MPE**.

- When you select **Auto** from this list, the host will determine if it is running under the MPE Command Interpreter or the POSIX shell. If it is the MPE CI, the name space is set to **MPE**; if it is the shell, the name space is set to **POSIX**.
NOTE: Even though the host determines the name space, the setting in the dialog box is not changed; it remains as Auto.

- Selecting **MPE-Only** from this list allows only valid MPE names to be accepted. Filenames starting with "." or "/" are treated as errors.

This option is for those users who used the ".groupname" construct for the host filename. This allowed you to transfer files into a different account. For example, specifying ".PUB" transferred files into the "PUB" group. With the introduction of POSIX, this behavior changed. By default, PCLINK2 interprets the ".PUB" as a POSIX name and therefore attempts to transfer the files as a single file named ".PUB". If the name space is set to **MPE-Only**, the old behavior is performed.

There is an alternative to setting the name space to **MPE-Only**. If the name space is left set to **MPE**, then the host name may be specified as ".@.groupname" as in ".@.PUB". This will result in the same behavior as described above for the **MPE-Only** name space.

**Related Topics**

- “HP Advanced File Transfer Options Dialog Box” on page 723
- “WRQ Tab (Transfer Settings Dialog Box)” on page 716
- “Configure File Transfer” on page 706

**OpenVMS Advanced File Transfer Options Dialog Box**

**Index Term**

- Primary: translation
- Secondary: carriage control characters (OpenVMS host)

**Index Term**

- Primary: SYS$PRINT queue

**Index Term**

- Primary: SYS$BATCH queue

**Index Term**

- Primary: record counts

**Index Term**

- Primary: DECDx format

**Index Term**

- Primary: carriage control
  - Secondary: FORTRAN or PRINT (OpenVMS host)

**Index Term**

- Primary: block mode
  - Secondary: receiving options from OpenVMS host

**Getting there**

1. Open a VT terminal session.

   The steps depend on your user interface mode (page 120).
2 From the **Transfer Settings** dialog box, select the WRQ/Reflection protocol.

3 Click the **WRQ** tab.

4 Under **Host system options**, from the **System type** list, select **OpenVMS**.

5 Click the **Advanced** button.

### Send options

- **Submit to print queue on send**
  - Select to submit the file to the SYS$PRINT queue upon completion of the transfer. Once the file has been submitted to the print queue, it is automatically deleted on the host, unless the **Keep file after submitting** option is selected.

- **Submit to batch queue on send**
  - Select to submit the file on the OpenVMS host to the SYS$BATCH queue upon completion of an ASCII transfer. Once the file has been submitted to the batch queue, it is automatically deleted on the host unless the **Keep file after submitting** option is selected.

- **Keep file after submitting**
  - This option is unavailable (dimmed) unless either the **Submit to print queue** or **Submit to batch queue** is selected. Once the files are in the queue, they are deleted unless you select this option.

- **Preserve record counts**
  - Select to transfer record byte counts with the data during a binary transfer to the host; this transfers files in DECDx format.

### Receive options

- **Use block reads**
  - Select to force VAXLINK2 to read the host file in block mode rather than record mode. For certain files in non-standard formats, this transfers every byte that is actually contained in the file, without regard to record lengths or carriage controls. It is equivalent to using the image transfer method but omitting the image header information.

- **Translate carriage control**
  - Select to translate FORTRAN or PRINT carriage control characters in OpenVMS files. Without this setting, you can enable TranslateCharacters to prevent carriage control characters from being translated unpredictably. When carriage control characters are not translated, they become part of the file's records.

### Related Topics

- “**WRQ Tab (Transfer Settings Dialog Box)**” on page 716
- “**Configure File Transfer**” on page 706
OpenVMS File Attributes Dialog Box

Index Term
Primary: record size
Secondary: variable (VT file transfer)

Index Term
Primary: record format
Secondary: file attributes (OpenVMS)

Index Term
Primary: record attributes (OpenVMS host)

Index Term
Primary: Owner UIC

Index Term
Primary: OpenVMS
Secondary: file attributes

Index Term
Primary: host record size
Secondary: variable (VT file transfer)

Index Term
Primary: file protection (OpenVMS host)

Index Term
Primary: file attributes
Secondary: OpenVMS

Index Term
Primary: contiguous files (OpenVMS host)

Index Term
Primary: block span

Index Term
Primary: block boundaries

Index Term
Primary: block allocation
Secondary: OpenVMS file attributes

Getting there

1 Open a VT terminal session.
   The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ribbon</td>
<td>On the Session ribbon, from the Transfer group, click the Transfer Settings launcher.</td>
</tr>
<tr>
<td>InfoConnect Browser</td>
<td>On the InfoConnect menu, choose Tools and then File Transfer. In the Transfer dialog box, click the Settings button.</td>
</tr>
<tr>
<td>TouchUx</td>
<td>Tap the Wrench icon and then under Tools, select File Transfer. In the Transfer dialog box, click the Settings button.</td>
</tr>
</tbody>
</table>
2 From the **Transfer Settings** dialog box, select the WRQ/Reflection protocol.
3 Click the **WRQ** tab.
4 Under **Host system options**, from the **System type** list, select **OpenVMS**.
5 Click the **Attributes** button.

The options are:

**File attributes**

- **Record attributes**
  - Select a record attribute from this list, or accept the default, which allows InfoConnect to examine the record and logically select the proper attribute for it.
- **No block span**
  - By default, records are allowed to cross block boundaries. Select this option if you do not want records to cross block boundaries.
- **Record format**
  - Select a record format from this list, or use the default, which allows the host program to determine the default record format based on the transfer method.
- **Control field size**
  - Type the maximum record size. This box is available only when the **Record format** list is set to **Variable w/ fixed Ctrl**.
- **Allocation**
  - Type the number of blocks initially allocated for the file at the time of creation. If you leave this box blank, or specify a value of 0, the entire file is preallocated.
- **File options**
  - Select **Contiguous** to create a contiguous file (the transfer fails if it is not possible); select **Best-try contiguous** to create a contiguous file (if that is possible).

**File protection**

Assign the protection for a destination file. If no selections are made, protection for the file is determined by the host system.

To prevent access to all files, select the **No access** option.

- **Owner UIC**
  - Type the Owner User Identification Code (UIC) for alternate owners of the file.

**Related Topics**
- “**WRQ Tab (Transfer Settings Dialog Box)**” on page 716
- “**Configure File Transfer**” on page 706

**UNIX Advanced File Transfer Options Dialog Box**

**Index Term**

**Primary:** show hidden files (VT file transfer)

**Index Term**

**Primary:** show hidden files (VT file transfer)

**Getting there**

1 Open a VT terminal session.
   - The steps depend on your user interface mode (page 120).
2 From the **Transfer Settings** dialog box, select the WRQ/Reflection protocol.

3 Click the **WRQ** tab.

4 Under **Host system options**, from the **System type** list, select **UNIX**.

5 Click the **Advanced** button.

The option is:

Show hidden files  
Select to show hidden files on the UNIX host when the host directory list is displayed in the **Transfer** dialog box.

Related Topics

- “WRQ Tab (Transfer Settings Dialog Box)” on page 716
- “Configure File Transfer” on page 706

**UNIX File Attributes Dialog Box**

Index Term
Primary: UNIX  
Secondary: file attributes

Index Term
Primary: file attributes  
Secondary: UNIX

**Getting there**

1 Open a VT terminal session.

   The steps depend on your user interface mode (page 120).

   **User Interface Mode**
   
   **Ribbon**

   On the **Session** ribbon, from the **Transfer** group, click the **Transfer Settings** launcher:

   **InfoConnect** Browser

   On the **InfoConnect** menu, choose **Tools** and then **File Transfer**. In the Transfer dialog box, click the **Settings** button.

   **TouchUx**

   Tap the Wrench icon and then under **Tools**, select **File Transfer**. In the Transfer dialog box, click the **Settings** button.

2 From the **Transfer Settings** dialog box, select the WRQ/Reflection protocol.
3 Click the **WRQ** tab.

4 Under **Host system options**, from the **System type** list, select **UNIX**.

5 Click the **Attributes** button.

The options are:

- **Owner**
  - Type the file owner name in this box. The value must correspond to a valid login name or user ID in the specified group.

- **Group**
  - Type the group of the file’s owner in this box. The value must correspond to a valid group name or group ID.

- **Set mode**
  - When selected, you’re allowed to assign Read, Write, and Execute protection for Owner, Group, Others, and All. If the **Set mode** option is not selected, permissions are determined by the default creation mode on the host.

- **Set user ID on execution**
  - When transferring an executable file, select to specify that the owner’s permissions should determine access when the program is run (instead of using the permissions of the person running the program).

- **Set group ID on execution**
  - Select to specify that the permissions of the login group of the person running the file determine access while the file is running. See chmod (1) in your UNIX documentation.

- **Save text image after execution**
  - If an executable file is prepared for sharing, selecting this option prevents the system from abandoning the swap space image of the program-text portion of the file when its last user terminates. When the next user of a file executes it, the text does not need to be read from the file system (it is swapped in), thus saving time.

**Related Topics**

- “**WRQ Tab (Transfer Settings Dialog Box)**” on page 716
- “**Configure File Transfer**” on page 706

**Zmodem Tab (Transfer Settings Dialog Box)**

**Index Term**
- Primary: Zmodem
- Secondary: configuration

**Index Term**
- Primary: automatic downloading (VT file transfer)

**Getting there**

1. Open a VT terminal session.

   The steps depend on your **user interface mode** (page 120).
From the Transfer Settings dialog box, select the Zmodem protocol.

3 Click the Zmodem tab.

The options are:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transfer type</td>
<td>When you perform a file transfer, it defaults to the transfer type you select from this list.</td>
</tr>
<tr>
<td>Select</td>
<td>To do this</td>
</tr>
<tr>
<td>ASCII</td>
<td>Apply the items under Translation options for ASCII transfers (set from the Translation tab) to be applied to the file contents, as well as any character set translation that you have opted to perform.</td>
</tr>
<tr>
<td>Binary</td>
<td>Transfer the file contents unchanged.</td>
</tr>
<tr>
<td>Auto-Detect</td>
<td>Have InfoConnect select the transfer type for you.</td>
</tr>
<tr>
<td>Character set translation (ASCII)</td>
<td>When you perform an ASCII transfer with this option selected, InfoConnect translates characters based on the settings from the Translation tab of the Transfer Settings dialog box and the Emulation tab of the Terminal Setup dialog box.</td>
</tr>
<tr>
<td>File name translation</td>
<td>Select to invoke settings automatically under File name translation options on the Translation tab.</td>
</tr>
<tr>
<td>Packet size</td>
<td>Select or type the sub-packet size for file transfers. This value tells Zmodem how many bytes of data to transfer at a time. In many cases, the Zmodem protocol will adjust this value during a transfer as necessary (the value shown in this dialog box does not change).</td>
</tr>
<tr>
<td>Allow automatic downloading</td>
<td>If selected, when you initiate a send (from either a host system or bulletin board), InfoConnect immediately starts receiving a remote file with the same name as soon as it detects a Zmodem header. It is not necessary for the protocol to be set to Zmodem in the Transfer dialog box for this to happen. NOTE: With automatic downloading, you are not prompted for a filename or a transfer method.</td>
</tr>
<tr>
<td>Delete cancelled receives</td>
<td>Select to have a partially received file deleted automatically if you cancel the transfer in the middle of receiving a file. (If a download stop, but you did not cancel it, the received file is always kept.</td>
</tr>
</tbody>
</table>
Host system options

These startup commands are initiated from the host, which is why the term receive is used to describe the action of sending files to the host.

NOTE: These settings are necessary only when transferring files to and from a host system; they are not required for transferring files to and from a bulletin board.

Receive startup command
When you send a file, this command is transmitted to the host. Type the name of the program that starts Zmodem receives on the host. If you do not indicate a receive startup sequence, you must manually start the Zmodem receive program on the host before you can send the local file.

Send startup command
When you receive a file, this command, along with the name of the file to be received, is transmitted to the host. Type the name of the program that starts Zmodem sends on the host. If you do not indicate a send startup sequence, you must manually start the Zmodem send program on the host before you can receive the host file. For OpenVMS hosts, this sequence must be defined as a foreign command.

Related Topics

- “Configure File Transfer” on page 706

Kermit Tab (Transfer Settings Dialog Box)

Index Term
Primary: SuperKermit
Secondary: configuration

Index Term
Primary: Kermit transfer
Secondary: configuration

Index Term
Primary: checksum
Secondary: Kermit error checking (VT file transfer)

Getting there

1. Open a VT terminal session.
   The steps depend on your user interface mode (page 120).

User Interface Mode | Steps
--- | ---
Ribbon | On the Session ribbon, from the Transfer group, click the Transfer Settings launcher.
InfoConnect Browser | On the InfoConnect menu, choose Tools and then File Transfer. In the Transfer dialog box, click the Settings button.
TouchUx | Tap the Wrench icon and then under Tools, select File Transfer. In the Transfer dialog box, click the Settings button.
2 From the Transfer Settings dialog box, select the Kermit protocol.
3 Click the Kermit tab.

The options are:

<table>
<thead>
<tr>
<th>Transfer type</th>
<th>When you perform a file transfer, it defaults to the transfer type you select from this list.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select</td>
<td>To do this</td>
</tr>
<tr>
<td>ASCII</td>
<td>Apply the items under Translation options for ASCII transfers (set from the Translation tab) to be applied to the file contents, as well as any character set translation that you have opted to perform.</td>
</tr>
<tr>
<td>Binary</td>
<td>Transfer the file contents unchanged.</td>
</tr>
<tr>
<td>Auto-Detect</td>
<td>Have InfoConnect select the transfer type for you.</td>
</tr>
</tbody>
</table>

Checksum

Kermit supports three types of error checking: single-byte checksum, double-byte checksum, and 3-byte CRC. If the Kermit program at the other end of the transfer does not support the selected level, single-byte checksum is used. Single-byte is fastest, but CRC is safest.

Character set translation (ASCII)

When you perform an ASCII transfer with this option selected, InfoConnect translates characters based on the settings from the Translation tab of the Transfer Settings dialog box and the Emulation tab of the Terminal Setup dialog box.

File name translation

Select to invoke settings automatically under File name translation options on the Translation tab.

Automatic server mode

When selected, InfoConnect interacts with the host Kermit server program in the following manner:

- When you first open the Transfer dialog box, no interaction with the host occurs.
- When you request a Kermit transfer, the host is put into server mode by transmitting the Server Startup command. If you do not specify a sequence, InfoConnect updates its state to reflect that the host Kermit is in server mode. InfoConnect takes no other action.
- As long as the Transfer dialog box remains open, the host Kermit remains in server mode and transfers occur as you request them.

When Automatic Server mode is selected, any of the following actions shut down the host Kermit server program: closing the Transfer dialog box, clicking the Setup button, or changing the file transfer protocol.
SuperKermit Options

Packet size
Select the requested packet size in bytes for Kermit transfers; this value tells the SuperKermit protocol how many bytes of data to transfer at a time. This value controls the packet size used for transfers from the host. For transfers to the host, the packet size set in the host's Kermit program is used. If the host Kermit server program does not support long packets, the packet size is set to 94 bytes. Programs that support packet sizes greater than 94 bytes are often designated SuperKermit programs.

In addition to the values available from the list box, you can also type in any value from 32 to 2,048.

Window size
If the remote Kermit program supports sliding windows, this parameter determines the size of a sliding window, in packets. This value is 0-based, so the default setting (1) configures InfoConnect for a two-packet sliding window. Programs that support sliding windows are often designated SuperKermit programs.

If the remote Kermit doesn't support sliding windows, InfoConnect reverts automatically to a window size of 0 (zero).

Host system options

These startup commands are initiated from the host, which is why the term receive is used to describe the action of sending files to the host.

NOTE: These settings are only necessary when transferring files to and from a host system; they are not required for transferring files to and from a bulletin board.

Receive startup command
When you send a file, this command is transmitted to the host. Type the program name that starts Kermit receives on the host. If you do not indicate a receive startup sequence, you must manually start the Kermit receive program on host before you can send the local file.

The $FILENAME macro can optionally be specified. If present, it is replaced with the filename or wildcard filespec of the file that the host is to send. Use the $FILENAME macro in cases where additional text needs to appear after the filename.

You can embed the $BINARY:<string> macro in the command. This causes the specified <string> to be included in the transmitted startup sequence if the transfer type is binary; otherwise, the string is omitted. The <string> is defined as everything between $BINARY: and the next space.

Send startup command
When you receive a file, this command, along with the name of the file to be received, is transmitted to the host. Type the name of the program that starts Kermit sends on the host. If you do not indicate a send startup sequence, you must manually start the Kermit send program on the host before you can receive the host file.

You can embed the $BINARY:<string> macro in the command. This causes the specified <string> to be included in the transmitted startup sequence if the transfer type is binary; otherwise, the string is omitted. The <string> is defined as everything between $BINARY: and the next space.
Server startup command

This command is used in conjunction with the Automatic server mode check box to allow InfoConnect to put the host Kermit in server mode automatically. This string, followed by a CR, is transmitted to the host when InfoConnect wants to put the host in server mode.

Related Topics

- “Transfer a File with Kermit” on page 696
- “Configure File Transfer” on page 706

Xmodem Tab (Transfer Settings Dialog Box)

Index Term

Primary: Xmodem
Secondary: configuration

Xmodem Tab (Transfer Settings Dialog Box)

The options are:

Transfer type

When you perform a file transfer, it defaults to the transfer type you select from this list.

Select  To do this

ASCII  Apply the items under Translation options for ASCII transfers (set from the Translation tab) to be applied to the file contents, as well as any character set translation that you have opted to perform.

Binary  Transfer the file contents unchanged.

Auto-Detect  Have InfoConnect select the transfer type for you.

Character set translation (ASCII)

When you perform an ASCII transfer with this option selected, InfoConnect translates characters based on the settings from the Translation tab of the Transfer Settings dialog box and the Emulation tab of the Terminal Setup dialog box.

Extensions

There are two variables to be aware of with Xmodem: The error checking (1-byte checksum or 2-byte CRC) and the packet size (128 or 1024 bytes, not including overhead).

With the default Extensions option selected, InfoConnect automatically switches between Xmodem-CRC and Xmodem-1K on receives to match what the other system is sending.

Related Topics

- “Configure File Transfer” on page 706

FTP Tab (Transfer Settings Dialog Box)

Index Term

Primary: passwords
Secondary: integrated FTP (VT)
Getting there

1. Open a VT terminal session. The steps depend on your user interface mode (page 120).

   **User Interface Mode** | **Steps**
   --- | ---
   Ribbon | On the **Session** ribbon, from the **Transfer** group, click the **Transfer Settings** launcher:
   InfoConnect Browser | On the **InfoConnect** menu, choose **Tools** and then **File Transfer**. In the Transfer dialog box, click the **Settings** button.
   TouchUx | Tap the Wrench icon and then under **Tools**, select **File Transfer**. In the Transfer dialog box, click the **Settings** button.

2. From the **Transfer Settings** dialog box, select the FTP protocol.

3. Click the **FTP** tab.

   The options are:

   **Log-in options**

   **User name**
   Enter your user name as it is registered on the FTP server. If you are logging in for the first time, try to log in as **Guest**, or log in by selecting the **Anonymous** check box.

   **Password**
   Enter the password the FTP server associates with the user name. When a password is expected and the **Anonymous** check box is selected, the password appears in plain text, instead of asterisks (*), as you type it. If no password is expected, click **OK** to continue.

   For added security, the number of asterisks that show do **NOT** match the number of characters in your password.

   Often, FTP servers expect an e-mail address as a password when you log in as an **Anonymous** user.

   **Anonymous**
   Log on to the FTP server as a guest, with the user name **anonymous**.

   **Enter Host (or System) Name or IP Address**
   Type the name or IP address of the FTP server to log on to.

   **Clear Log-in Options**
   Specify when logon information should be cleared from the controls and fields in this tab (and thus not used as logon information for, as an example, a new host you wish to log on to).

   **Transfer type**
   When you perform a file transfer, it defaults to the transfer type you select from this list.
### Select

<table>
<thead>
<tr>
<th>Option</th>
<th>To do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASCII</td>
<td>Apply the items under <strong>Translation options for ASCII transfers</strong> (set from the <strong>Translation</strong> tab) to be applied to the file contents, as well as any character set translation that you have opted to perform.</td>
</tr>
<tr>
<td>Binary</td>
<td>Transfer the file contents unchanged.</td>
</tr>
<tr>
<td>Auto-Detect</td>
<td>Have InfoConnect select the transfer type for you.</td>
</tr>
</tbody>
</table>

#### Character set translation (ASCII)

When you perform an ASCII transfer with this option selected, InfoConnect translates characters based on the settings from the **Translation** tab of the **Transfer Settings** dialog box and the **Emulation** tab of the **Terminal Setup** dialog box.

#### File name translation

If you are using FTP for ASCII transfers to a host, you can select this option to invoke settings automatically under **File name translation** options on the **Translation** tab.

#### System type

Select the type of host to which you will send files to or receive files from.

#### Use passive mode

When selected, the client sends a PASV command to communicate with the server in passive mode (sometimes called **PASV mode**). This initiates a separate data connection for directory listings and file transfers.

Use passive mode to minimize connection problems with firewalls, such as the Windows firewall enabled by default in some versions of Windows XP.

#### Transfer with

There are two different implementations of FTP available from the FTP tab: InfoConnect FTP and Microsoft FTP.

- **InfoConnect FTP** provides connections to any host InfoConnect supports. Microsoft FTP provides connections to UNIX hosts, and can be used only for FTP transfers to hosts whose FTP server supports UNIX or Windows NT-style server command interfaces.

#### Default upload directory

Select the host directory to which InfoConnect should be set after an FTP connection is made. If a directory is listed in this box, the command in the **Host directory command** box is ignored.

#### Host directory command

Type a host command in this box to retrieve the location of your host's current directory. InfoConnect uses this information to set the current host directory after an FTP connection is made. The command that's listed can be changed if it does not match your host's "get current host directory" command.

If a directory is listed in the **Default upload directory** box, that value is used and the command in the **Host directory command** box is ignored.

**NOTE:** When **System type** is **Unisys**, only the **Default upload directory** box can be used to set the current host directory.

---

**Related Topics**

- “Transferring Files with FTP” on page 701
- “Configure File Transfer” on page 706
Reflection FTP Client

You can use the FTP Client to transfer files between the local computer and a remote host. Launch the client from the Windows Start menu or from the InfoConnect workspace.

- When you launch from the Windows Start menu, you'll see the Connect to FTP Site dialog box, which you can use to select a host.
- When you use the FTP Client button in the workspace, the client connects to the current host.

In this Section

- “Introducing Reflection FTP Client” on page 741
- “Connecting to an FTP or SFTP Server” on page 745
- “Working with FTP Client Settings Files” on page 761
- “Configuring Site and Global Properties” on page 765
- “Transferring Files” on page 780
- “Managing Files and Folders” on page 792
- “Customizing FTP Client Startup” on page 801
- “FTP Client Troubleshooting” on page 805
- “Using the FTP Command Window” on page 815
- “FTP Scripting” on page 819
- “Command Reference” on page 825

Introducing Reflection FTP Client

Index Term

Primary: FTP Client
Secondary: introduction

Reflection FTP Client enables you to connect to FTP sites and quickly transfer files using the FTP protocol. It includes the following features:

- A split pane view allows you to browse for both local and server files. View menu options allow you to select the display preferences you prefer for viewing files.
- Use standard Windows drag-and-drop and copy-and-paste operations to transfer files between the server and your PC.
- The FTP Client supports a variety of security protocols, including SOCKS, SSL/TLS, Kerberos, Secure Shell, and firewall servers.
- The FTP Site Wizard leads you through the steps necessary to configure your FTP site. To launch the wizard, click New in the Connect to FTP Site dialog box.
- The FTP Client automatically recognizes most common FTP servers. Troubleshooting options for problem servers include support for creating simplified file lists and the Directory Definition Wizard.
- An optional command window allows you to view all messages sent between the FTP Client and server. In this view, you can also communicate with the FTP server by entering standard FTP commands directly on a command line.
- Smart file transfer allows FTP client to automatically recognize which transfer method (ASCII or Binary) is appropriate for specified types of files.
• A script recorder allows you to capture actions you take using the FTP Client as command scripts and to play back those scripts to automate connections and file transfers.

• OLE Automation support allows you to script FTP transfers from external applications.

Related Topics

• “Transfer Files with FTP Client” on page 780

In this Section

• “Connect to FTP Site Dialog Box” on page 742
• “View the Local PC Files” on page 742
• “View the Server Files” on page 743
• “FTP Client Settings Files” on page 744
• “Options for Automating FTP Client Transfers” on page 744

Connect to FTP Site Dialog Box

Index Term
Primary: connecting (FTP Client)
Secondary: Connect to FTP Site dialog box

The Connect to FTP Site dialog box opens when you start the FTP Client. You can also open it by choosing Connect from the Connection menu. This dialog box shows all sites that you have defined and saved to the current settings file.

Connect to the selected site. The client connects using settings you have configured for that site.

Add an FTP site. This opens the Add FTP Site wizard.

View or modify the settings for the selected site.

Configure secure connections to the selected site.

Related Topics

• “Add a New Site to your Connection List” on page 746
• “Connect to a Site” on page 745
• “Secure FTP Client Connections” on page 747
• “Troubleshooting FTP Client Connections” on page 806
• “Connecting to an FTP or SFTP Server” on page 745

View the Local PC Files

Index Term
Primary: FTP Client
Secondary: local pane

To work with items on the local PC, use the left pane of the FTP Client. Commands on the File and Edit menus, and most buttons on the toolbar, apply to folders and files in the currently active pane.
To view the local PC files

1. Start the FTP Client.
2. Click the left pane to make it active.
3. Use the left pane to browse your files and folders.

**NOTE**

- To see and navigate the hierarchy of all folders, go to the active pane, click the **Go to a different folder** list box, then choose the folder you want to open.
- To change the way files are displayed, go to the active pane and use the commands on the **View** menu, or use the four view buttons on the toolbar.

**Related Topics**

- “Managing Files and Folders” on page 792

**View the Server Files**

**Index Term**

Primary: FTP Client
Secondary: server pane

To work with items on the server, use the right pane of the FTP Client. Commands on the **File** and **Edit** menus, and most buttons on the toolbar, apply to folders and files in the currently active pane.

**To view the server files**

1. Start the FTP Client and connect to the remote site.
2. Click the right pane to make it active.
3. To open a folder or file, or to start a program, double-click it.

   To display the contents of a file or run a program, the FTP Client first copies the file from the server to your default local home folder.

**NOTE**

- For FTP connections (but not SFTP connections) you can use a file view filter to limit the current directory listing to files of a specific type. From the **View** menu, choose **Filter**.
- To see and navigate the hierarchy of all folders, go to the active pane, click the **Go to a different folder** list box, then choose the folder you want to open.
- To change the way files are displayed, go to the active pane and use the commands on the **View** menu, or use the four view buttons on the toolbar.

**Related Topics**

- “Working with Server Directories” on page 794
- “Filter the Server File Listing” on page 797
- “Set Default Home Directories” on page 795
- “Run the Directory Definition Wizard” on page 798
The **Reflection FTP Client** uses settings files to save your configuration. Settings files include the following information:

- All the sites you have configured, including all site properties. If you have elected to save passwords, these are saved as encrypted text in the settings file.
- Your settings for **Transfer Method** and **If File Exists**.
- Settings that you have configured using the **Options** dialog box.

By default the client automatically opens a settings file named `Settings.rfw` when you start up. You can create shortcuts to launch the client and automatically open any settings file. The client’s title bar displays the name of the currently open settings file. Settings files use an `.RFW` file extension.

**NOTE**

- When you open a settings file, the settings in the file you open replace any currently configured settings.
- You can also use the **Import Settings** command to modify your client settings. When you do, imported settings are appended to any currently configured settings and the title of your session remains unchanged.
- Some display preferences are saved to the Windows registry, not settings files. These settings include your command pane display and your local and server pane view settings. Changes you make to any of these settings affect all client sessions regardless of what settings file is open.
- Prior to version 13.0, settings were saved in the Windows registry. If you have upgraded from an older version your settings are migrated automatically to a settings file the first time you run the client.

**Related Topics**

- “Working with FTP Client Settings Files” on page 761
- “Create a Shortcut to Load a Settings File” on page 802
- “Import FTP Client Settings” on page 763

**Options for Automating FTP Client Transfers**
The **FTP Client** provides the following options for automating file transfers:

- Use FTP Client scripts to automate connections and file transfers from within the client. For details, see “FTP Scripting” on page 819 and the “Command Reference” on page 825.
- Use the FTP Client Automation API to automate transfers from external applications. You can download detailed information about this programming interface from the Attachmate Web site. For more information, see Technical Note 2362 (http://support.attachmate.com/techdocs/2362.html).

## Connecting to an FTP or SFTP Server

### In this Section

- “Connect to a Site” on page 745
- “Add a New Site to your Connection List” on page 746
- “View Connection Information” on page 746
- “Preserve a Connection to a Server” on page 747
- “Secure FTP Client Connections” on page 747

### Connect to a Site

You can connect to an FTP or SFTP server in any of these ways:

- Use the **Connect to FTP Site** dialog box that opens when you launch the client.
- Create a shortcut that launches a settings file and automatically connects you to a site.
- Enter an **OPEN** command at the FTP command line. For more information, see the Open topic (page 839) in the Command Reference.
- Start the client with a startup command that runs a script or connects to a server and performs a file transfer command automatically.
- Connect to a second site in the same session using **Connect > Connect to a Second Site**.

### Related Topics

- “Connect to FTP Site Dialog Box” on page 742
- “Create a Shortcut to Connect to a Site” on page 802
- “FTP Client Startup Switches” on page 802
- “Add a New Site to your Connection List” on page 746
- “Customizing FTP Client Startup” on page 801
- “Secure FTP Client Connections” on page 747
Add a New Site to your Connection List

Index Term
Primary: FTP Client
Secondary: configuring a new site

Use the Connect to FTP Site dialog box to add new sites to your connection list.

To add a new FTP or SFTP site to your connection list

1. Start the FTP Client.
   This opens the Connect to FTP Site dialog box. (If the FTP Client is already running and this
dialog box is not open, go to Connection > Connect.)
2. Click New to start the Add FTP Site Wizard.
3. Type the host name or IP address of the FTP (or SFTP) server and click Next.
4. Specify whether to log in with a user name or using an anonymous login. (Anonymous logons
are not allowed for SFTP connections.)
5. (Optional) To configure additional site properties, click Advanced in the Login Information
panel.
6. (Optional) To configure a secure connection, click Security in the Login Information panel.
   
   NOTE: You can also modify the security and other properties later. To do this select the site in
the Connect to FTP Site dialog box and click Security or Properties.
7. If you are configuring a connection for a registered user, you'll see the FTP User Login panel.
   Type your user name. You can also save your password as obfuscated text in the settings file.
8. In the Connect panel, enter a descriptive name for this site. This name is used in the Connect
to FTP Site dialog box.
9. Specify whether you want to connect to the site now and click Finish.
10. From the File menu, click Save to save this change to the current settings file.

Related Topics

- “Connecting to an FTP or SFTP Server” on page 745
- “Create a Shortcut to Connect to a Site” on page 802
- “Secure FTP Client Connections” on page 747

View Connection Information

Index Term
Primary: connecting (FTP Client)
Secondary: displaying connection information

When you are connected to a host you can display information about the server and the connection.

To view connection information

1. From the Connection menu, click Site Properties.
2. Click the Information tab.

The Information tab provides these statistics:

- Some characteristics of the server
The date and time the connection was opened
- How long the connection has been active
- Duration of the last file transfer operation
- Speed of the last file transfer operation
- Average speed of all file transfer operations during the current session
- Security information about the current session

Preserve a Connection to a Server

Index Term
Primary: connecting (FTP Client)
Secondary: preserving a connection

Most servers have an "idle time" value that specifies how long a user's session can last when no activity is detected. When the user exceeds the time limit, the server connection is closed. To prevent the server from closing the connection due to inactivity, you can configure the FTP Client to send "keep alive" commands.

To preserve a connection to the server

1. Open the Site Properties dialog box and then click the Connection tab.
2. Select Send keep alive every <n> seconds and specify how many seconds to wait in between sending consecutive keep alive (NOOP) commands.
3. Click OK.

NOTE: This setting has no effect on SFTP connections. For SFTP connections use Server Keep Alive on the General tab of the Secure Shell Settings dialog box.

Related Topics
- "Reflection Secure Shell Settings Dialog Box" on page 353

Secure FTP Client Connections

Index Term
Primary: secure connections
Secondary: FTP Client

The FTP Client supports a variety of security protocols, including SOCKS, SSL/TLS, Kerberos, Secure Shell, and firewall servers.

In this Section
- "Connect Using a SOCKS Proxy Server" on page 748
- "Connect via a Firewall" on page 749
- "Kerberos Connections (FTP Client)" on page 753
- "Secure Shell Connections (FTP Client)" on page 756
- "SSL/TLS Connections (FTP Client)" on page 759
Connect Using a SOCKS Proxy Server

Index Term
Primary: SOCKS
Secondary: configuring (FTP Client)

Use this procedure to configure connections in the FTP Client if your site uses a SOCKS proxy server.

To connect using a SOCKS proxy server

1 Start the FTP Client.

   This opens the Connect to FTP Site dialog box. (If the FTP Client is already running and this dialog box is not open, go to Connection > Connect.)

2 Perform one of the following tasks:

   To Do This
   Create a new site From the Connect to FTP Site dialog box, click New.
   In the Add FTP Site dialog box, enter the name or IP address of your FTP server host, and then click Next.
   In the Login Information dialog box, select User.
   Modify an existing site From the Connect to FTP Site dialog box, select a site.

3 Click Security.

4 SOCKS configuration is different for FTP and SFTP connections:

   To Do this
   Configure an FTP connection On the SOCKS tab select Use SOCKS. Click Configure to configure your SOCKS proxy servers and destination routes.
   Configure an SFTP connection On the Secure Shell tab click Configure to open the Reflection Secure Shell Settings dialog box. On the General tab, select Use SOCKS Proxy. Click Configure SOCKS to configure your SOCKS proxy servers and destination routes.

5 Perform one of the following tasks:

   If you are Do This
   Creating a new site Click OK to close the Security Properties dialog box and then click Next.
   In the FTP User Login dialog box, type your user name on the FTP server and then click Next.
   Modifying an existing site Click Finish.

   Click OK to close the open dialog boxes.

NOTE: The default port number for SOCKS servers is 1080.
Connect via a Firewall

Index Term
Primary: firewall (FTP Client)
Secondary: configuring in (FTP Client)

Use this procedure if you connect to your FTP or SFTP server through a firewall.

To connect via a firewall

1 Start the FTP Client.
   This opens the Connect to FTP Site dialog box. (If the FTP Client is already running and this dialog box is not open, go to Connection > Connect.)
2 Perform one of the following tasks:

   To                      Do This
   Create a new site       From the Connect to FTP Site dialog box, click New.
                            In the Add FTP Site dialog box, enter the name or IP address of your FTP server host, and then click Next.
                            In the Login Information dialog box, select User.
   Modify an existing site From the Connect to FTP Site dialog box, select a site.

3 Click Security.
4 On the Firewall tab, select Use Firewall.
5 Use Style to select the authentication command sequence used by your firewall. (The style you select determines which options you can configure in the dialog box.)
6 Configure the appropriate authentication information for your server.
7 Perform one of the following tasks:

   If you are                Do This
   Creating a new site      Click OK to close the Security Properties dialog box and then click Next.
                            In the FTP User Login dialog box, type your user name on the FTP server and then click Next.
                            Click Finish.
   Modifying an existing site Click OK to close the open dialog boxes.

NOTE

• The Firewall tab is not available for SFTP connections.
• The settings in the Firewall tab of the Security Properties dialog box are used for all sites that you configure to connect via a firewall.
• When Use passive mode is enabled (the default), the FTP Client initiates a separate data connection for directory listings and file transfers. This is required for connections through some firewalls. If passive mode has been turned off and a directory listing does not display or you get an error "425 Can't open data connection," you should enable this setting.
The **FTP Client** sends different commands for logging onto a firewall and connecting to an FTP server based on the style of server you specify. During this authentication sequence, the FTP Client uses information you have configured in the **Site > Properties** dialog box and the **Firewall** tab of the **Security Properties** dialog box. If you have not configured all or part of this information, you'll be prompted for it each time you make a connection.

The following styles are available:

**SITE servername**

Use this style if your passthrough server sends a SITE command to connect to the FTP server. For details, see the "SITE Servername Authentication Command Sequence" on page 751.

**username@servername**

Use this style if your passthrough server requires server logon information in the format **username@servername**. For details, see the "Username@servername Authentication Command Sequence" on page 751.

**USER-PASS-ACCT**

Use this style when you don't need to specify a proxy server because your network automatically routes connections through the firewall. In this logon sequence both the FTP site and firewall user names are sent with a single USER command and the firewall password is sent with the ACCT command. For details, see the "USER-PASS-ACCT Authentication Command Sequence" on page 752.

**Transparent**

Use this style when you don't need to specify a proxy server because your network automatically routes connections through the firewall. In connections made using this style, a sequence of USER and PASS commands sends logon information for the firewall followed by the FTP server. For details, see the "Transparent Authentication Command Sequence" on page 752.

**Challenge/Response**

Use this style if your server requires you to use a hardware token to enter identification information when you open a connection. When you select this style, you can't preconfigure password information. During the login process, you'll see a challenge prompt. Use your token to determine the correct information to enter in response to this prompt. For details, see the "Challenge/Response Authentication Command Sequence" on page 752.
UserID@FireID@RemoteHost

Use this style if your server requires a login of the style UserID@FireID@RemoteHost. If you leave the other boxes blank, the FTP Client prompts for information in this order when you make a connection: Firewall address, Firewall user name, Firewall password, FTP server address, FTP user name.

FirewallUser@FTPServer

Use this style if your server requires a login of the style FirewallUser@FTPServer. If you leave the other boxes blank, the FTP Client prompts for information in this order when you make a connection: Firewall address, Firewall username, Firewall password and FTP username. For details, see “FirewallUser@FTPServer Authentication Command Sequence” on page 753.

FtpUser@FtpServer FirewallUser

Use this style if your server requires a login of the style FtpUser@FtpServer FirewallUser. If you leave the other boxes blank, the FTP Client prompts for information in this order when you make a connection: Firewall address, Firewall username, Firewall password, FTP user name and FTP password. For details, see “FTPUser@FTPServer FirewallUser Authentication Command Sequence” on page 753.

Related Topics

- “Connect via a Firewall” on page 749
- “Firewall Tab (Security Properties Dialog Box)” on page 513

SITE Servername Authentication Command Sequence

Index Term
Primary: SITE servername authentication command sequence

The FTP Client uses the following command sequence to make a connection when you have configured Style to SITE servername in the Firewall tab of the Security Properties dialog box.

```
OPEN <proxy_server>
USER <firewall_username>
PASS <firewall_password>
SITE <FTP_server>
USER <FTP_server_username>
PASS <FTP_server_password>
```

Related Topics

- “Connect via a Firewall” on page 749
- “Firewall Tab (Security Properties Dialog Box)” on page 513

Username@servername Authentication Command Sequence

Index Term
Primary: Username@servername authentication command sequence

The FTP Client uses one of the following command sequences to make a connection when you have configured Style to username@servername in the Firewall tab of the Security Properties dialog box.

When Passthrough authentication is selected:

```
OPEN <proxy_server>
USER <firewall_username>
PASS <firewall_password>
USER <username>@<FTP_server>
PASS <FTP_server_password>
```
When **Passthrough authentication** is not selected:

```
OPEN <proxy_server>
USER <username>@<FTP_server>
PASS <FTP_server_password>
```

**Related Topics**

- “Connect via a Firewall” on page 749
- “Firewall Tab (Security Properties Dialog Box)” on page 513

**USER-PASS-ACCT Authentication Command Sequence**

Index Term
Primary: USER-PASS-ACCT authentication command sequence

The **FTP Client** uses the following command sequence to make a connection when you have configured **Style** to **USER-PASS-ACCT** in the **Firewall tab** of the **Security Properties** dialog box.

```
OPEN <FTP_server>
USER <FTP_server_username> <firewall_username>
PASS <FTP_server_password>
ACCT <firewall_password>
```

**Related Topics**

- “Connect via a Firewall” on page 749
- “Firewall Tab (Security Properties Dialog Box)” on page 513

**Transparent Authentication Command Sequence**

Index Term
Primary: Transparent authentication command sequence

The **FTP Client** uses the following command sequence to make a connection when you have configured **Style** to **Transparent** in the **Firewall tab** of the **Security Properties** dialog box.

```
OPEN <FTP_server>
USER <firewall_username>
PASS <firewall_password>
USER <FTP_server_username>
PASS <FTP_server_password>
```

**Related Topics**

- “Connect via a Firewall” on page 749
- “Firewall Tab (Security Properties Dialog Box)” on page 513

**Challenge/Response Authentication Command Sequence**

Index Term
Primary: Challenge/Response authentication command sequence

The **FTP Client** uses the following command sequence to make a connection when you have configured **Style** to **Challenge/Response** in the **Firewall tab** of the **Security Properties** dialog box.

```
OPEN <FTP_server>
USER <firewall_username>
PASS <challenge_response_from_token>
USER <FTP_server_username>
PASS <FTP_server_password>
```
Related Topics

- “Connect via a Firewall” on page 749
- “Firewall Tab (Security Properties Dialog Box)” on page 513

**FirewallUser@FTPServer Authentication Command Sequence**

The **FTP Client** uses the following command sequence to make a connection when you have configured **Style** to **FirewallUser@FTPServer** in the **Firewall** tab of the **Security Properties** dialog box.

OPEN <Firewall_server>
USER <Firewall_username>@<FTP_server>
PASS <Firewall_password>
USER <FTP_username>

Related Topics

- “Firewall Tab (Security Properties Dialog Box)” on page 513
- “Connect via a Firewall” on page 749

**FTPUser@FTPServer FirewallUser Authentication Command Sequence**

The **FTP Client** uses the following command sequence to make a connection when you have configured **Style** to **FTPUser@FTPServer FirewallUser** in the **Firewall** tab of the **Security Properties** dialog box.

OPEN <Firewall_server>
USER <FTP_username>@<FTP_server> <Firewall_username>
PASS <FTP_server_password>
ACCT <Firewall_password>

Related Topics

- “Firewall Tab (Security Properties Dialog Box)” on page 513
- “Connect via a Firewall” on page 749

**Kerberos Connections (FTP Client)**

You can configure the **FTP Client** to use Kerberos for authentication and encryption.

Related Topics

- “Configure Kerberos for FTP Client” on page 753
- “Configure Kerberos (SFTP Connections)” on page 755

**Configure Kerberos for FTP Client**

Index Term
Primary: Kerberos (Secure Shell connections)
Secondary: configuring in the FTP Client

If you are configuring FTP connections, you can use Kerberos for both authentication and encryption.

**To configure Kerberos authentication for the FTP Client**

1. Start the **FTP Client**.
   - This opens the **Connect to FTP Site** dialog box. (If the **FTP Client** is already running and this dialog box is not open, go to **Connection > Connect**.)
2 Perform one of the following tasks:

<table>
<thead>
<tr>
<th>To</th>
<th>Do This</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a new site</td>
<td>From the <strong>Connect to FTP Site</strong> dialog box, click <strong>New</strong>.</td>
</tr>
<tr>
<td></td>
<td>In the <strong>Add FTP Site</strong> dialog box, enter the name or IP address of your FTP server host, and then click <strong>Next</strong>.</td>
</tr>
<tr>
<td></td>
<td>In the <strong>Login Information</strong> dialog box, select <strong>User</strong>.</td>
</tr>
<tr>
<td>Modify an existing site</td>
<td>From the <strong>Connect to FTP Site</strong> dialog box, select a site.</td>
</tr>
</tbody>
</table>

3 Click **Security**.

4 On the **Kerberos** tab, select the **Reflection Kerberos** check box.

5 Select the principal and realm you want to use for Kerberos authentication to this server. If the **Initial Configuration** dialog box appears, type the settings for the principal name, realm, **KDC** (page 888) host, and credentials. (This dialog box doesn't appear if your PC has a Kerberos Manager configuration file installed.)

6 Configure any additional Kerberos options on this tab or by clicking **Kerberos Manager**. For more information about **Kerberos Manager**, see the documentation included with the application.

7 Perform one of the following tasks:

<table>
<thead>
<tr>
<th>If you are</th>
<th>Do This</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating a new site</td>
<td>Click <strong>OK</strong> to close the <strong>Security Properties</strong> dialog box and then click <strong>Next</strong>.</td>
</tr>
<tr>
<td></td>
<td>In the <strong>FTP User Login</strong> dialog box, type your user name on the FTP server and then click <strong>Next</strong>.</td>
</tr>
<tr>
<td></td>
<td>Click <strong>Finish</strong>.</td>
</tr>
<tr>
<td>Modifying an existing site</td>
<td>Click <strong>OK</strong> to close the open dialog boxes.</td>
</tr>
</tbody>
</table>

8 Click **Connect** to authenticate to this host and establish a connection.

A key and/or padlock icon appears on the status bar when you have made a successful secure connection. The key indicates secure authentication, the padlock indicates an encrypted data stream.

Settings on the **Kerberos** tab of the **Security Properties** dialog box are saved to your **Reflection FTP Client** settings file. Settings from **Kerberos Manager** and the **Initial Configuration** dialog box are saved in the Windows registry and apply to all installed Reflection applications that support Kerberos.

**NOTE:** Kerberos support is not available with the **Reflection FTP Client** that ships as part of Reflection NFS Client (full product).

**Related Topics**

- “**Kerberos Connections (FTP Client)**” on page 753
Configure Kerberos (SFTP Connections)

Index Term
Primary: Kerberos (Secure Shell connections)
Secondary: authentication for SFTP connections

If you are configuring SFTP connections, you can use Kerberos for authentication.

To configure Kerberos authentication for SFTP sessions

1 Start the FTP Client.
   This opens the Connect to FTP Site dialog box. (If the FTP Client is already running and this
dialog box is not open, go to Connection > Connect.)

2 Perform one of the following tasks:

   To Do This
   Create a new site From the Connect to FTP Site dialog box, click New.
   In the Add FTP Site dialog box, enter the name or IP address of your
   FTP server host, and then click Next.
   In the Login Information dialog box, select User.
   Modify an existing site From the Connect to FTP Site dialog box, select a site.

3 Click Security.

4 Click the Secure Shell tab.

5 Select Use Reflection Secure Shell.

6 (Optional) Specify an SSH config scheme. (If you leave SSH config scheme blank, Reflection
saves any changes you make to an SSH configuration scheme with the same name as the
current host.)

7 Click Configure.

8 On the General tab, under User Authentication, select GSSAPI/Kerberos.

9 Click the GSSAPI tab.

10 Configure GSSAPI authentication.

   When SSPI is selected, Reflection uses your Windows domain login credentials to authenticate
to the Secure Shell server. Selecting SSPI as your GSSAPI provider configures Reflection to
authenticate using Microsoft’s Security Support Provider Interface (SSPI).

   When Reflection Kerberos is selected, Reflection uses the Reflection Kerberos client for
Kerberos/GSSAPI authentication. Before you can make connections using the Reflection
Kerberos client, you must configure Reflection Kerberos on your computer. You can use the
Configure button to configure Kerberos if it has not yet been configured on your system, or to
modify your existing Kerberos configuration.
11 Perform one of the following tasks:

<table>
<thead>
<tr>
<th>If you are</th>
<th>Do This</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating a new site</td>
<td>Click OK to close the <strong>Security Properties</strong> dialog box and then click <strong>Next</strong>.</td>
</tr>
<tr>
<td></td>
<td>In the <strong>FTP User Login</strong> dialog box, type your user name on the FTP server and then click <strong>Next</strong>.</td>
</tr>
<tr>
<td>Modifying an existing site</td>
<td>Click <strong>Finish</strong>.</td>
</tr>
</tbody>
</table>

**NOTE:** Kerberos support is not available with the Reflection FTP Client that ships as part of Reflection NFS Client (full product).

**Related Topics**

- “Kerberos Connections (FTP Client)” on page 753

**Secure Shell Connections (FTP Client)**

Secure Shell connections require both server and user authentication. The Secure Shell protocol also provides data encryption. When you configure Secure Shell connections in the **FTP Client**, you can use either of the following approaches to ensure that all transferred data is securely encrypted.

- Transfer files using the SFTP protocol.
- Transfer files using the FTP protocol and use tunneling to forward all communications through the secure SSH tunnel.

**Related Topics**

- “Connect Using Secure Shell (FTP Client)” on page 756
- “Forward FTP communications” on page 758

**Connect Using Secure Shell (FTP Client)**

The following procedure describes how to use Secure Shell for authentication and encryption in the **FTP Client**.

**To configure secure Shell connections in the **FTP Client****

1. Start the **FTP Client**.  
   This opens the **Connect to FTP Site** dialog box. (If the **FTP Client** is already running and this dialog box is not open, go to **Connection > Connect**.)
2 Perform one of the following tasks:

<table>
<thead>
<tr>
<th>To</th>
<th>Do This</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a new site</td>
<td>From the Connect to FTP Site dialog box, click New.</td>
</tr>
<tr>
<td></td>
<td>In the Add FTP Site dialog box, enter the name or IP address of your FTP server host, and then click Next.</td>
</tr>
<tr>
<td></td>
<td>In the Login Information dialog box, select User.</td>
</tr>
<tr>
<td>Modify an existing site</td>
<td>From the Connect to FTP Site dialog box, select a site.</td>
</tr>
</tbody>
</table>

3 Click Security.

4 Click the Secure Shell tab.

5 Select Use Reflection Secure Shell.

6 Select one of the following options:

- **SFTP**
  - Reflection will connect using SFTP (Secure FTP) protocol. SFTP supports fewer commands than the full FTP protocol.

- **Tunnel FTP using port forwarding**
  - Reflection will secure the port you specify for Local port through the SSH tunnel. With this configuration you have access to the full range of FTP commands. All communications are sent through the SSH tunnel. This includes FTP commands (including user name and password) and all transmitted data (including directory listings and the contents of the files you transfer).

7 (Optional) Specify an SSH config scheme. (If you leave SSH config scheme blank, Reflection saves any changes you make to an SSH configuration scheme with the same name as the current host.)

8 (Optional) Click Configure to open the Reflection Secure Shell Settings dialog box. Use this dialog box to configure user authentication and additional Secure Shell settings.

9 Perform one of the following tasks:

<table>
<thead>
<tr>
<th>If you are</th>
<th>Do This</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating a new site</td>
<td>Click OK to close the Security Properties dialog box and then click Next.</td>
</tr>
<tr>
<td></td>
<td>In the FTP User Login dialog box, type your user name on the FTP server and then click Next.</td>
</tr>
<tr>
<td></td>
<td>Click Finish.</td>
</tr>
<tr>
<td>Modifying an existing site</td>
<td>Click OK to close the open dialog boxes.</td>
</tr>
</tbody>
</table>

**NOTE**

- Host authentication enables the Secure Shell client to reliably confirm the identity of the Secure Shell server. This authentication is done using public key authentication. If the host public key has not previously been installed on the client, the first time you attempt to connect you see a message indicating that this is an unknown host. This message includes a fingerprint that identifies the host. To be sure that this is actually your host, you should contact the host system.
administrator who can confirm that this is the correct fingerprint. Until you know that the host is actually your host, you are at risk of a “man-in-the-middle” attack, in which another server poses as your host.

- In most cases Reflection will connect to your host and allow you to log in with your password using the default Secure Shell configuration. Use the **Reflection Secure Shell Settings** dialog box if you need to configure alternate user authentication methods or to make other changes to your Secure Shell configuration.

- The default **Server Type** setting for the FTP Client is **Auto detect**. This setting is not valid when Secure Shell is configured for SFTP. The FTP Client will automatically modify this setting from **Auto detect** to **UNIX** when you configure Secure Shell to use SFTP. To change to a different server type, use the **General** tab of the **Site > Properties** dialog box after you configure the Secure Shell settings.

**Related Topics**

- “Secure Shell Connections (FTP Client)” on page 756
- “Connect using Secure Shell (SSH)” on page 349
- “Reflection Secure Shell Settings Dialog Box” on page 353

**Forward FTP communications**

**Index Term**

Primary: tunneling
Secondary: Forward TCP communications

Index Term

Primary: tunneling
Secondary: Forward FTP communications

Index Term

Primary: port forwarding
Secondary: Forward TCP communications

Index Term

Primary: port forwarding
Secondary: Forward FTP communications

Index Term

Primary: SSH
Secondary: configure FTP forwarding

Index Term

Primary: Secure Shell
Secondary: configure FTP forwarding

Use this procedure to encrypt FTP protocol communications (including the FTP command channel and all data channels) using Secure Shell port forwarding. By using port forwarding, you can make secure connections to FTP servers and have access to the full range of FTP options and commands, including some that are not available with SFTP connections.

**NOTE:** To enable forwarding of the data channel(s), the FTP Client must be configured to communicate in passive (PASV) mode (the default).

**To forward FTP communications**

1. Start the FTP Client.
This opens the Connect to FTP Site dialog box. (If the FTP Client is already running and this
dialog box is not open, go to Connection > Connect.)

2 Perform one of the following tasks:

<table>
<thead>
<tr>
<th>To</th>
<th>Do This</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a new site</td>
<td>From the Connect to FTP Site dialog box, click New.</td>
</tr>
<tr>
<td></td>
<td>In the Add FTP Site dialog box, enter the name or IP address of your FTP server host, and then click Next.</td>
</tr>
<tr>
<td></td>
<td>In the Login Information dialog box, select User.</td>
</tr>
<tr>
<td>Modify an existing site</td>
<td>From the Connect to FTP Site dialog box, select a site.</td>
</tr>
</tbody>
</table>

3 Click Security.

4 Click the Secure Shell tab.

5 Select Use Reflection Secure Shell.

6 Select Tunnel FTP using port forwarding

7 This step is required only if your Secure Shell server is on a different host than the FTP server.
   - Select FTP host is different than Secure Shell host.

   **NOTE:** When you select FTP host is different than Secure Shell host, FTP commands and data are transmitted securely from your client computer to the Secure Shell server through a secure tunnel. The commands and data are transmitted in the clear between the Secure Shell server and the FTP server.

   - For SSH server address, type your Secure Shell server host name or IP address.
   - For SSH user name, type your login name on the Secure Shell server.

8 Perform one of the following tasks:

   If you are
<table>
<thead>
<tr>
<th>Creating a new site</th>
<th>Do This</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Click OK to close the Security Properties dialog box and then click Next.</td>
</tr>
<tr>
<td></td>
<td>In the FTP User Login dialog box, type your user name on the FTP server and then click Next.</td>
</tr>
<tr>
<td></td>
<td>Click Finish.</td>
</tr>
<tr>
<td>Modifying an existing site</td>
<td>Click OK to close the open dialog boxes.</td>
</tr>
</tbody>
</table>

   **NOTE:** You will need to authenticate to both the Secure Shell server and the FTP server.

**SSL/TLS Connections (FTP Client)**

The Secure Sockets Layer protocol (SSL) and its compatible successor, the Transport Layer Security protocol (TLS), enable a client and server to establish a secure, encrypted connection over a public network. When you connect using SSL/TLS, the client authenticates the server before making a connection, and all data passed between InfoConnect and the server is encrypted. Depending on the server configuration, the server may also authenticate the client.
Configure SSL/TLS (FTP Client)

Index Term
Primary: SSL/TLS
Secondary: configuring in the FTP Client

NOTE: SSL/TLS connections use digital certificates for authentication. Depending on how your certificate was issued and the way your host is configured, you may need to install a host and/or personal certificate before you can connect using SSL/TLS.

To configure a secure SSL/TLS connection in the FTP Client

1. Start the FTP Client.

   This opens the Connect to FTP Site dialog box. (If the FTP Client is already running and this dialog box is not open, go to Connection > Connect.)

2. Perform one of the following tasks:

   To | Do This
   ---|---------------------------------------------------------------
   Create a new site | From the Connect to FTP Site dialog box, click New.
       | In the Add FTP Site dialog box, enter the name or IP address of your FTP server host, and then click Next.
       | In the Login Information dialog box, select User.
   Modify an existing site | From the Connect to FTP Site dialog box, select a site.

3. Click Security.

4. Click the SSL/TLS tab, and then click Use SSL/TLS Security.

5. (Optional) To specify the minimum allowable level of encryption for SSL/TLS connections, select a level in the Encryption strength list. The connection fails if this level cannot be provided.

   NOTE: If you select Default, any encryption level is permitted, and InfoConnect negotiates with the host system to choose the strongest encryption level supported by both the host and the PC.

6. (Optional) Click Configure PKI.

   The PKI Configuration dialog box opens, from which you can manage the digital certificates used for authentication.

   6a Click Reflection Certificate Manager.

   6b In the Reflection Certificate Manager dialog box, select the Trusted Certificate Authorities tab.

   6c Click Import and browse to select the CA certificate for the server.

   6d Modify default settings as required. (For example, to use only the InfoConnect store, you might choose to clear Use System Certificate Store for SSL/TLS connections. When this option is selected, InfoConnect looks for certificates in both the InfoConnect store and the Windows certificate store.)

   When you customize any of the default PKI settings, the pki_config file is created.

   6e Close the Certificate Manager dialog box and click OK to close the other open dialog boxes.
The imported certificate is saved in the `trust_store.p12` file.

**6f** After a connection is established, click the Save button on the Quick Access toolbar and save the session document.

7 Perform one of the following tasks:

<table>
<thead>
<tr>
<th>If you are</th>
<th>Do This</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating a new site</td>
<td>Click <strong>OK</strong> to close the <strong>Security Properties</strong> dialog box and then click <strong>Next</strong>. In the <strong>FTP User Login</strong> dialog box, type your user name on the FTP server and then click <strong>Next</strong>. Click <strong>Finish</strong>.</td>
</tr>
<tr>
<td>Modifying an existing site</td>
<td>Click <strong>OK</strong> to close the open dialog boxes.</td>
</tr>
</tbody>
</table>

**NOTE**

- Before making an SSL/TLS connection, Reflection authenticates the host system. The certificate presented by the host for this purpose must be from a trusted certificate authority. If your computer does not recognize the certificate authority, you will not be able to make SSL/TLS connections. Depending on how a host certificate was issued, you may need to install the certificate on your computer.

- When you make an SSL/TLS connection, a padlock icon appears indicates that the data stream is encrypted. A key icon indicates that the command channel (including the entered password) is encrypted.

**Related Topics**

- “SSL/TLS Overview” on page 337
- “Digital Certificates in SSL/TLS Sessions” on page 341
- “Certificate Authentication (PKI)” on page 437
- “SSL/TLS Tab (FTP Options)” on page 521
- “Connect Using SSL/TLS” on page 339

**Working with FTP Client Settings Files**

The Reflection FTP Client uses settings files to save your configuration. Settings files use an `.RFW` file extension.

**Related Topics**

- “FTP Client Settings Files” on page 744

**In this Section**

- “Save your FTP Client Settings” on page 762
- “Load Saved FTP Client Settings” on page 762
- “Import FTP Client Settings” on page 763
- “Import WS_FTP Settings into FTP Client” on page 763
Save your FTP Client Settings

When you start the FTP Client from the Windows Start menu, the client automatically opens a settings file named Settings.rfw and any changes you make to your configuration are saved to this file. If you choose, you can also create additional settings files.

To save your settings to the currently open settings file

From the File menu, choose Save.

To save your settings to a different settings file

1. From the File menu, select Save As and save the .mst file to the same folder as the installer package file for Reflection (setup.exe).

2. Type a name for the file you are saving.

3. (Optional) Select Save shortcut on desktop if you want to save a shortcut to your desktop that will launch the client and open the settings file you are saving.

4. Click Save.

Load Saved FTP Client Settings

When you start the FTP Client from the Windows Start menu, the client automatically opens a settings file named Settings.rfw and any changes you make to your configuration are saved to this file. If you have created additional settings files, you can use either of these techniques to open them.

To open a settings file from the FTP Client

From the File menu, choose Open and then browse to locate your saved file.

To open a settings file using a Windows shortcut

1. When you save your settings file, create a shortcut to it.

2. Use this shortcut to launch the client and load that settings file.
Import FTP Client Settings

You can export FTP Client settings to XML format using the Export Settings command. This procedure imports settings from an XML file.

To import settings from an XML file

1. From the File menu, choose Import Settings.
2. Browse to locate the XML file that contains your site configuration.
3. Click Open.
   You will see a message telling you that the sites were imported successfully.
4. Click OK.

**NOTE:** Settings in the imported file are appended to any currently configured settings, and your session title is not changed. This is different from opening a saved settings file (*.rfw). When you open a settings file, the settings in that file replace any currently configured settings in the client, and your session title changes to the name of the open settings file.

Related Topics
- “Save your FTP Client Settings” on page 762
- “Create a Shortcut to Load a Settings File” on page 802
- “Import FTP Client Settings” on page 763
- “FTP Client Settings Files” on page 744

Import WS_FTP Settings into FTP Client

If you are migrating from WS_FTP, you can import your settings into FTP Client.

Before you begin, locate your wsftp_options.ini file, typically in one of the following locations:

C:\Users\<user>\AppData\Roaming\IPSwitch\WS_FTP
C:\Documents and Settings\<user>\Application Data\Ipswitch\WS_FTP

To import WS_FTP settings

1. From the FTP Client File menu, choose Import Settings.
2. From the Files of type drop-down list, select "Import WS_FTP (wsftp_options.ini)."
3. Browse to locate your wsftp_options.ini file, click Open, then click OK.
You should see a message saying that your settings were imported successfully.
Click **File > Save** to save the imported settings.

Related Topics
- “Save your FTP Client Settings” on page 762

### Save Changes on Exit Dialog Box

**Index Term**
- Primary: saving settings (FTP Client)
- Secondary: Save Changes on Exit

Reflection FTP Client displays the **Save Changes on Exit** dialog box if you have made any changes to your settings in the current session. The options are:

- **Save**: Saves all changes you have made to settings.
- **Discard**: Exits without saving any changes you have made during the current session.
- **Cancel**: Cancels the exit command and returns you to the Reflection session without saving any changes.

### Export FTP Settings Dialog Box

**Index Term**
- Primary: XML FTP Client file

**Index Term**
- Primary: saving settings (FTP Client)
- Secondary: exporting settings

**Index Term**
- Primary: exporting settings (FTP Client)

Getting there
- From the **FTP Client** File menu, choose **Export Settings**.

The options are:

**Sites**
Site-specific settings are configured using the **Site > Properties** dialog box or the **Directory Definition Wizard**. All settings are exported for each site with the exception of user name and password, which are included only when **User Settings** is also selected.

Select which of your currently configured sites are included in the exported settings file. Select a site and click **Remove** if you don't want the site included in the exported file.

**Application Settings**
Application settings affect the behavior of the FTP Client and are independent of both site and user. The following information is included:

- **Options** dialog box, **General** tab - Default local home folder
- **Options** dialog box, **File Types** tab - All features
- **Options** dialog box, **Preferences** tab - All features
User Settings

The following information is included:

- **Site Properties** dialog box - User and Password
- **Options** dialog box, General tab - Anonymous password
- Custom rules created using the Directory Definition Wizard.

File Name

Type a path and filename for the exported settings file. If you change the default filename, you must include a file extension if you wish to use one.

Related Topics

- “Change Global Settings for the FTP Client” on page 765
- “Change Settings for an FTP or SFTP Site” on page 769
- “Run the Directory Definition Wizard” on page 798

Configuring Site and Global Properties

In this Section

- “Change Global Settings for the FTP Client” on page 765
- “Change Settings for an FTP or SFTP Site” on page 769

Change Global Settings for the **FTP Client**

**Index Term**

*Primary: FTP Client*
*Secondary: global settings*

Global settings allow you to configure the default behavior for connections to all servers.

**To configure global settings**

1. From the **Tools** menu, choose **Options**.

Related Topics

- “General Tab (Options Dialog Box)” on page 765
- “File Types Tab (Options Dialog Box)” on page 766
- “Preferences Tab (Options Dialog Box)” on page 767
- “Change Settings for an FTP or SFTP Site” on page 769

**General Tab (Options Dialog Box)**

**Index Term**

*Primary: Options dialog box (FTP Client)*
*Secondary: General tab*

**Index Term**

*Primary: local home folder (FTP Client)*
*Secondary: global default*
Anonymous Password
Type the default password to use for anonymous connections to FTP sites.
This feature is not available for SFTP connections.

Default local home folder
Specify the folder that displays automatically when you start the client and receives files transferred from the server. Your Windows user folder is the default.

**Default local home folder** is a global default. It is ignored if you specify a site-specific value for **Home folder** on the **Directories** tab in the **Site > > Properties** dialog box.

You can specify a local home folder using UNC paths such as:
```
\\<computername>\<sharename>\<pathname>
```

Related Topics
- “Directories Tab (Site Properties Dialog Box)” on page 773

**File Types Tab (Options Dialog Box)**

Use this tab to configure Smart file transfer. When Smart file transfer is enabled, any file of a defined file type is transferred using the transfer method specified for that file type. To enable Smart file transfer, go to **Tools > Transfer Method > Smart.**
The options are:

- **Smart file transfer types**: Lists all file types that have been assigned a transfer method.
- **New**: Open the Add Smart File Type dialog box.
- **Delete**: Remove the currently selected file type from the list.
- **Change**: Edit the currently selected file type.
- **Transfer method for undefined file types**: Specify a default for files types that have no associated transfer method. If **Ask User** is specified, you are prompted to specify a transfer method when you transfer a file with that extension. At that time you can select a specific transfer method or choose **Always ask user**.

**Related Topics**

- “Set the Transfer File Type (Transfer Method)” on page 781
- “Add Smart File Type Dialog Box” on page 791

**Preferences Tab (Options Dialog Box)**

**Index Term**
- Primary: site-to-site transfer (**FTP Client**)
- Secondary: force through local computer

**Index Term**
- Primary: Options dialog box (**FTP Client**)
- Secondary: Preferences tab

**Index Term**
- Primary: FTP options
- Secondary: Preferences tab

**Getting There**

- From the FTP Client **Tools** menu, choose **Options**.
The options are:

**When the FTP Client exits**
Select how the client handles configuration changes. If you select **Save configuration automatically**, changes are saved to the current settings file.

**Confirm file delete**
Select whether the client prompts you for confirmation before deleting a file or folder.

**Hide progress window**
Suppress the connection progress, transfer progress, and error notification dialog boxes.

**Do not use animation**
By default Reflection uses animation during certain actions, for example a waving flashlight appears while you are waiting for a directory listing. Turning off the use of animation may fix some problems that cause Reflection to become unresponsive.

**Force site-to-site transfers through local machine**
Force all site-to-site transfers to copy files first to the local computer then to the destination server. Use this for FTP servers that don’t support direct site-to-site transfers.

**NOTE:** If there is a secure connection to either server, or the transfer type is not **Binary**, the client always transfers files this way, regardless of the value of this setting.

**Related Topics**
- “FTP Client Settings Files” on page 744
- “Working with FTP Client Settings Files” on page 761
- “Transfer Files between Two Remote Sites” on page 785

**File Attributes Tab (Options Dialog Box)**

**Getting There**
- From the FTP Client **Tools** menu, choose **Options**.

Use this tab to configure default attributes for file transfers.
Set default file attributes on uploads

Set default permissions for files copied to the server. When **Set default file attributes on uploads** is selected, you can specify permissions using either the **Permission Mode** box, or using the **Owner**, **Group**, and **Public** check boxes.

**NOTE**

- To specify non-default permissions during a file transfer, you can configure **Site Properties > Transfer > Show upload options before transfer**. When this setting is enabled, the **File Upload Options** dialog box is displayed before you transfer files to the server.

- When **Set default file attributes on uploads** is selected, the client sends a **chmod** command to the server to set the permissions you have specified. If your server does not support this command, you will receive a server error message that the **chmod** command is unrecognized.

Set default file attributes on downloads

Set default attributes for files copied to the client. When **Set default file attributes on downloads** is selected, you can specify attributes using the **Read-only** and/or **Hidden** check boxes.

**NOTE**: To specify non-default permissions during a file transfer, you can configure **Site Properties > Transfer > Show download options before transfer**. When this setting is enabled, the **File Download Options** dialog box is displayed before you transfer files to the client.

**Related Topics**

- “Set File and Directory Permissions” on page 798
- “Change the Filename when Downloading” on page 785
- “Change the Filename when Uploading” on page 786
- “Set Time and Date of Downloaded Files” on page 784

**Change Settings for an FTP or SFTP Site**

**Index Term**

**Primary**: FTP Client

**Secondary**: site-specific settings

Use the **Site Properties** dialog box to configure how the client behaves when connecting and interacting with a particular remote site.

**To modify the settings for a particular site**

1. Start the **FTP Client**.
   
   This opens the **Connect to FTP Site** dialog box. (If the **FTP Client** is already running and this dialog box is not open, go to **Connection > Connect**.)

2. From the **Connect to FTP Site** dialog box, select a site.

3. Click the **Properties** button.

**NOTE**

- If you are already connected to a site, from the **Connection** menu, choose **Site Properties**.
- Some changes you make using the **Site > Properties** dialog box when connected will not take effect until the next time you connect to the site.
Related Topics

- “General Tab (Site Properties Dialog Box)” on page 770
- “Connection Tab (Site Properties Dialog Box)” on page 771
- “Directories Tab (Site Properties Dialog Box)” on page 773
- “Translation Tab (Site Properties Dialog Box)” on page 776
- “Transfer Tab (Site Properties Dialog Box)” on page 777
- “Information Tab (Site Properties Dialog Box)” on page 779
- “Change Global Settings for the FTP Client” on page 765

General Tab (Site Properties Dialog Box)

Index Term
Primary: server settings (FTP Client)
Secondary: server type

Index Term
Primary: server settings (FTP Client)
Secondary: FTP address

Index Term
Primary: passwords
Secondary: save FTP site passwords

Index Term
Primary: FTP server type

Index Term
Primary: FTP address

Index Term
Primary: anonymous logins
Secondary: site-specific setting

Getting there

1 Start the FTP Client.
   This opens the Connect to FTP Site dialog box. (If the FTP Client is already running and this
dialog box is not open, go to Connection > Connect.)
2 From the Connect to FTP Site dialog box, select a site.
3 Click the Properties button.

NOTE

- If you are already connected to a site, from the Connection menu, choose Site Properties.
- Some changes you make using the Site > > Properties dialog box when connected will not take
effect until the next time you connect to the site.

Use this tab to provide connection information for the specified site.
The options are:

- **FTP address**: Type the FTP or SFTP server to log on to. This can be a domain name, a URL, or an IP address.

- **Server type**: In most cases, FTP Client will correctly identify your server when this value is set to *Auto detect*. If FTP Client is not successfully identifying the type of server you are connecting to, select it from this list.

  *Auto detect* is not available for SFTP sessions. The default for these sessions is *UNIX*.

### Log on as

- **Anonymous**: Log on to the FTP server as a guest, with the user name `anonymous`. (Anonymous logons are not allowed for SFTP connections.)

  If you log on to this server anonymously, the *Password* box is automatically filled in with the anonymous password specified on the *General* tab in the *Options* dialog box. If this FTP site expects a different password for anonymous users, type the site-specific password here.

- **User**: Log on to the specified server using a registered user name.

- **User name**: Type your user name as it is registered on the FTP server.

- **Save password**: Save your password as obfuscated text in your settings file and use it to log on to this server.

- **Password**: Type the password the FTP server associates with the user name.

### Security

Configure a secure connection to the specified server.

### Connection Tab (Site Properties Dialog Box)

- **Index Term**
  - Primary: PASV

- **Index Term**
  - Primary: Passive Mode

- **Index Term**
  - Primary: NOOP

- **Index Term**
  - Primary: keep alive
  - Secondary: FTP Client connections

- **Index Term**
  - Primary: FTP site properties
  - Secondary: Connection tab

### Getting there

1. Start the FTP Client.

   This opens the *Connect to FTP Site* dialog box. (If the FTP Client is already running and this dialog box is not open, go to *Connection > Connect*.)
2 From the Connect to FTP Site dialog box, select a site.
3 Click the Properties button.

NOTE

- If you are already connected to a site, from the Connection menu, choose Site Properties.
- Some changes you make using the Site > > Properties dialog box when connected will not take effect until the next time you connect to the site.

Use this tab to configure settings for maintaining connections and to set timeout intervals.

NOTE: For SFTP connections, the only setting available from this tab is Use IPV6.

Connection options

Use passive mode
When selected, the client sends a PASV command to communicate with the server in passive mode (sometimes called PASV mode). This initiates a separate data connection for directory listings and file transfers.

Use passive mode to minimize connection problems with firewalls, such as the Windows firewall enabled by default in some versions of Windows XP.

If passive mode has been turned off and a directory listing does not display or you get an error “425 Can’t open data connection,” you should enable this setting.

TCP port
Use the TCP port box to specify a non-standard TCP service port number or socket for FTP. The default value 21 is the standard service port for FTP.

Account
If your server requires an account name for file access, type it here. For case-sensitive servers, be sure to use the appropriate case.

When a connection is opened, if Account is filled in, the client automatically sends the account name to the server as the last logon step.

Timeouts in seconds

Connect
Select the maximum number of seconds to continue trying to establish an FTP server connection. Entering 0 (zero) in this box prevents the FTP Client from ever timing out on a connection attempt.

Session
Select the maximum number of seconds to wait for data packets being transferred to or from the host. If nothing is received within the period specified, a timeout error displays and the transfer is aborted; in this case, try the operation again. If you receive repeated timeout errors, increase the timeout value. Entering 0 (zero) in this box prevents the FTP Client from ever timing out when waiting for a response.

Other settings

Use IPV6
Select whether connections to the host use IPV6 (Internet Protocol version 6) or the older IPv4 protocol. By default, the client attempts to connect using IPv6, and uses IPv4 when IPv6 is not available. You may need to change this value to "Never" if you are having problems connecting to hosts on an IPv4 network from a client computer with IPv6 enabled.
Initial umask

Use this setting to specify an initial umask value to send to the server upon connection. You can use umask to modify the default permissions attributes set on newly created files. When you specify a umask, the client sends the following to the FTP server when you login, where nnnn is your specified umask value.

SITE umask nnnn

To find out if umask is a supported SITE command for your FTP server, enter this command at the FTP command line:

QUOTE help site

NOTE

- The umask set by the FTP client cannot be less restrictive than user permissions set on the server.
- This option is not available if you have configured global upload attributes using Tools > Options > Attributes > Set default attributes on uploads.
- This option is not available for SFTP connections.

Directories Tab (Site Properties Dialog Box)

Index Term
Primary: show directory upon connection (FTP Client)

Index Term
Primary: server settings (FTP Client)
Secondary: show directory upon connection

Index Term
Primary: server settings (FTP Client)
Secondary: home directory setting

Index Term
Primary: server settings (FTP Client)
Secondary: display file names only

Index Term
Primary: server settings (FTP Client)
Secondary: Directories Tab (Site Properties dialog box)

Index Term
Primary: Resolve links

Index Term
Primary: Refresh directory automatically

Index Term
Primary: PWD

Index Term
Primary: NLST

Index Term
Primary: local home folder (FTP Client)
Secondary: site-specific

Index Term
Primary: LIST command parameters
Index Term
Primary: FTP site properties
Secondary: Directories tab

Index Term
Primary: File View Filter

Index Term
Primary: file names (FTP Client)
Secondary: display file names only

Index Term
Primary: directory management (FTP servers)
Secondary: Directories Tab (Site Properties dialog box)

Index Term
Primary: cache directory listing

Getting there

1 Start the FTP Client.
This opens the Connect to FTP Site dialog box. (If the FTP Client is already running and this
dialog box is not open, go to Connection > Connect.)

2 From the Connect to FTP Site dialog box, select a site.

3 Click the Properties button.

NOTE
- If you are already connected to a site, from the Connection menu, choose Site Properties.
- Some changes you make using the Site > > Properties dialog box when connected will not take
effect until the next time you connect to the site.

Use this tab to specify how your directory listings are displayed. The options are:

Server

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Home directory</td>
<td>Select the host directory to which InfoConnect should be set after an</td>
</tr>
<tr>
<td></td>
<td>FTP connection is made.</td>
</tr>
<tr>
<td>Show directory upon connection</td>
<td>Select whether a list of the files and folders in the working server</td>
</tr>
<tr>
<td></td>
<td>directory is displayed in the right pane each time you open a connection</td>
</tr>
<tr>
<td></td>
<td>to this site. If you choose not to show server directories and you want to</td>
</tr>
<tr>
<td></td>
<td>change to a different server directory, use the Go To command on the Tools</td>
</tr>
<tr>
<td></td>
<td>menu or use the “CD” on page 859 command at the FTP command line.</td>
</tr>
<tr>
<td>Refresh directory automatically</td>
<td>Select whether the server directory listing shown in the right pane is</td>
</tr>
<tr>
<td></td>
<td>updated when you execute a “CD” on page 859 command, or perform any</td>
</tr>
<tr>
<td></td>
<td>operation that adds or deletes files or directories on the server.</td>
</tr>
<tr>
<td>Try to convert to dates to local</td>
<td>Select whether dates display in the format specified by the regional</td>
</tr>
<tr>
<td>system format</td>
<td>settings in Windows Control Panel. Leave this check box cleared if you</td>
</tr>
<tr>
<td></td>
<td>want dates to display in the date format used on the server.</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Resolve links</strong></td>
<td>Select how directory listings are created when you are connected to a server that supports symbolic links. When this box is checked, the server pane correctly uses folders to display symbolic links that identify directories. Clear this box if you don’t need this feature and you want to improve response time for new or refreshed file listings.</td>
</tr>
<tr>
<td><strong>Cache directory listing</strong></td>
<td>Select whether directory listings are cached on your local PC. Using cached directory listings speeds up the server pane display as you navigate through your server directories, but will not reflect changes you have made to your server files. When this box is cleared, file listings are updated from the server each time you change the display.</td>
</tr>
<tr>
<td><strong>Display file names only</strong></td>
<td>Select whether directory listings include filenames only. You can use this setting as a troubleshooting tool if the client is having difficulty displaying directory listings for your host. When this check box is cleared, file listings are created using the FTP LIST command; when it is selected, file listings use NLST. This setting does not apply to SFTP connections.</td>
</tr>
<tr>
<td><strong>Don't send PWD command</strong></td>
<td>When this option is selected, the FTP Client does not send a PWD command when you are connected to the server. Enabling this setting may fix connection problems encountered with some hosts. When it is enabled, the current server directory path won’t be displayed in the server’s title bar, and the Go to a different Folder list box (located on the left side of the toolbar), will not display host directory information. You will see your local PC directories even when the server pane is selected.</td>
</tr>
<tr>
<td><strong>File View Filter</strong></td>
<td>Type a default file view filter for the server using wildcard characters that are recognized by the server. For more information, see the “Filter the Server File Listing” on page 797 topic. This feature is not available for SFTP connections.</td>
</tr>
<tr>
<td><strong>LIST command parameters</strong></td>
<td>Specify the command parameters the FTP Client uses when it sends an FTP LIST command to the server. The appropriate parameters depend on the type of server you are connecting to. Changing this value may help troubleshoot some problems. Use caution when modifying LIST command parameters for use with the “MDEL” on page 836 command. On some systems the list can be set to recursively list files in subfolders. This feature is not available for SFTP connections.</td>
</tr>
<tr>
<td><strong>Show attributes before creating directory</strong></td>
<td>Select this option to see a dialog box that enables you to set directory permissions whenever you create a new directory on the server.</td>
</tr>
</tbody>
</table>
Local

**Home folder**
Type the path to a home (default) folder for the FTP Client. When a connection to the site is opened, the local working folder is set automatically to the specified home path and that location will receive any server files you transfer using the **Download** command.

The global **Default local home** folder setting is ignored for this site.

---

**Related Topics**
- "Filter the Server File Listing" on page 797

**Translation Tab (Site Properties Dialog Box)**

**Index Term**
Primary: Translation tab (**FTP Client**)  
Secondary: Translation tab

**Getting there**

1. **Start the FTP Client.**  
   This opens the **Connect to FTP Site** dialog box. (If the FTP Client is already running and this dialog box is not open, go to **Connection > Connect**.)

2. **From the Connect to FTP Site** dialog box, select a site.

3. **Click the Properties button.**

---

**NOTE**
- If you are already connected to a site, from the **Connection** menu, choose **Site Properties**.
- Some changes you make using the **Site > Properties** dialog box when connected will not take effect until the next time you connect to the site.

Use this tab to control conversion of formatting characters in ASCII data transferred to the client or to the server.

---

**NOTE:** **Translation** tab settings are not available for SFTP connections.
To server

**Change tabs to spaces**  
Spaces replace tab characters in uploaded files.

**Spaces per tab**  
Define the size of the tab stops used if you change spaces to tabs or tabs to spaces.

**Read CTRL-Z as end of file**  
When selected, file transfer uses a Ctrl-Z (^Z) character as the end-of-file marker, and strips it from the file being sent. Otherwise, the character count in the file directory is used to determine the file length.

The FTP Client never sends Ctrl-Z if it is the last character in an ASCII file.

From server

**Change spaces to tabs**  
Select to have tab characters replace consecutive spaces in downloaded files. Use **Spaces per tab** (under To server) to specify how many spaces equal one tab.

**Write Ctrl-Z at end of file**  
On the local computer, ASCII text files normally end with a Ctrl-Z (^Z) character. If you want a ^Z character added to the file when it is received from the server, keep this option selected. Some Windows applications require this marker.

**Delete trailing spaces**  
Select to save local disk space. Some host text files use fixed-length records to delimit lines; they pad the end of each record with blanks. Most PC text processing programs use a carriage return and linefeed sequence to delimit lines and paragraphs, and thus do not need blanks preceding a delimiter.

**A six digit date on the server**

represents  
Select how six digit dates on the server are interpreted. **MM** represents the month, **DD** the day, and **YY** the year.

**Additional options**

**Character Sets button**  
Open the **Character Sets** dialog box to configure translation between the server character set and either the Windows or DOS character set.

## Related Topics

- “Character Sets Dialog Box” on page 788

## Transfer Tab (Site Properties Dialog Box)

**Index Term**

Primary: FTP site properties
Secondary: Transfer tab

### Getting there

1. **Start the FTP Client**
   
   This opens the **Connect to FTP Site** dialog box. (If the FTP Client is already running and this dialog box is not open, go to **Connection > Connect**.)

2. **From the Connect to FTP Site** dialog box, select a site.

3. **Click the Properties button.**
**NOTE**

- If you are already connected to a site, from the **Connection** menu, choose **Site Properties**.
- Some changes you make using the **Site > > Properties** dialog box when connected will not take effect until the next time you connect to the site.

Use this tab to specify how filenames and dates are handled during file transfers to and from the server. The options are:

### Download from server options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Preserve server file date</strong></td>
<td>Retain the original date stamps associated with downloaded files. If you want files transferred from the server to be date stamped with the time and date when they were transferred, keep this check box cleared.</td>
</tr>
<tr>
<td><strong>NOTE:</strong></td>
<td>Server file dates will not be preserved if the <strong>Display file names only</strong> setting on the <strong>Directories</strong> tab has been enabled.</td>
</tr>
<tr>
<td></td>
<td>Server file dates are not preserved when files are dragged to the Windows desktop or Windows Explorer folder. Drag files to the local pane of the FTP Client to preserve file dates.</td>
</tr>
<tr>
<td></td>
<td>To retain original server dates in transfers done by a script, you can either load your site settings when you launch the script (page 804) or add the following line to the beginning of the script:</td>
</tr>
<tr>
<td></td>
<td><code>PRESERVE-FILE-DATE yes</code></td>
</tr>
<tr>
<td><strong>Create Windows file names in 8.3 format</strong></td>
<td>Select to receive host files in the DOS 8.3 filename format. For example, a file with the name <code>Longfilename.Document</code> will be converted automatically to <code>Longfile.doc</code> when transferred to your PC.</td>
</tr>
<tr>
<td><strong>NOTE:</strong></td>
<td>During wildcard transfers with this check box selected, if two long filenames translate to the same DOS 8.3 format name, the second file transferred will overwrite the first when <strong>If File Exists</strong> is set to <strong>Overwrite</strong>. To prevent this, change the <strong>If File Exists</strong> setting to <strong>Unique</strong>.</td>
</tr>
<tr>
<td><strong>Try to resume partial binary downloads</strong></td>
<td>Select to have the FTP Client try to resume downloading the untransferred portion of files after an interruption.</td>
</tr>
<tr>
<td></td>
<td>For more information, see the “<strong>Resume an Incomplete Server File Download</strong>” on page 787 topic.</td>
</tr>
<tr>
<td><strong>Show download options before transfer</strong></td>
<td>Select this option if you want to be queried for the transfer method (for example, ASCII or binary) and file properties (read-only or hidden) before downloading a new file from the server.</td>
</tr>
</tbody>
</table>

### Upload to server options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Remove file name extension</strong></td>
<td>Remove the filename extension from files transferred to the host. If an uploaded file’s name contains one or more dots, the final dot and any subsequent characters are removed from the filename.</td>
</tr>
<tr>
<td><strong>Prepend these characters to the file name</strong></td>
<td>Add the specified characters before the filename for files copied to the host. For example, you can use this feature to specify a member name for transfers to an IBM host. If you are connected to an HP POSIX host, the client automatically sets this value to a period followed by a slash (<code>./</code>).</td>
</tr>
</tbody>
</table>
**Server file name limit** | Set a limit to the number of characters in the filename for files transferred to the host. Filenames beyond this limit are truncated.
---|---
**Set case for long file names transferred to server** | Select how case is handled in when the transferred filename does not conform to the DOS 8.3 file naming convention.
---|---
**Set case for 8.3 file names transferred to server** | Select how case is handled when the transferred filename does conform to the DOS 8.3 file naming convention.
---|---
**Compute space on MVS** | By default, the FTP Client computes and preallocates the number of tracks on MVS system based on the local file size. Clear this option to disable this feature. This setting applies to uploads to MVS hosts only.
---|---
**Send SITE command before transfer** | Type a SITE command to be executed before a file is uploaded. To find out what SITE commands are supported by the current FTP server, enter this command at the FTP command line:

```
QUOTE help site
```
This feature is not available for SFTP connections.
---|---
**Show upload options before transfer** | Select this option if you want to be queried for the transfer method (for example, ASCII or binary) and file permission attributes before uploading a new file to the server.

---

**Related Topics**

- “Handle Existing Files (Transfer Mode)” on page 783
- “Resume an Incomplete Server File Download” on page 787
- “Directories Tab (Site Properties Dialog Box)” on page 773
- “Set Time and Date of Downloaded Files” on page 784

---

**Information Tab (Site Properties Dialog Box)**

**Index Term**

Primary: FTP site properties
Secondary: Information tab

**Getting there**

1. Start the FTP Client.
   This opens the Connect to FTP Site dialog box. (If the FTP Client is already running and this dialog box is not open, go to Connection > Connect.)
2. From the Connect to FTP Site dialog box, select a site.
3. Click the Properties button.

---

**NOTE**

- If you are already connected to a site, from the Connection menu, choose Site Properties.
- Some changes you make using the Site > Properties dialog box when connected will not take effect until the next time you connect to the site.

This tab shows information about the current FTP Client connection. It is available only when you are connected to a site.
Click **Reset** to reset the transfer time and transfer rate data to zero.

**Transferring Files**

In this Section

- “Transfer Files with FTP Client” on page 780
- “Set the Transfer File Type (Transfer Method)” on page 781
- “Add a Smart File Transfer Type” on page 782
- “Specify a Default Smart File Transfer Type” on page 783
- “Handle Existing Files (Transfer Mode)” on page 783
- “Set Time and Date of Downloaded Files” on page 784
- “Transfer Files between Two Remote Sites” on page 785
- “Change the Filename when Downloading” on page 785
- “Change the Filename when Uploading” on page 786
- “Resume an Incomplete Server File Download” on page 787
- “Character Sets Dialog Box” on page 788
- “Add Smart File Type Dialog Box” on page 791
- “Smart Transfer File Type Dialog Box” on page 791
- “Confirm File Replace Dialog Box” on page 792

**Transfer Files with FTP Client**

Index Term
Primary: transferring files (**FTP Client**)  
Secondary: using drag-and-drop

Index Term
Primary: transferring files (**FTP Client**)  
Secondary: how to

Index Term
Primary: FTP Client  
Secondary: how to transfer files

Index Term
Primary: file transfers (**FTP Client**)  
Secondary: how to transfer

You can transfer files in the FTP Client with a simple drag and drop operation. You can drag individual files, multiple files, and entire folders.

**To transfer files with FTP Client**

1. Connect to an FTP site.
2. Specify a transfer method (**Tools** > **Transfer Method**).
3. Set the preference for handling existing files. (**Tools** > **If File Exists**).
NOTE: Additional file transfer settings are available from the Site > Properties dialog box. You can use these site-specific properties to configure file transfer.

4 Browse to locate the files or folders you want to transfer and the destination location.
5 Select the files or folders you want to transfer and drag them from the source location to your desired destination.

NOTE: If you prefer to transfer files using FTP (or SFTP) file transfer commands, you can initiate transfers directly from the FTP command line.

Related Topics
- “Connect to a Site” on page 745
- “Set the Transfer File Type (Transfer Method)” on page 781
- “Handle Existing Files (Transfer Mode)” on page 783
- “View the Local PC Files” on page 742
- “View the Server Files” on page 743
- “Use the FTP Command Line” on page 817

Set the Transfer File Type (Transfer Method)

Use Transfer Method to specify the file type for transfers. The currently active transfer method is indicated on the status bar, on the toolbar, and in the Transfer Method menu.

To change the current file transfer method
- From the Tools menu, point to Transfer Method and then click the transfer method you want to use.
The options are:

**ASCII**

Select **ASCII** for text files. ASCII data is transferred according to settings in the **Character Sets** dialog box.

**Binary**

Use the **Binary** transfer method to transfer binary files, such as **.exe** files and **.doc** files. Binary files are not converted or translated during the transfer.

**Tenex (Local 8)**

Select **Tenex** (also known as "Local 8") if you're moving files to or from a server that uses a non-8-bit byte, such as the DECsystem-20.

**Smart**

Select **Smart** if you want the **FTP Client** to determine what transfer method to use (**ASCII**, **Binary**, **Tenex**, or **Ask User**) based on the source file extension. To configure this, use **Tools > Options > File Types**.

Related Topics

- "Character Sets Dialog Box" on page 788
- "Add a Smart File Transfer Type" on page 782
- “Specify a Default Smart File Transfer Type” on page 783
- “Add Smart File Type Dialog Box” on page 791

### Add a Smart File Transfer Type

**Index Term**

Primary: Smart file transfer (**FTP Client**)  
Secondary: adding file types

**Index Term**

Primary: file transfers (**FTP Client**)  
Secondary: smart file transfer

Use the Smart transfer method if you want the **FTP Client** to determine which transfer method to use (**ASCII**, **Binary**, **Tenex**, or **Ask User**) based on the source file extension. When performing a Smart file transfer, the client refers to the list of Smart file types to determine what transfer method to use for the current file. You can add file types to the default Smart file types list, or change the file transfer method used for existing file types. For example, you might specify that files with names ending in **.doc** use the **Binary** transfer method.

**To add a new Smart file transfer type**

1. From the **Tools** menu, choose **Options**.
2. Click the **File Types** tab.
3. Click **New**.
4. Use the following settings from the **Add Smart File Type** dialog box to define a new file type:
To define a transfer method for files that don't have an extension, choose `<none>` in the `File type` box, and then select a transfer method.

If a file extension might identify files of several types, you can specify `Ask User` as the transfer method for that extension.

### Related Topics
- “Set the Transfer File Type (Transfer Method)” on page 781
- “Specify a Default Smart File Transfer Type” on page 783
- “Add Smart File Type Dialog Box” on page 791

## Specify a Default Smart File Transfer Type

The default Smart transfer type applies to any file types that have not been defined previously.

### To specify a default Smart file transfer type

1. From the **Tools** menu, choose **Options**.
2. Click the **File Types** tab.

**NOTE**: If you have files that have the same file extension, but require a different transfer method, do not set a default type. Set **Transfer method for undefined file types** to **Ask User**. Or, set the file transfer method you want to use prior to transferring the file(s).

### Related Topics
- “Set the Transfer File Type (Transfer Method)” on page 781
- “Add a Smart File Transfer Type” on page 782

## Handle Existing Files (Transfer Mode)

**Index Term**

Primary: transferring files (FTP Client)
Secondary: if file exists

**Index Term**

Primary: file transfers (FTP Client)
Secondary: if file exists at destination
You can set a transfer mode to specify how the FTP Client should handle transfer when a file with the same name already exists in the target location. The current transfer mode is indicated on the status bar next to the transfer method.

**To specify how to handle existing files**

- From the **Tools** menu, point to **If File Exists** and then click the transfer mode you want to use.

<table>
<thead>
<tr>
<th>Transfer Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Append</strong></td>
<td>Append the downloaded file to the destination file. This option is only available for transfers from the host.</td>
</tr>
<tr>
<td><strong>Ask User</strong></td>
<td>Open the <strong>Confirm File Replace</strong> dialog box to allow the user to decide what to do.</td>
</tr>
<tr>
<td><strong>Cancel</strong></td>
<td>The file transfer is canceled when a file with the specified name already exists. If the file is part of a wildcard set (files being transferred using wildcards or a string of filenames), no other files are transferred to the PC after a duplicate is found.</td>
</tr>
<tr>
<td><strong>Overwrite</strong></td>
<td>Overwrite the destination file.</td>
</tr>
<tr>
<td><strong>Skip</strong></td>
<td>Do not transfer this file. If additional files are specified for this transfer operation, continue with the next file.</td>
</tr>
<tr>
<td><strong>Update</strong></td>
<td>Overwrite the destination file only if the file being transferred is newer than the destination file.</td>
</tr>
<tr>
<td><strong>Unique</strong></td>
<td>Automatically create a unique name for the destination file. The names of any files that are renamed during the transfer operation are shown in the FTP command window.</td>
</tr>
</tbody>
</table>

**NOTE:** In some circumstances, this setting is ignored. The value you specify using the **If File Exists** command applies only to transfers within the FTP Client. If you use drag-and-drop to transfer a file from a client display pane to your desktop or an open Windows Explorer window, Windows will always display a **Confirm File Replace** dialog box whenever a file exists, regardless of the FTP Client configuration. To take advantage of the currently configured option, always use Reflection panes for drag-and-drop transfers.

**Related Topics**

- “Confirm File Replace Dialog Box” on page 792
- “Transfer Files with FTP Client” on page 780
- “Commands for Error Handling” on page 823

**Set Time and Date of Downloaded Files**

**Index Term**
- **Primary:** transferring files (FTP Client)
- **Secondary:** configuring file dating

**Index Term**
- **Primary:** file transfers (FTP Client)
- **Secondary:** handling file dates
Index Term
Primary: dates
Secondary: in FTP Client transfers

1. Open the Site Properties dialog box and then click the Transfer tab.
2. Select Preserve server file date if you want all files transferred from the server to retain the original time and date. Clear this box if you want files transferred from the server to be stamped with the time and date when they were transferred.

Related Topics
- “Change Settings for an FTP or SFTP Site” on page 769
- “Transfer Tab (Site Properties Dialog Box)” on page 777

Transfer Files between Two Remote Sites

Index Term
Primary: transferring files (FTP Client)
Secondary: site-to-site transfer

Index Term
Primary: site-to-site transfer (FTP Client)
Secondary: procedure

You can use the FTP Client to drag files between two remote sites.

To transfer files between two remote sites

1. Connect to your first server site.
2. From the Connection menu, click Connect to a second site.
   The server pane will display files and folders for both sites.
3. Use the drag-and-drop method to transfer files directly from one server to another.

NOTE
- If the transfer type is Binary and both connections are configured without security features in place (such as use of a proxy server, Kerberos, Secure Shell, port forwarding, or sftp) the data is transferred directly over the data channel between the two sites.
- If there is a secure connection to either server, or the transfer type is not Binary, the client downloads the file to a temporary location on your PC and then uploads it to the other site. The temporary file is deleted after the transfer is complete.

Related Topics
- “Transfer Files with FTP Client” on page 780
- “Connect to a Site” on page 745
- “Preferences Tab (Options Dialog Box)” on page 767

Change the Filename when Downloading

Index Term
Primary: transferring files (FTP Client)
Secondary: using Download As
The **Download As** command is available when you right-click on a file in the server pane. You may prefer this command over drag-and-drop file transfer when you want to transfer a server file to your PC and use a different file name on the PC.

**To download a file using a different name**

1. Right-click on the file you want to download, and then choose **Download As**.
2. From the **Download As** dialog box, in the **Download As** box, type the name you want to use for the file on the PC.
3. Click **OK** to complete the transfer.

Also, wildcard characters are supported. You can download multiple files at once, changing all of the filenames. For example, you could change all of the `.htm` files in a directory to `.html` when you download them to your PC.

**To download multiple files using a different name**

1. Right-click on one of the files you want to download, and then choose **Download As**.
2. From the **Download As** dialog box, in the **Server file(s)** box, replace one or more parts of the filename with wildcards, leaving enough to identify which files you want.
   
   For example, `*.htm` or `*_info_???.text`
3. From the **Download As** dialog box, in the **Download As** box, make the same wildcard replacements, and change the part of the filename you want to make different on your PC.
   
   For example, `*.html` or `*_info_???.txt`.
4. Click **OK** to complete the transfer.

**Related Topics**

- “View the Server Files” on page 743
- “Transfer Files with FTP Client” on page 780

**Change the Filename when Uploading**

The **Upload to Server** command is available when you right-click on a file in the left pane of the FTP Client. You may prefer this command over drag-and-drop file transfer when you want to transfer a local file to the server and use a different file name on the server.
To upload a file using a different name

1. Right-click on the file you want to upload, and then choose **Upload As**.
2. From the **Upload As** dialog box, in the **Upload As** box, type the name you want to use for the file on the server.
3. If you are connected to two remote sites, both site names will appear in the **Upload As** dialog box. Select the site to which you want the file transferred.
4. Click **OK** to complete the transfer.

Also, wildcard characters are supported. You can upload multiple files at once, changing all of the filenames. For example, you could change all of the `.htm` files in a directory to `.html` when you upload them to the server.

To upload multiple files using a different name

1. Right-click on one of the files you want to upload, and then choose **Upload As**.
2. From the **Upload As** dialog box, in the **Source file(s)** box, replace one or more parts of the filename with wildcards, leaving enough to identify which files you want.
   
   For example, `*.htm` or `*_info_???.text`
3. From the **Upload As** dialog box, in the **Upload As** box, make the same wildcard replacements, and change the part of the filename you want to make different on your server.
   
   For example, `*.html` or `*_info_???.txt`.
4. Click **OK** to complete the transfer.

Related Topics

- "View the Local PC Files" on page 742
- "Transfer Files with FTP Client" on page 780

Resume an Incomplete Server File Download

**Index Term**

Primary: transferring files (FTP Client)
Secondary: resuming incomplete download

**Index Term**

Primary: resume incomplete file transfer

**Index Term**

Primary: Reget (FTP Client)

**Index Term**

Primary: file transfers (FTP Client)
Secondary: resuming incomplete download

**Index Term**

Primary: auto resume (FTP Client)
Secondary: how to resume an incomplete download

Sometimes when downloading a server file to your PC, the transfer does not complete successfully, perhaps due to a loss of the network connection on a "noisy" or low-speed link.

**NOTE:** This feature is not available for SFTP connections.
When a file transfer fails to complete, the auto resume feature lets you resume the incomplete file transfer operation. The auto resume feature works only under these circumstances:

- The FTP server must support the REST command

To auto resume a file transfer, the FTP Client sends a REST command (restart) to the server. If the server does not support the REST command, the file transfer will start from the beginning of the file. For each site, after the first auto resume operation is attempted, the FTP Client will remember the result. If the server does not support the REST command, the Client won’t attempt to perform an auto resume for any file transferred from that server.

To determine if a particular server supports this feature, enter the following on the command line:

```
quote help rest
```

If `rest` is identified as a restart command, your server supports the feature

- File transfer method (or type) must be Binary

Auto resume compares the size of the source file to the size of the incomplete target file to determine at what point in the source file it should resume the transfer. An ASCII file transfer creates a file on the local machine that may differ in size from the source file.

- File transfer mode cannot be Append

When you transfer a file using the Append mode, the FTP Client can’t use the existing target file size to determine the restarting point to use in the source file.

To resume an incomplete download

1. If necessary, reconnect to the server where the source file resides.
2. Confirm the three circumstances above.
3. From the Transfer tab of the Site Properties dialog box, select **Try to resume partial binary downloads**.
4. Restart the server file download. For example, select the server file that failed to transfer and drag it again to the destination on your PC.
5. The client detects that a prior incomplete file transfer operation occurred for that file, and gives you the option to resume the incomplete transmission at the interruption point, instead of beginning a new file transfer of the entire file.
6. Click **Resume**.

Related Topics

- “Set the Transfer File Type (Transfer Method)” on page 781
- “Handle Existing Files (Transfer Mode)” on page 783
- “Transfer Tab (Site Properties Dialog Box)” on page 777

**Character Sets Dialog Box**

**Index Term**

Primary: character translation
Secondary: character translation (**FTP Client**)

**Getting There**

1. From the **Connect to FTP Site** dialog box, select a site, and then click the **Properties** button.
   - Or-

---

788  InfoConnect 2014 User’s Guide
If you are already connected to a site, from the Connection menu, choose Site Properties.

2 Click the Translation tab and then click the Character Sets button.

The need to translate characters is dictated by differences between the character set used by the source and the character set used at the destination. In most situations, no translation is necessary.

- If both client and server use the DOS character set, no translation is necessary.
- If the client uses the Windows character set and the server uses the ISO-Latin-1 character set, no translation is necessary.

The FTP Client can translate between the server character set and either the Windows or DOS character set. These settings apply to ASCII file transfers and characters sent from the server that are written to the screen.

**NOTE:** This feature is not available for SFTP connections.

The options are:

- **Translate files**
  Enable translation of ASCII files. Character translations occur when a PC file is sent to the server and when characters sent from the server are written to a client file.

- **Translate server messages**
  Enable translation when characters sent from the server are written to the screen.

- **Detect server Kanji type**
  Specify that character translation should be based on the type of Kanji character set detected in a file or message. This option is available only when Server is set to EUC, DEC 1983 Kanji, or JIS X0208-1983, and either Translate files or Translate server messages is selected.

  Clear this check box to use the specified Server Kanji character set at all times.

- **Client**
  Specify the character set to use on the client PC when Translate files is selected. The default setting is the current Windows character set.

- **Server**
  Specify the character set to use during ASCII file transfers (if Translate files is selected) and when translating server messages (if Translate server messages is selected).

- **ISO-7/NRC**
  Specify the national character set (NRC) to use for replacement purposes. Translation replaces certain characters from the ASCII set with accented characters and symbols for a specific national language.

  This option is only available when the Server character set is DEC Supplemental, ISO Latin-1, or HP Roman 8 and Change Roman-8 to ISO-7 and Change ISO-7 to Roman-8 are selected, or Change MCS to NRC and Change NRC to MCS are selected.
To server

These options are available only when either Translate files or Translate server messages is selected.

Change Roman-8 to ISO-7

If ISO-7/NRC is set to a value other than US ASCII, select this option to have Roman 8 characters translated to an equivalent ISO-7 character when possible. The ISO-7/NRC value determines the character conversion.

This option is available only when the Server character set is HP Roman 8.

Change MCS to NRC

Specify whether characters are translated from the DEC multinational character set (MCS) to the current national replacement character (NRC) set. The ISO-7/NRC value determines the character conversion.

This option is available only when the Server character set is DEC Supplemental or ISO Latin-1.

Half- to full-width Katakana

Specify whether characters are translated from the current half-width Katakana character set to the full-width Katakana character set.

The Server value determines which Kanji character set is used during the conversion.

This option is available only when the Server character set is one of the JIS types (except Shift-JIS), the two DEC Kanji types, and EUC (Unicode).

From server

These options are available only when either Translate files or Translate server messages is selected.

Change ISO-7 to Roman-8

If ISO-7/NRC is set to a value other than US ASCII, select this option to have ISO-7 characters converted to equivalent Roman 8 characters. The ISO-7/NRC value determines the character conversion.

This option is available only when the Server character set is HP Roman 8.

Change NRC to MCS

Specify whether characters should be translated from the current national replacement character (NRC) set to the DEC multinational character (MCS) set. The ISO-7/NRC value determines the character conversion.

This option is available only when the Server character set is DEC Supplemental or ISO Latin-1.

Full- to half-width Katakana

Specify whether characters are translated from the current full-width Katakana character set to the half-width Katakana character set.

The Server value determines which Kanji character set is used during the conversion.

This option is available only when the Server character set is one of the JIS types (except Shift-JIS), the two DEC Kanji types, and EUC (Unicode).
Add Smart File Type Dialog Box

Getting There

1. From the Tools menu, choose Options.
2. Click the File Types tab, and then click New.

When Smart file transfer is enabled, all filenames with a specified extension are transferred using the associated transfer method.

<table>
<thead>
<tr>
<th>File type</th>
<th>Type a file extension to associate with a specific transfer method, or select a file type from the list.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transfer method</td>
<td>Select the transfer method you want to use for files with this extension.</td>
</tr>
</tbody>
</table>

Smart Transfer File Type Dialog Box

This dialog box appears when you have selected the Smart transfer method and you are transferring a file with an undefined file type. Specify what transfer method you want to use for files with this file extension.

**NOTE:** Save your settings file to add this association permanently to your Smart file transfer list.

The options are:

- **ASCII**
  Use ASCII transfer for text files, such as .txt and .html.

- **Binary**
  Use binary transfer for binary files, such as .exe files and .doc files. Binary files are not converted or translated during the transfer.

- **Tenex**
  Use Tenex (also known as "Local 8") if you're moving files to or from a server that uses a non-8-bit byte, such as the DECsystem-20.

- **Always ask user**
  Select this option if you always want to be asked how to handle files with this extension. For example, you might want to select this option if the same file extension is used for different file types.

  **NOTE:** This option is not available if Always ask user has already been specified for this file type.
Confirm File Replace Dialog Box

When If File Exists is set to Ask User, this dialog box opens each time a client or server file being transferred already exists on the destination. The options are:

- **Append server file to local file**: Append the downloaded file to the destination file. This option is only available for transfers from the host.

- **Overwrite local/server file**: Overwrite the destination file.

- **Skip this file**: Do not transfer this file. If additional files are specified for this transfer operation, continue with the next file.

- **Copy to a different name**: Type in the new filename to use in the destination folder, and click OK.

- **Copy using a unique name**: Automatically create a unique name for the destination file. The names of any files that are renamed during the transfer operation are shown in the FTP command window.

- **Update local/server file if older**: Overwrite the destination file only if the file being transferred is newer than the destination file.

Related Topics

- “Handle Existing Files (Transfer Mode)” on page 783

Managing Files and Folders

In this Section

- “Working with Files” on page 793
- “Working with Local Folders” on page 793
- “Create a Shortcut to a Local File or Folder” on page 794
- “Working with Server Directories” on page 794
- “Set Default Home Directories” on page 795
- “Working with Filename Characters” on page 796
- “Filter the Server File Listing” on page 797
- “Run the Directory Definition Wizard” on page 798
- “Set File and Directory Permissions” on page 798
- “Server View Filter Dialog Box” on page 800
- “Server File Properties Dialog Box” on page 800
- “Go To Folder Dialog Box” on page 801
Working with Files

Commands on the File and Edit menus, and most buttons on the toolbar, apply to folders and files in the currently active pane. These commands let you rename, delete, and do other directory management tasks within the FTP Client.

Also, you can right-click a file to access commands in the context menu. For example, to get information about a file, right-click it and choose Properties.

Double-click a file to open or run it.

NOTE: In order to display the contents of a server file or run a program located on the server, the file is copied from the server to your Windows user folder.

Related Topics
- “Working with Local Folders” on page 793
- “Working with Server Directories” on page 794
- “Working with Filename Characters” on page 796
- “Filter the Server File Listing” on page 797

Working with Local Folders

Index Term
Primary: folders (FTP Client)
Secondary: going directly to a local folder

Index Term
Primary: folders (FTP Client)
Secondary: changing local folder

To work with items on the local PC, use the left pane of the FTP Client. You can browse disk drives on your computer or local network, create new folders, and do other directory management tasks within the FTP Client. Commands on the File and Edit menus, and most buttons on the toolbar, apply to folders and files in the currently active pane.

New folders can be added from the File menu, context menu (right-click), or toolbar. Use the context menu to create shortcuts to folders.

To view the local directory structure, use the Go to a different folder list box in the upper left corner of the main window. To see how the current folder fits in the hierarchy on your computer, click the down arrow in the list box. The Tools menu and toolbar provide access to the Up One Level command. Also, you can navigate directly to a folder using the Go to command.

To navigate directly to a local folder

1 From the Tools menu, choose Go to.
2 Type the name of the directory you want to open.
   For example: J:\Payroll\July.
3 Select Local Computer to indicate that the folder is available on your PC.

NOTE: You can enter UNC (Universal Naming Convention) names for directory paths. There is a 47-character limit for UNC names, and each name can contain any character, both uppercase or lowercase, except the following: ? " / | < > * :

File and Data Transfer 793
The syntax of a UNC name is as follows:
```
\\<computername>\\<sharename>\\<pathname>
```

Related Topics
- “View the Local PC Files” on page 742
- “Set Default Home Directories” on page 795
- “Create a Shortcut to a Local File or Folder” on page 794

Create a Shortcut to a Local File or Folder

Index Term
- Primary: shortcuts (FTP Client)
- Secondary: to local files and folders

Index Term
- Primary: folders (FTP Client)
- Secondary: creating shortcut to

Index Term
- Primary: file management (FTP Client)
- Secondary: creating shortcuts to files

To create a shortcut to a local file using the FTP Client

1. In the left pane, select the files and folders you want to create shortcuts to.
2. Click the right mouse button to open the context menu.
3. From the context menu, click Create Shortcut to create a shortcut to each of the selected files and folders.

   The shortcuts are created in the current folder on the PC.

Related Topics
- “Working with Local Folders” on page 793
- “Working with Files” on page 793
- “View the Local PC Files” on page 742

Working with Server Directories

Index Term
- Primary: server settings (FTP Client)
- Secondary: opening a server directory

Index Term
- Primary: directory management (FTP servers)
- Secondary: going directly to a directory

To work with items on the server, use the right pane of the FTP Client. You can browse remote directories, create new folders, and filter the file listing. Commands on the File and Edit menus, and most buttons on the toolbar, apply to folders and files in the currently active pane.

New folders can be added from the File menu, context menu (right-click), or toolbar.
To view the remote directory structure, use the **Go to a different folder** list box in the upper left corner of the main window. To see how the current directory fits in the hierarchy on your server site, click the down arrow in the list box. The **Tools** menu and toolbar provide access to the **Up One Level** command. Also, you can navigate directly to a remote directory using the **Go to** command.

**To navigate directly to a remote directory**

1. From the **Tools** menu, choose **Go to**.
2. Type the name of the directory you want to open.
   - Follow the server’s syntax for directory names.
3. Select **site name** to indicate that the directory is located on the server.

**Related Topics**

- “View the Server Files” on page 743
- “Set Default Home Directories” on page 795
- “Filter the Server File Listing” on page 797
- “Run the Directory Definition Wizard” on page 798

### Set Default Home Directories

**Index Term**

**Primary:** home directory (FTP Client)

**Index Term**

**Primary:** FTP options
- Secondary: setting default home directories

**Index Term**

**Primary:** directory management (FTP servers)
- Secondary: setting default home directories

Use default home directories to determine which files you see by default in the FTP Client. The default server directory determines which files you see in the server pane when you first connect to a site. There are two kinds of default local home folders. One is the global setting for the FTP Client, and the other kind is specific to each site that you connect to. Once you've configured a site-specific local home folder, the FTP Client will show that folder in the local pane, and the default server home directory in the server pane.

**To set the default server directory**

1. Use the right pane to browse for the server directory you want to set as the default.
2. From the **Connection** menu, choose **Site Properties** and then click the **Directories** tab.
3. Under **Server**, click **Use Current**.
   - This enters the current server location in the **Home directory** text box.
4. Click **OK**.

**NOTE:** To change the default server home directory, you can also right-click the folder you want to use, and then choose **Set Home Directory**.

**To set the default local folder for a specific site**

1. From the **Connect to FTP Site** dialog box, select a site, and then click the **Properties** button.
-Or-

If you are already connected to a site, from the **Connection** menu, choose **Site Properties**.

2 Click the **Directories** tab.

3 Under **Local**, click **Browse** and select the PC directory you want to set as the default.

4 Click **OK**.

**To set the default local folder for the FTP Client**

1 From the **Tools** menu, choose **Options**.

2 Click the **Directories** tab.

3 Under **Default local home folder**, click **Browse** and select the PC directory you want to set as the default.

4 Click **OK**.

**Related Topics**

- “Directories Tab (Site Properties Dialog Box)” on page 773
- “General Tab (Options Dialog Box)” on page 765
- “Working with Local Folders” on page 793
- “Working with Server Directories” on page 794

**Working with Filename Characters**

The **FTP Client** supports long filenames. Long filenames in Windows can contain spaces. The only characters that are not allowed are:

\ / : * ? " < > |

The following length limitations apply:

- Maximum path (excluding the filename): 246 characters (including drive letter, : character and \ character). This limit of 246 allows for the addition of a filename in the standard 8.3 format with the terminating null character.
- Maximum filename: 256 characters (including terminating null character)
- Maximum fully qualified name (path + filename): Varies slightly with different Windows operating systems. Use 259 characters to ensure a valid path for all Windows systems.

**Working with filenames that contain spaces**

When you use FTP or SFTP commands, any filename that contains spaces must be enclosed in double quotation marks. For rules on how quotation marks are used, see the “Quotation Marks in FTP or SFTP Commands” on page 818 topic.

**Working with server filenames that contain prohibited characters or are too long**

For file transfers to the PC, the **FTP Client** automatically ensures that the name given to the file on your PC is valid in Windows by using the following rules:

- Strip all illegal characters. Example: fast*lane becomes fastlane.
- Invalid characters are: \ / : * ? " < > |
- If necessary, truncate the filename. In Windows, the length limitations described above are applied.
The Windows path is always preserved. If the server filename plus the destination Windows path is greater than the maximum allowed, the server filename is truncated.

- If the filename begins with a period, the appropriate number of characters are removed from the end of the filename. If the filename contains periods, the client determines the location of the last period in the name and truncates the appropriate number of characters to the left of the period.

If you want transfers from a server site to automatically derive a valid DOS name when the server filename is too long or when it contains invalid characters, select the **Create Windows file names in 8.3 format** option on the **Transfer** tab in the **Site Properties** dialog box.

**Related Topics**
- “Quotation Marks in FTP or SFTP Commands” on page 818
- “Working with Files” on page 793
- “Transfer Tab (Site Properties Dialog Box)” on page 777

**Filter the Server File Listing**

Using a file filter allows you to view a subset of the files on the server. You can specify a default file filter or a temporary file filter. If the server directories contain a lot of files, specifying a default filter provides a way to speed up retrieval and display of directory listings.

**NOTE:** This feature is not available for SFTP connections.

**To specify a default file filter for a server**

1. From the **Connection** menu, choose **Site Properties** and then click the **Directories** tab.
2. In the **File View Filter** box, type a default view filter for all server directory listings for that site.
   - For example, type `*.txt` to list all files in the current directory that end in `.txt`. The specification must use wildcard characters that are recognized by the type of server running at the site.
3. Click **OK**.
   - The FTP Client automatically refreshes the server directory listing.

**To apply a temporary file filter**

1. From the **View** menu, choose **Filter**.
2. In the **Server View Filter** dialog box, type a view filter specification.
   - For example, type `*.txt` to list all files in the current directory that end in `.txt`. The specification must use wildcard characters that are recognized by the type of server running at the site.
3. Click **OK**.
   - The FTP Client automatically refreshes the server directory listing.

**NOTE**

- If you are connected to two servers in the same session, the **View** menu **Filter** command applies to both servers. To apply a filter to only one server, right-click in the display pane for that server, and select **Filter** from the context menu.
- When a view filter is in effect, the filter is shown in the title bar of the server pane.
- To request a listing of all files in the folder, type `*` (asterisk) for your view filter specification.
Run the Directory Definition Wizard

The Directory Definition Wizard helps you to define the directory format for an unrecognized type of FTP server. The Wizard allows you to identify the filename and other fields in the directory output from the current FTP site so that server directory listings can be displayed and interpreted properly in the right pane of the FTP Client window.

NOTE: This wizard should not be used if the files on the FTP site already display properly.

To use the Directory Definition Wizard

NOTE: To use the Directory Definition Wizard, you must have Server type set to Auto detect (the default value) on the General tab of the Site Properties dialog box.

1. Connect to a site.
2. From the Tools menu, choose Directory Definition Wizard.
3. Complete the steps as directed by the wizard.

NOTE: File name is the only required field. You can leave the other fields undefined.

4. When you are done specifying the location of fields, click Finish.

The FTP Client automatically refreshes the server directory listing.

5. If the directory listing is still unusable, re-run the Directory Definition Wizard and continue experimenting with the location of directory fields until you get better results.

Set File and Directory Permissions

Related Topics

- “FTP Client Troubleshooting” on page 805
Index Term
Primary: directory management (FTP servers)
Secondary: permissions

You can change file permissions on the server using the server pane or the FTP command line. You can also configure global defaults for new files and directories. For individual sites, you can configure the client to query you for permission values each time you transfer a file or create a new directory.

To change file and directory permissions using the server pane
1. Connect to a UNIX or Linux host.
2. In the server pane, select one or more files or directories.
3. Right-click your selection and choose Properties.
4. Change the attributes of the selected item(s) using either of the following techniques:
   - In the Permission Mode box, type a three digit number that is a valid value for the UNIX chmod command. Valid values have digits from 0 to 7.
   - Under Owner, Group, and Public, select options to allow each user type permission to read, write, or execute.
5. Click OK.

To configure global defaults for transferred files or newly created directories
1. Go to Tools > Options
2. To set default permissions for uploaded and downloaded files, use the File Attributes tab.
3. To set default permissions for newly created directories, use the Directory Attributes tab.
4. Click OK.

To set permissions each time you transfer a file or create a directory
1. Open the site properties dialog box.
   1a. Start the FTP Client.
      This opens the Connect to FTP Site dialog box. (If the FTP Client is already running and this dialog box is not open, go to Connection > Connect.)
   1b. From the Connect to FTP Site dialog box, select a site.
   1c. Click the Properties button.

   NOTE
   - If you are already connected to a site, from the Connection menu, choose Site Properties.
   - Some changes you make using the Site > > Properties dialog box when connected will not take effect until the next time you connect to the site.

2. To set permissions each time you transfer a file, click the Transfer tab and select either or both of the following options: Show download options before transfer and Show upload options before transfer.
3. To set permissions each time you create a directory on the server, click the Directories tab and select Show attributes before creating directory.
4. Click OK.

To change file and directory permissions using the FTP command line:
1. Connect to a UNIX or Linux host.
2 Press F7 to display the command line if it is not already visible.
3 Enter a UNIX chmod command using a numeric permission mask.
   For example, the following commands sets attributes to -rw-r--r-- for the specified file.
   chmod 644 myfile.htm

   **NOTE:** Permissions changes you make to directories are not recursive; that is they do not affect the files within the directory.

**Related Topics**

- “Use the FTP Command Line” on page 817
- “Server File Properties Dialog Box” on page 800
- “Set Time and Date of Downloaded Files” on page 784
- “Change the Filename when Downloading” on page 785
- “Change the Filename when Uploading” on page 786

**Server View Filter Dialog Box**

**Getting there**

- From the **FTP Client** **View** menu, choose **Filter**.

Use the **Server View Filter** dialog box to request a remote site directory listing that shows server files of a specific type.

Type a wildcard specification. For example, type *.txt to list all files in the current directory that end in .txt. The specification must use wildcard characters that are recognized by the type of server running at the site. When you click **OK**, the server directory listing refreshes in the right pane, showing only the files that match your specification.

   **NOTE**

- This feature is not available for SFTP connections.
- When a view filter is in effect, the filter is shown in the title bar of the server pane.
- To request a listing of all files in the folder, type * (asterisk) for your view filter specification.

**Server File Properties Dialog Box**

**Getting there**

1 Start the **FTP Client**.
   This opens the **Connect to FTP Site** dialog box. (If the **FTP Client** is already running and this dialog box is not open, go to **Connection** > **Connect**.)
2 Connect to a site and then select a file or folder in the server pane.
3 From the **File** menu, choose **Properties**.

This dialog box displays information about the currently selected server file or directory. You can also use it to set permissions on a UNIX or Linux server.
Permissions changes you make to directories are not recursive; that is they do not affect the files within the directory.

**Attributes**
Displays the current attributes.

**Permission Mode**
Type a three digit number that is a valid value for the UNIX `chmod` command. Valid values have digits from 0 to 7.

**Owner, Group, and Public**
Select options to allow each user type permission to read, write, or execute the currently selected item.

**Related Topics**
- “Set File and Directory Permissions” on page 798
- “Working with Server Directories” on page 794

**Go To Folder Dialog Box**

**Getting there**
- From the **FTP Client** Tools menu, choose **Go to**.
  - Type the name and path of the folder you want to open.
- Click **Local Computer** to specify a path on the local computer.
- If you are connected to a server, the server name is shown. Click this option to specify a path on the server.

**Related Topics**
- “Working with Local Folders” on page 793
- “Working with Server Directories” on page 794

**Customizing FTP Client Startup**

You can customize how the **FTP Client** starts using shortcuts, startup switches, and script files. You can use Windows shortcuts to provide quick and easy access to the Reflection FTP Client and to your servers. You can create a shortcut to:
- Open a settings file and display a list available sites
- Connect to a specific host site

**In this Section**
- “Create a Shortcut to Load a Settings File” on page 802
- “Create a Shortcut to Connect to a Site” on page 802
- “FTP Client Startup Switches” on page 802
- “Startup Command Examples” on page 804
- “Run a Script File at Startup” on page 804
- “Example of Starting the Client with a Script File” on page 805
Create a Shortcut to Load a Settings File

Index Term
Primary: shortcuts (FTP Client)
Secondary: to open a settings file

You can create a shortcut that loads an FTP Client settings file and automatically opens the Connect to FTP Site dialog box showing a list of available sites.

To create a shortcut that launches the FTP Client and loads a settings file

1. From the File menu, select Save As and save the .mst file to the same folder as the installer package file for Reflection (setup.exe).
2. (Optional) Type a new name for the file you are saving.
3. Select the Save shortcut on desktop option in the lower left corner of the Save Settings dialog box.
4. Click Save.

Related Topics
- “FTP Client Settings Files” on page 744
- “Connect to FTP Site Dialog Box” on page 742

Create a Shortcut to Connect to a Site

Index Term
Primary: shortcuts (FTP Client)
Secondary: to connect to a site

You can create a shortcut that launches the FTP Client and automatically connects to a server.

To create a shortcut that launches the FTP Client and connects to a site

1. The Connect to FTP Site dialog box opens when you start the FTP Client. You can also open it by choosing Connect from the Connection menu.
2. Right-click on any site in the list and select Create Shortcut.
   You will see a message telling you that a shortcut has been created on the desktop.
3. Click OK.

Related Topics
- “Connect to FTP Site Dialog Box” on page 742

FTP Client Startup Switches

Index Term
Primary: Starting the FTP Client
Secondary: executing a command at startup

Index Term
Primary: command line
Secondary: Startup Switches (FTP Client)
You can start the FTP Client and provide command line parameters that automatically connect to a predefined site, run a specified script file, connect using a settings file, or connect to a server specified with a URL.

- You can set up a shortcut with a startup command that automatically executes the startup command when you double-click it. The properties you specify for the shortcut determine whether the Client runs in a window or runs minimized on the desktop when you start it.
- You can enter a startup command in the Open box when you use the **Run** command on the Start menu.

### Startup Command Syntax

```
<executable>.exe [<site>] /<switch> <parameter>
```

- `<executable>.exe` Provides the path and name of the FTP executable file, for example:
  
  "C:\Program Files\Attachmate\Reflection\Rftpc.exe"

- `<site>` Specifies a site defined in a settings file. The site properties are in effect when the client starts. If the site name contains spaces, enclose it in quotation marks, for example "ADA Home".

  When included, the `<site>` argument is always the first argument on the command line. When used in conjunction with the `/W` switch, the `<site>` argument is ignored.

  If the defined site is not in the default settings file (Settings), use the `/RFW` switch to specify the settings file that includes the site definition.

- `/<switch> <parameter>` Use one or more of the switches listed below to specify the operations you want to perform when the client starts up:

#### Startup Switches

- **/D <diagnostic file>** Directs the client to record in the specified file all communications between the client and the server, as well as other diagnostic information that may be useful for troubleshooting. The specified diagnostic file is placed in your My Documents folder. This file is refreshed each time you start the client.

- **/E** Directs the client to log events to the Application event log. Note: The diagnostic file created with /D includes more detailed information than this event log.

- **/FMIGRATE** Launches the Reflection F-Secure Migration Wizard, which you can use to migrate F-Secure profiles to Reflection settings files.

- **/L <log file>** Directs the client to record in the specified log file all communication between the client and the server to which it connects. This is a cumulative log file; new information is added after existing information.

- **/N** Suppresses the display of the Reflection startup screen.

- **/RFS <script file>** Runs the specified script. If the script ends in a QUIT command, the client shuts down when the script completes.

- **/RFW <settings file>** Allows you to connect using the specified settings file.

- **/X <export file>** Launches the Export Settings dialog box directly without launching the main client window.
Startup Command Examples

The following example command runs the FTP Client (rftpc.exe) and connects to a site named West Coast, which is defined in the default settings file.

"InfoConnect\rftpc.exe" "West Coast"

In the example above, quotation marks must surround the executable file specification because the path specifies a folder name that contains a space. Similarly, the site name is surrounded by quotation marks because it contains a space in the name.

The next example command uses the /W switch to specify the URL for an FTP site and the /L switch to direct the FTP Client (rftpc.exe) to log all client/server communication to a log file named Ftpinfo.log.

"InfoConnect\rftpc.exe" /W ftp://ftp.myco.com /L Ftpinfo.log

The following example command tells the FTP Client to connect using a settings file and run a script file. The /RFW switch directs the FTP Client to connect using the settings file Myfile.rfw. The /RFS switch directs the FTP Client to run the script file Transfer.rfs after connecting to the server specified in the settings file.

"InfoConnect\rftpc.exe" /RFW "C:\Users\username\Documents\Attachmate\Reflection\Myfile.rfw" /RFS "C:\Users\username\Documents\Attachmate\Reflection\Transfer.rfs"

Run a Script File at Startup

You can start the client and provide command line parameters that automatically execute all the commands in a script file. This allows you to automate sequences of commands.

- You can set up a shortcut with a startup command that automatically executes a script when you double-click it. The properties you specify for the shortcut determine whether the client runs in a window or runs minimized on the desktop when you start it.
- You can enter a startup command in the Open box when you use the Run command from the Start menu.
Startup Command Syntax to Execute a Script File

\texttt{<executable>.exe [\textit{<site>}] /RFS \textit{<script file>}}

Use a space to separate each argument in the command line.

\texttt{<executable>.exe}

Provides the path and name of the FTP Client executable file.

For example:

\texttt{InfoConnectRftpc.exe \textit{<site>}}

Specifies a previously defined site. The site properties are in effect when the client starts. If the FTP site name contains spaces, enclose it in quotation marks, for example "ADA Home".

When included, the \textit{<site>} argument is always the first argument on the command line. When used in conjunction with the \texttt{/W} switch, the \textit{<site>} argument is ignored.

\texttt{/RFS \textit{<script file>}}

Provides the path and name of the FTP script file. If the script file name or path contains spaces, enclose it in quotation marks, for example "C:\My Script Files\Get lab reports.rfs".

Related Topics

- “FTP Client Startup Switches” on page 802
- “Example of Starting the Client with a Script File” on page 805

Example of Starting the Client with a Script File

The following command runs the FTP Client, connects to the FTP site "Central" and executes an FTP script file named \textit{Upload.rfs}.

\texttt{Rftpc.exe Central /RFS Upload.rfs}

In this example, the FTP Client starts and automatically connects to the FTP site "Central". The site properties defined for the "Central" FTP site are in effect when the script runs.

\textbf{NOTE:} Any site or script filename containing spaces must be enclosed in quotation marks. For example:

\texttt{Rftpc.exe "My Site" /RFS "Central files download.rfs"}

Related Topics

- “Run a Script File at Startup” on page 804
- “FTP Scripting” on page 819

FTP Client Troubleshooting

Index Term

Primary: troubleshooting (FTP Client)
Secondary: overview of solutions

In this Section

- “Identifying the Source of the Problem” on page 806
Identifying the Source of the Problem

When you encounter a problem with the Reflection FTP Client, it may help to compare the behavior to that of another client. You can use the Microsoft FTP client to open a connection to the FTP server where the problem occurs; then try using this client to duplicate the operation that causes the problem.

If you can duplicate the problem when you use a different FTP client, one of these conditions may apply:
- The server you are connecting to does not support the FTP operation you are attempting.
- The server you are connecting to is configured incorrectly.
- You are specifying incorrect information in your command (for example, you are specifying a non-existent path or filename when attempting a file transfer).

If the problem only occurs when using the Reflection FTP Client (you can’t duplicate the problem when you connect to the server using a different FTP client), check the troubleshooting solutions.

Related Topics
- “Troubleshooting FTP Client Connections” on page 806
- “Troubleshooting FTP File Transfer Problems” on page 808
- “Troubleshooting FTP Directory Listing” on page 809
- “Troubleshooting FTP Site-to-Site Transfer” on page 810
- “FTP Client Error messages” on page 811
- “Windows Sockets Error Messages” on page 813
- “Error Messages” on page 814

Troubleshooting FTP Client Connections

Index Term
Primary: troubleshooting (FTP Client)
Secondary: server connection problems
Use this topic to troubleshoot problems making connections using the FTP Client.

**Configuring Connections**

- Did you enter your server name, user name, and password correctly? If you are connecting to a case-sensitive server, be sure to use the correct case when making these entries.
- Does your site use a passthrough server or SOCKS proxy server to ensure that only authorized users have access to server sites? If so, you should configure the client to connect via the firewall or SOCKS proxy server.
- When opening a connection, the server name you provide is resolved via the HOSTS file or a domain name server. If you have no domain name server on the local network and don't use a HOSTS file, you must specify the full IP address of the host server. For example: 124.24.36.85
- If the FTP server is not running on the remote system, you can't connect.
- Server response time can be affected by the distance between sites. If you see the message "Connection timed out" when trying to connect to a server, increase the value of **Timeouts in seconds** on the **Connection** tab of the **Site Properties** dialog box.
- If the FTP Client is unable to determine the server type, server directory listings may display incorrectly. You can use the **Directory Definition Wizard** to modify the directory format.
- If you are having trouble making a Secure Shell connection, use the Secure Shell log to get troubleshooting information.

**Connection Troubleshooting**

**Error message: "Could not resolve host address."**

Several things can cause this message to appear:

- The host name or IP address you entered for the server is invalid. Re-enter the host name; if you are connecting to a case-sensitive server, be sure to use the correct case.
- The host name you provide is resolved via the HOSTS file or a domain name server. Is the computer that acts as the domain name server working? Has the HOSTS file on your PC been corrupted? If no domain name server or HOSTS file is available, you must specify the full IP address of the host server. For example: 124.24.36.85.
- You have entered an IPv6 address, but have not enabled IPv6 support on your PC. Contact Microsoft for more information.
- You must have an appropriately configured IP router (gateway) in order to connect to servers outside your own network. Check to see whether the computer serving as the router is up and running.

**Error message: "Connection timed out."**

Server response time can be affected by the distance between sites. If you see this message when trying to connect to a server, increase the **Connect Timeout** setting to give the server more time to respond during the login process.

**Reflection FTP hangs when you try to connect**

On some systems, turning off the use of animation (such as showing a waving flashlight while you are waiting for a directory listing) fixes display problems that cause Reflection to hang when you attempt a connection. To disable the use of animation, open the **Tools** menu, click **Options**, open the **Preferences** tab and enable **Do not use animation**.
Host cannot respond to the PWD command

By default, Reflection sends a PWD command when you connect to your server. Some servers don't support this command. Press F7 to open the command window before you try connecting to your server. If the server returns an error after Reflection sends the PWD command, try enabling this setting. To configure Reflection to connect without the PWD command, open the Directories tab of the Site Properties dialog box and select Don't send PWD Command.

Error Message: PASV is not implemented by the server

By default, the client connects using the PASV command. This causes the client to initiate a separate data connection for directory listings and file transfers, which is required for connections through some firewalls. If your server does not support the PASV command, you can disable the Use passive mode setting on the Connection tab of the Site Properties dialog box.

Related Topics

- “Secure FTP Client Connections” on page 747
- “Connection Tab (Site Properties Dialog Box)” on page 771
- “Run the Directory Definition Wizard” on page 798
- “Secure Shell Log File” on page 810

Troubleshooting FTP File Transfer Problems

Index Term
Primary: troubleshooting (FTP Client)
Secondary: file transfer

Index Term
Primary: transferring files (FTP Client)
Secondary: troubleshooting

Index Term
Primary: file transfers (FTP Client)
Secondary: troubleshooting

If you're having trouble transferring files using the FTP or SFTP client, consult the following list:

- You must be connected to a server before you can transfer files.
- If a transferred file is not usable (for example, you can't unzip a zipped file, you can't run an executable file, or you can't read an ASCII file), be sure that you are selecting the correct file transfer method prior to transferring the file.
- Transfers to a server may be unsuccessful if you don't have write permission to the destination directory on the server.
- If an "Access denied" message displays when you attempt to transfer a server file to your PC, you have a read-only file in the PC destination directory that has the same name as the file you are trying to receive, or you do not have write permission to the PC directory.
- If you see an error message when you attempt to transfer files between two remote hosts, the sending or receiving server may not be configured to support this feature.
- If a transferred ASCII file contains incorrect characters, you may need to use character translation to preserve the characters present in the source file when they are transferred to the destination file. When necessary, the FTP Client can translate between the server character set and either the Windows or DOS character set. Character translation ensures that characters present in the source character set are translated to characters available in the destination
character set. For example, if you transfer files from a server that uses the DOS character set for use in a Windows application, or if you want to transfer an ASCII file that contains accented characters and symbols for a specific national language, you need to set character translation options to perform necessary translation during file transfer. See the “Character Sets Dialog Box” on page 788 topic for more information.

- If you are having trouble transferring files when the file names contain spaces, quotation marks, or wildcard characters, see the “Quotation Marks in FTP or SFTP Commands” on page 818 topic for more information.
- If you are having trouble canceling a file transfer you may need to reconnect to the server. Some servers close your connection if you cancel a transfer while you are receiving (getting) a server file.
- If File Exists settings apply only to transfers within the Reflection FTP Client. If you use drag-and-drop to transfer a file from a FTP Client display pane to your desktop or an open Windows Explorer window, Windows will always display a Confirm File Replace dialog box whenever a file with the same name exists in the selected location, regardless of the configuration of the Reflection FTP Client. To take advantage of the currently configured FTP Client option, always use the FTP Client panes for drag-and-drop transfers.

Troubleshooting FTP Directory Listing

Consult the following list if you are having trouble obtaining directory listings at an FTP or SFTP site:

Trouble obtaining a directory listing or Server returns error "425 Can't open data connection"

If you don't see a directory listing in either the server pane or the command window, your server may not support the PASV command. Try clearing the Use passive mode setting in the Connection tab of the Site Properties dialog box.

Trouble seeing all files in a server directory

You may have specified a default wildcard filter for the site's server directory listings. The wildcard filter limits directory listings to files of a specific type. For example, if the filter specifies *.txt, directory listings will show only files that match the wildcard (that is, files ending in .txt).

- The default wildcard filter for server directory listings is set on the Directories tab in the Site Properties dialog box.
- When a wildcard filter is in effect, the filter will be shown in the title bar of the FTP Site pane (the right pane).
- To temporarily override the default wildcard filter for server directory listings, use View > Filter. To see all files and folders in the directory, type * (an asterisk).

Incorrect or empty server file display when connecting to a UNIX server using SFTP

Try changing the Use structured listing data setting (Site Properties > Security > Secure Shell) if you are connecting using SFTP and the server pane display is missing or is not correctly displayed. This setting specifies which data list style sent by the server is used to create the directory display in the right pane of the FTP Client. When this setting is not selected (the default), the FTP Client uses the standard UNIX-style data list. When it is selected, the FTP Client uses the structured data list.
You see an error message saying "The system cannot find the path specified" when you connect to the server

This error may indicate that the FTP Client is trying to find a local file path that does not exist. Check the local Home folder setting to be sure that the folder path exists on your computer. To view or edit this setting, open the Site Properties dialog box, click Directories, then find Home folder under Local.

Related Topics

- “Run the Directory Definition Wizard” on page 798

Secure Shell Log File

Reflection maintains a log file with information about your last Secure Shell connection. Use either of the following techniques to view this log for the FTP Client:

- Start logging (Tools > Start Logging) to send log information to a file.
- Open the FTP command window (View > Command Window) to view the log on screen.

**NOTE:** You can use the Logging Level setting to determine how much information is written to the Secure Shell log. This setting is available on the Reflection Secure Shell Settings (page 353)A2D removed a broken link to: reflection_secure_shell_settings_topic_gta in an excluded topic. dialog box -- General tab.

Troubleshooting FTP Site-to-Site Transfer

Index Term
Primary: troubleshooting (FTP Client)
Secondary: site-to-site transfer

Index Term
Primary: site-to-site transfer (FTP Client)
Secondary: troubleshooting

If you see any of the following error messages when you attempt to transfer files between two remote hosts, the sending or receiving server may not be configured to support this feature:

- 500 Illegal PORT command
- 501 IP address for data destination does not match client's
- 425 Can't open data connection
- 502 PASV command not implemented by this server

When the FTP Client encounters this problem, it attempts to transfer to the local PC, and then to the target site, after the error is received. Note that even though the transfer may complete successfully, you will see the error message before the transfer is completed.

If you regularly transfer between servers that don't support direct site-to-site transfer, you can configure the FTP Client to force all site-to-site transfers to copy files first to the local machine then to the destination server. This configuration allows you to transfer between sites without seeing one of the error messages listed above.
To force all site-to-site transfers to copy files first to the local computer

1. From the Tools menu, choose Options.
2. On the Preferences tab, select Force site to site transfers through local machine, and then click OK.

Review the following for more information about configuring servers to support direct site-to-site transfer.

Sending server configuration

Site-to-site transfer feature requires that any FTP server sending a binary file must accept a PORT command from the Reflection FTP Client to an IP address that is different from the client's IP address. (On some servers this support may be disabled for security reasons.) The PORT command specifies the TCP PORT to which the data should be sent. If the sending server does not accept this use of the PORT command, you will see two server error messages: usually a "500 Illegal PORT command" or a "501 IP address for data destination does not match client's" from the sending server, followed by a "425 Can't open data connection" from the receiving server. You will also see a file of zero bytes created on the receiving server because the file index is created prior to receiving any data. To enable site-to-site transfer, contact the administrator of the sending server to determine whether PORT commands to a different IP address can be enabled on the server.

Receiving server configuration

Site-to-site transfer requires that any FTP server receiving a binary file must accept a PASV command from the Reflection FTP Client and return the PORT information to be passed on to the sending server. If the receiving server does not accept the PASV command, the site-to-site transfer will fail with an error message: "502 PASV command not implemented by this server". To enable site-to-site transfer, contact the administrator of receiving server to determine whether PASV can be enabled on the server.

Related Topics

- "Transfer Files between Two Remote Sites" on page 785

FTP Client Error messages

Index Term
Primary: error messages (FTP Client)

Following is a list of the FTP Client error messages that may appear and an explanation of how to resolve the error condition.

A connection has not been established.

Command line error. You issued a command to a server (for example PWD, CD, DIR, LS, or QUOTE <command>) but you aren't currently logged in to the server. Open a server connection.

Access denied.

You cannot access the protected file or folder. Check that you have correct permissions for the operation you attempted.

Already connected to a site.

Command line error. You issued an OPEN or PASSTHRU command, but you are already logged in to a server. Use the CLOSE command to close the current connection prior to opening a new one.
Connection timed out.

When connecting to a server, the FTP Client waits up to \( n \) seconds for a response from the server. If nothing is received within the period specified, this message is displayed; in this case, try to connect again. If the message appears again, increase the connection timeout value to give the server more time to respond during the login process. To do this, open the Connection tab and edit the Connect text box under Timeout in seconds; or enter `SET TIMEOUT-CONNECT` at the command line.

Could not resolve host address.

Several things can cause this message to appear:

- The host name or IP address you entered for the server is invalid. Re-enter the host name; if you are connecting to a case-sensitive server, be sure to use the correct case.
- The host name you provide is resolved via the HOSTS file or a domain name server. Is the computer that acts as the domain name server working? Has the HOSTS file on your PC been corrupted? If no domain name server or HOSTS file is available, you must specify the full IP address of the server. For example: 124.24.36.85.
- You must have an appropriately configured IP router (gateway) in order to connect to FTP or SFTP servers outside your own network. Check to see whether the computer serving as the router is up and running.

Command \textit{<command>} needs more arguments.

Command line error. The command you entered requires one or more arguments. Type `help \textit{<command>}` at the FTP command line for a quick summary of the syntax for the command or consult the online help.

File already exists.

File transfer to the client was unsuccessful because the \textit{If File Exists} file transfer mode is set to Cancel and a file with the same name as the server file already exists on the local computer.

Out of memory.

There is not enough memory on the local computer. Close other open Windows applications and try again.

Session timed out.

After you are connected to a server, the client waits up to \( n \) seconds for data packets being transferred to or from the host. If nothing is received within the period specified, this timeout error appears; in this case, try the operation again. If you have received repeated timeout errors, increase the session timeout value. To do this open the Connection tab, and edit the Session text box under Timeout in seconds, or use `SET TIMEOUT-SESSION` at the command line. (Connection timeouts are governed by a separate Connect text box).

Server response time can be affected by the distance between sites. Specifying a higher value gives the server more time to respond.

Unknown command \textit{<command>}. Type ‘help’ for a list of valid commands.

Command line error. The command you entered is not recognized. Type `help` at the FTP command line for a list of the available FTP commands, type `help \textit{<command>}` for a summary of the syntax for a specific command, or see the Command Reference topic.

502 PASV command not implemented by this server

If you receive an error message saying that PASV is not implemented by the server, you should disable the Use passive mode setting, which is enabled by default. This setting supports connections through some firewalls.
Windows Sockets Error Messages

Following is a list of the Windows Sockets error messages that may appear during a Reflection FTP Client session and an explanation of how to resolve the error condition. These error messages (which are all preceded by the identifying string “WINSOCK error:”) are returned by the Windows Sockets library if an error occurs in the network interface layer between Windows and the TCP/IP stack you are using. The Windows Sockets library (supplied in a module called Wsock32.dll) is included as part of the Windows operating system.

For some network Windows Sockets implementations, when you are connected to a server, several things can cause this message to be displayed:

- You tried to start a file transfer or perform a directory operation (such as changing directories or refreshing the current directory). If you see this error when attempting to transfer a file or to obtain a directory listing, then your network implementation does not work with the FTP Client.
- You started another instance of the FTP Client and tried to open another connection to the same server. If you get this error message when trying to connect, it indicates that your network implementation supports only one connection at a time to a given server. You cannot start separate instances of the FTP Client and attempt to connect to the same server with each instance.

**Connection refused**

The connection attempt was unsuccessful due to a problem on the host; possibly the host is down or the server is not running at this time. Wait a while, and then try to connect again.

**Connection reset by peer**

During a file transfer, the remote host reset the server connection. Close the server connection, reconnect, and try the transfer again.

**Connection timed out**

The attempt to connect to a server was timed out by your network software without establishing a connection. This may be because the server is not running. Wait a while, and then try to connect again.

**Network is down**

The Windows Sockets implementation has detected that the network subsystem has failed. Your network should be restarted.

**Network is unreachable**

The network can't be reached from this host at this time. This error can occur when you use an IP router (gateway) to connect to servers outside your own network. The message indicates that one of the IP routers along the path from your gateway to the destination networks is down. Contact your system administrator, who can check the hops between your gateway and the destination network.
No buffer space available
There are too many open connections. This error condition can occur when opening a
connection to a server or transferring a file, or when the client requests server directory
information. Close other open server connections or applications that use Windows Sockets and
try the operation again. Check your network documentation for information about how to
increase the buffer space for which your network is configured.

Operation not supported on socket
The client must open a data session prior to performing a file transfer or directory listing
operation. A data session can't be opened using your network's Windows Sockets
implementation.

Software caused connection abort
While transferring files to or from the server, the virtual circuit used for the server connection was
aborted due to a timeout or other failure (possibly the host went down, or the FTP or SFTP
server is not running). Close the server connection, reconnect, and try the transfer again.

Too many open files
To solve this problem, exit Windows, increase the Files= setting in your Config.sys file and
reboot your PC. If you still get this message, try closing other open client sessions and then try to
open the connection again. If your problem is still unresolved, contact the manufacturer of your
Wsock32.dll for help.

Related Topics
- “FTP Client Error messages” on page 811

Error Messages
Click on an error message to view details.

Could not resolve host address.
Several things can cause this message to appear:

- The host name or IP address you entered for the server is invalid. Re-enter the host name; if you
  are connecting to a case-sensitive server, be sure to use the correct case.
- The host name you provide is resolved via the HOSTS file or a domain name server. Is the
  computer that acts as the domain name server working? Has the HOSTS file on your PC been
  corrupted? If no domain name server or HOSTS file is available, you must specify the full IP
  address of the host server. For example: 124.24.36.85.
- You have entered an IPv6 address, but have not enabled IPv6 support on your PC. Contact
  Microsoft for more information.
- You must have an appropriately configured IP router (gateway) in order to connect to servers
  outside your own network. Check to see whether the computer serving as the router is up and
  running.

Connection timed out.
Server response time can be affected by the distance between sites. If you see this message when
trying to connect to a server, increase the Connect Timeout setting to give the server more time to
respond during the login process.
Reflection FTP hangs when you try to connect

On some systems, turning off the use of animation (such as showing a waving flashlight while you are waiting for a directory listing) fixes display problems that cause Reflection to hang when you attempt a connection. To disable the use of animation, open the Tools menu, click Options, open the Preferences tab and enable Do not use animation.

Host cannot respond to the PWD command

By default, Reflection sends a PWD command when you connect to your server. Some servers don't support this command. Press F7 to open the command window before you try connecting to your server. If the server returns an error after Reflection sends the PWD command, try enabling this setting. To configure Reflection to connect without the PWD command, open the Directories tab of the Site Properties dialog box and select Don't send PWD Command.

PASV is not implemented by the server

By default, the client connects using the PASV command. This causes the client to initiate a separate data connection for directory listings and file transfers, which is required for connections through some firewalls. If your server does not support the PASV command, you can disable the Use passive mode setting on the Connection tab of the Site Properties dialog box.

Server returns error "425 can't establish data connection"

If you don't see a directory listing in either the server pane or the command window, your server may not support the PASV command. Try clearing the Use passive mode setting in the Connection tab of the Site Properties dialog box.

System cannot find the path

This error may indicate that the FTP Client is trying to find a local file path that does not exist. Check the local Home folder setting to be sure that the folder path exists on your computer. To view or edit this setting, open the Site Properties dialog box, click Directories, then find Home folder under Local.

Using the FTP Command Window

In this Section

- “The FTP Command Window” on page 815
- “Clear the Command Window” on page 816
- “Use the FTP Command Line” on page 817
- “FTP and SFTP Command Syntax” on page 817
- “Quotation Marks in FTP or SFTP Commands” on page 818

The FTP Command Window

Index Term
Primary: FTP commands
Secondary: FTP command window

Index Term
Primary: FTP Client
Secondary: command window
The **FTP Client** command window shows the data sent to and from the server and also includes the FTP Command line, which you can use to enter FTP or SFTP commands. Use **View > Command Window** to show or hide the command window.

An identifying color is assigned to each type of client/server communication that displays in the window. For example, if you are using the Windows default color scheme:

<table>
<thead>
<tr>
<th>Color of text</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>black</td>
<td>A command status message received from the server (command status messages are the server's responses to FTP or SFTP commands issued by the client)</td>
</tr>
<tr>
<td>royal blue</td>
<td>A Reflection FTP or SFTP command entered at the FTP command line</td>
</tr>
<tr>
<td>dark blue</td>
<td>A data channel response from the server, generally a file listing. After a connection is made, this color is also used to display the presumed server type.</td>
</tr>
<tr>
<td>green</td>
<td>A client FTP or SFTP command that the <strong>FTP Client</strong> is sending to the server</td>
</tr>
<tr>
<td>red</td>
<td>An error message</td>
</tr>
</tbody>
</table>

**NOTE**

- If the window background for your current Windows color scheme is set to blue, green, black, or red, the client changes the identifying colors used in the datacomm display window to ensure that text is visible against the window background. The display color for messages received from the server defaults to the color of window text in your current Windows color scheme.

- If you are connected to two sites in the same **FTP Client** window, you can use the command line to view communication between the client and the server, but you cannot enter commands. Commands sent to and from the second server are preceded by this identifier: **[Server 2]**. If there is more than one line of output (such as directory listings and multi-line banners), only the first line has this identifier.

**Related Topics**

- “Use the FTP Command Line” on page 817
- “Clear the Command Window” on page 816
- “FTP and SFTP Command Syntax” on page 817
- “Command Reference” on page 825

**Clear the Command Window**

**Index Term**

Primary: FTP Client  
Secondary: clearing the command window

**To clear the **FTP Client** command window**

1. In the Command window, click the right mouse button and select **Clear All**.
Use the FTP Command Line

The FTP Client command line provides an alternate way for you to communicate with the server. You can enter FTP or SFTP commands on the FTP command line to move files between the FTP server and your PC.

To show or hide the FTP command line

- From the View menu, choose Command Window to toggle the command window display.
  
  The FTP command line appears at the bottom of the command window.

To enter commands

1. Click in the command line or press Shift+F7 to move the cursor to the command line.
2. Enter an FTP or SFTP command, depending on your connection type.
3. Press the Enter key to execute the command.

The FTP Client keeps a list of up to 50 commands from the current session. You can use the drop-down arrow on the right side of the command line to recall items from this list.

**NOTE:** If you are connected to two sites in the same FTP Client window, you can use the command line to view communication between the client and the server, but you cannot enter commands. Commands sent to and from the second server are preceded by this identifier: [Server 2]. If there is more than one line of output (such as directory listings and multi-line banners), only the first line has this identifier.

Related Topics

- “FTP and SFTP Command Syntax” on page 817
- “FTP Scripting” on page 819
- “Command Reference” on page 825

FTP and SFTP Command Syntax

Related Topics

- “FTP and SFTP Command Syntax” on page 817
- “FTP Scripting” on page 819
- “Command Reference” on page 825
Index Term
Primary: FTP commands
Secondary: command syntax

FTP Command Index (page 825)  SFTP Command Index (page 858)

Case is not important for commands and keywords entered at the FTP command line. Depending on your FTP server computer, however, passwords, directory names, filenames, and other server-specific information may be case sensitive.

The FTP Client accepts abbreviated versions of commands, requiring that you type only as much of the command keyword as is necessary to make it unique. For example, the GET command can be abbreviated to G; to get the server file jokes.old you could enter g jokes.old at the FTP command line.

In the command references in this guide, the following conventions apply:

- When parameters are enclosed in angle brackets, they represent a string that must be added to complete the command. For example, <clientfile> means you must give a complete path to clearly reference a particular file. Do not include the brackets when entering the parameter.
- A vertical bar separates mutually exclusive options. For example, <servername> | <ip address> means you may use either of the options, but not both.
- Parameters enclosed in square brackets indicate optional components of a command; that is, any information contained within a pair of such brackets can, but need not, be included in the command. For example, the following indicates that the LCD command can be used with or without a PC directory:

  lcd [<pc directory>]

Related Topics
- “Quotation Marks in FTP or SFTP Commands” on page 818
- “Using the FTP Command Window” on page 815
- “FTP Scripting” on page 819
- “Use the FTP Command Line” on page 817

Quotation Marks in FTP or SFTP Commands

Index Term
Primary: FTP commands
Secondary: use of quotation marks

If a command takes only one argument, no quotation marks are required. For example:

CD Travel Agents

With commands that take more than one argument, any argument that contains spaces must be enclosed in double quotation marks. For example, to transfer the server file Account History to the PC and name it Accthist.txt, you would enter this command:

GET "Account History" TO Accthist.txt

If an argument begins with a double quotation mark, all double quotation marks in the argument must be doubled. For example, to transfer the server file "Remembering You", you would enter a command in this format:

GET ""Remembering You""
FTP Scripting

Related Topics

- “Options for Automating FTP Client Transfers” on page 744

In this Section

- “FTP Client Scripting” on page 819
- “Record a Script” on page 820
- “Run a Script” on page 820
- “Edit a Script” on page 821
- “FTP Client Script File Format” on page 821
- “Which Actions Are Captured by the Script Recorder?” on page 822
- “Password Security within Scripts” on page 823
- “Commands for Error Handling” on page 823
- “Running a Script as a Background Task” on page 824
- “Creating Script Log Files” on page 825

FTP Client Scripting

Index Term
Primary: scripts (FTP Client)
Secondary: overview

Index Term
Primary: FTP Client script files
Secondary: overview

FTP Client scripts allow you to automate connection and file transfer operations. For example, you can automate file transfers to and from a server. Automated transfers can be carried out without the need to interact directly with the FTP Client.

A script file is an ASCII text file that contains a sequence of FTP (or SFTP) commands. Each command must be on a separate line. You can create a script using the Script Recorder. You can also create a new script or modify an existing script using a text editor (such as Notepad).

Use the FTP Client script recorder to record actions as commands—you do not have to do any writing or programming to create a script that can be played back later. Scripts can automate many sorts of tasks (for example, configuring file transfer options, connecting to an FTP site, or transferring files).

When you play back a script, commands are executed as though they had been entered at the FTP command line.

Related Topics

- “Record a Script” on page 820
- “Run a Script” on page 820
- “Edit a Script” on page 821
- “FTP Client Script File Format” on page 821
Record a Script

Index Term
Primary: scripts (FTP Client)
Secondary: recording a script

Use the FTP Client script recorder to record actions as commands—you do not have to do any writing or programming to create a script that can be played back later. Scripts can automate many sorts of tasks (for example, configuring file transfer options, connecting to an FTP site, or transferring files).

To record a script

1. From the Script menu, choose Start Recording.
   When the script recorder is active, a camera icon appears in the status bar.
2. Perform the actions you want to record.
3. From the Script menu, choose Stop Recording.
4. In the Save Script dialog box, type a name for the script in the File name box.
   The default extension for script files is .rfs.
5. Click Save.

**NOTE:** You cannot record scripts when you are connected to two sites in the same session.

Related Topics

- “Run a Script” on page 820
- “Edit a Script” on page 821
- “Which Actions Are Captured by the Script Recorder?” on page 822
- “FTP Scripting” on page 819

Run a Script

Index Term
Primary: scripts (FTP Client)
Secondary: running a script

1. From the Script menu, choose Run Script.
2. In the Run Script dialog box, select the script you want to run.
3. Click Open to play back the selected script.

Related Topics

- “Running a Script as a Background Task” on page 824
- “Creating Script Log Files” on page 825
- “FTP Client Scripting” on page 819
Edit a Script

1. From the Script menu, choose Edit Script.
2. In the Edit Script dialog box, select the script you want to edit.
3. Click Open to open the file in Notepad.

Related Topics
- “FTP Client Script File Format” on page 821
- “Password Security within Scripts” on page 823
- “Commands for Error Handling” on page 823
- “FTP Client Scripting” on page 819

FTP Client Script File Format

A script file is an ASCII text file that contains a sequence of FTP (or SFTP) commands.

- Each command must be on a separate line.
- Space and tab characters can precede the command on a line.
- Use a semicolon character (;) for comments. The FTP Client ignores comment text.

You can use comments to explain one or more lines of code. For example:

;The following lines connect to the server and change
;the working directories to PREPRESS (client) and
;PRESS (server).
open forum thomasp XOYRCNEL973L9L960376ONMO770L35L7NMO87PM79
lcd c:\prepress
cd /press

You can also add a comment at the end of a command. For example:

set transfer-disposition unique ;do not overwrite files
mput script is s*.doc ;copy the .DOC files

NOTE: Semicolons are not supported for comments in scripts supplied to the sftp command line using the -B option. Use the number sign (#) to mark comments in these batch files.

Related Topics
- “Edit a Script” on page 821
- “Password Security within Scripts” on page 823
- “Commands for Error Handling” on page 823
- “FTP Client Scripting” on page 819
Which Actions Are Captured by the Script Recorder?

Most connection and file transfer operations you perform while the script recorder is on are recorded, but there are some exceptions: configuration options that you change via the graphical user interface are not recorded. To include file transfer and character translation configuration settings in a recorded script, enter `SET` parameters at the command line or edit the script to add `SET` parameters.

**NOTE:** You cannot record scripts when you are connected to two sites in the same session.

The following actions generate FTP script commands that are recorded:

- All commands entered in the command window are recorded.
- File operations you perform using the graphical user interface (GUI). See the following table to see which FTP commands are recorded.

<table>
<thead>
<tr>
<th>FTP Command</th>
<th>GUI Action That Generated It</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPEN</td>
<td>Opening an FTP Site (Open toolbar button or menu).</td>
</tr>
<tr>
<td>CLOSE</td>
<td>Closing an FTP Site.</td>
</tr>
<tr>
<td>CD</td>
<td>Clicking on a folder in the Site pane (or using Go to dialog box).</td>
</tr>
<tr>
<td>LCD</td>
<td>Clicking on a folder in the Local pane.</td>
</tr>
<tr>
<td>DELETE*</td>
<td>Deleting a file in the Site pane.</td>
</tr>
<tr>
<td>LDELETE*</td>
<td>Deleting a file in the Local pane.</td>
</tr>
<tr>
<td>RDALL*</td>
<td>Deleting a folder in the Site pane.</td>
</tr>
<tr>
<td>LRDALL*</td>
<td>Deleting a folder in the Local pane.</td>
</tr>
<tr>
<td>MD</td>
<td>Creating a folder in the Site pane.</td>
</tr>
<tr>
<td>LMD</td>
<td>Creating a folder in the Local pane.</td>
</tr>
<tr>
<td>GET*</td>
<td>Dragging a file from the Site pane to the Local pane.</td>
</tr>
<tr>
<td>&lt;None&gt;</td>
<td>Dragging a file from the Site pane to Windows Explorer, the desktop, or a My Computer folder.</td>
</tr>
<tr>
<td>CPDIR*</td>
<td>Dragging a folder from the Site pane to the Local pane.</td>
</tr>
<tr>
<td>&lt;None&gt;</td>
<td>Dragging a folder from the Site pane to Windows Explorer, the desktop, or a My Computer folder.</td>
</tr>
<tr>
<td>PUT*</td>
<td>Dragging a file from the Local pane to the Site pane.</td>
</tr>
<tr>
<td>PUT*</td>
<td>Dragging a file to the Site pane from Windows Explorer, the desktop, or a My Computer folder.</td>
</tr>
<tr>
<td>LCPDIR*</td>
<td>Dragging a folder from the Local pane to the Site pane.</td>
</tr>
<tr>
<td>LCPDIR*</td>
<td>Dragging a folder to the Site pane from Windows Explorer, the desktop, or a My Computer folder.</td>
</tr>
</tbody>
</table>

* Multiple selection invokes this FTP Command multiple times.
If you enter an open <servername> <username> <password> command, the <password> is saved as obfuscated text in the script file. For example:

open ftp.myco.com joe WPD6119003929K148O6KN706S2L0739LL00875N44O274

If the server returns an error message when a command is entered, that error message is recorded as a comment line in the script. For example:

cd /users/bobc
; 550 /users/bobc: No such file or directory.

Password Security within Scripts

Passwords can be included in scripts for establishing FTP (but not SFTP) connections. When you write a script in a text editor, if the script includes a complete OPEN command (open <servername> <username> <password>), or includes a PASSTHRU command, passwords you add manually will be visible in the editor as plain text. For greater password security use one of these methods:

- Use the Script Recorder to record the connection to the server. Passwords are stored as obfuscated text in the script file. When the script runs and a connection is opened, the client deciphers the password and sends it to the server.
- Edit the script to remove the <password> parameter, which is the last parameter in the OPEN command. The OPEN command should have the format: open <servername> <username>. When the script runs and a connection is opened, the client prompts the user for a password. You may also want to omit the <username> parameter, which causes the client to prompt for both the user name and the password.

Commands for Error Handling

Include a CONTINUE command in your script file to tell the FTP Client how to handle errors that occur when you are using wildcards to transfer files or delete local files. When CONTINUE is on, file transfers or local file deletes proceed until all files satisfying the wildcard specification have been...
transferred or deleted, even when an error occurs. When CONTINUE is OFF, the transfer or delete operation aborts if an error occurs during the process; the script file terminates in response to the error, unless ABORT-ON-ERROR is set to NO.

The ABORT-ON-ERROR parameter specifies whether execution of a script stops whenever an error occurs in response to a command. When ABORT-ON-ERROR is set to YES, script execution will terminate any time a command results in an error response from the FTP Client or server.

Use caution when setting ABORT-ON-ERROR to NO. Continuing command execution after an error can yield unexpected results.

**Related Topics**

- “Command Reference” on page 825
- “CONTINUE” on page 829
- “Creating Script Log Files” on page 825
- “Handle Existing Files (Transfer Mode)” on page 783

**Running a Script as a Background Task**

Index Term
Primary: FTP Client script files
Secondary: running as background tasks

You can create a script and configure the FTP Client so that, when the script executes, the client runs as a background task and there is no interaction or communication with the user. To do so:

- Create a shortcut with a startup command that automatically executes the script. In the Run box, select Minimized to specify that the FTP Client should run minimized on the desktop.
- Have the script connect to a site for which you already have saved the user name and password and any passthrough settings needed to connect to that site. This prevents the client from prompting for connection information.
- Include a QUIT command to have the client shut down when the script completes.
- Use the following SET parameters to control the client display of messages and prompts:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>QUIET-STATUS</td>
<td>Set to YES to suppress the connection and transfer progress dialog boxes and the Directory Definition Wizard.</td>
</tr>
<tr>
<td>SMART-TYPE-DEFAULT</td>
<td>Do not set to ASKUSER. When set to ASKUSER, the user is prompted for a transfer method if the script transfers an unrecognized file type.</td>
</tr>
<tr>
<td>TRANSFER-DISPOSITION</td>
<td>Do not set to PROMPT. When set to PROMPT, the user is prompted during transfer to specify handling for files that exist at the destination.</td>
</tr>
<tr>
<td>CONFIRM-DELETE</td>
<td>Set to NO to prevent the client from prompting for confirmation prior to deleting files or folders.</td>
</tr>
<tr>
<td>RESUME-PARTIAL-TRANSFERS</td>
<td>Do not set to ASKUSER. When set to ASKUSER, the user is prompted to choose whether to resume a partial transfer if the FTP Client detects that a prior incomplete server file download occurred.</td>
</tr>
</tbody>
</table>
Creating Script Log Files

When you start the FTP Client with a startup command that executes a script file, you can include a command line switch that directs the client to create a log file that stores a record of the results of the commands that are executed.

If you want to create a log file when you execute a script file from within the client application, from the Tools menu, choose Start Logging, and then, from the Script menu, choose Run Script.

If you are using the FTP Automation API to control the FTP Client application, you can control logging using the StartLog and StopLog methods.

Related Topics
- “FTP Client Startup Switches” on page 802
- “Run a Script File at Startup” on page 804
- “Options for Automating FTP Client Transfers” on page 744

Command Reference

The commands available to you for use on the command line and in scripts depend on which kind of connection you have made.

TIP: When you open a command topic, you can tell if it is available with FTP, SFTP, or both by looking to see which list or lists are linked to at the top of the topic.

In this Section
- “FTP commands” on page 825
- “SFTP commands” on page 858

FTP commands
You can use the commands in this list on the FTP Client command line or in a script. (If you have made a Secure Shell SFTP connection, use the “SFTP commands” on page 858 instead of the commands in this list.) Use the following links to view additional command reference information.

In this Section

- “ACCOUNT” on page 827
- “APPEND” on page 827
- “ASCII” on page 828
- “BINARY” on page 828
- “CD” on page 828
- “CHMOD” on page 828
- “CLOSE” on page 829
- “CONNECT” on page 829
- “CONTINUE” on page 829
- “CPDIR” on page 830
- “DELETE” on page 830
- “DIR” on page 831
- “DISCONNECT” on page 831
- “DISPLAY” on page 831
- “EXIT” on page 832
- “GET” on page 832
- “HELP” on page 832
- “LCD” on page 833
- “LCPDIR” on page 833
- “LDEL” on page 833
- “LDIR” on page 834
- “LMD” on page 834
- “LRENAME” on page 835
- “LS” on page 836
- “LTYPE” on page 836
- “MD” on page 836
- “MDEL” on page 836
- “MGET” on page 837
- “MPUT” on page 838
- “OPEN” on page 839
- “PASSTHRU” on page 840
- “PUT” on page 841
- “PWD” on page 842
- “QUIT” on page 842
ACCOUNT

Syntax: account <accountname>

FTP Command Index (page 825)

Some servers (for example, some IBM FTP servers) require the name of the account that the user wants to access. For servers with this requirement, you cannot work with the files in that account until you supply an account name. If you connect using an “OPEN” on page 839 command that includes an <account> parameter, the account name is not actually sent to the server unless the server specifically prompts for an account during the login. If your server requires an account name, but doesn't request that name during the login process, use the ACCOUNT command to explicitly tell the server which account you want to use.

<accountname> Specifies an account that the logged in user has rights to access. For case-sensitive servers, be sure to use the appropriate case when typing the account name.

APPEND

Syntax: append <clientfile> [to] [<serverfile>]

FTP Command Index (page 825)

The APPEND command sends a file to the FTP server, appending it to the current server file. If the server file does not exist, this command creates it, and works exactly like the “PUT” on page 841 command.

<clientfile> Specifies the PC file to transfer to the FTP server.

to <serverfile> Specifies the server file to which the PC file should be appended. If this option is omitted, the PC file is appended to a server file having the same name as the PC file. If the specified server file does not exist, it is created. The TO keyword is optional.

Examples

The following command appends a PC file to a server file of the same name:

APPEND WHATSNEW.DOC
This command appends a PC file to the specified server file:

```
APPEND WHATSNEW.DOC TO DOCUMENT.TXT
```

**ASCII**

**Syntax:** ascii

FTP Command Index (page 825) SFTP Command Index (page 858)

The `ASCII` command changes the current file transfer method to ASCII. Use this transfer method to move ASCII text files between the server and your PC.

**BINARY**

**Syntax:** binary

FTP Command Index (page 825) SFTP Command Index (page 858)

The `BINARY` command changes the current file transfer method to binary (image). Use this transfer method to transfer binary files, such as .EXE files and compressed files, between two PCs (via a server), or between two servers (via a PC).

**CD**

**Syntax:** cd <server directory>

FTP Command Index (page 825) SFTP Command Index (page 858)

The `CD` command changes the working directory on the FTP server.

```
<server directory> Specifies a directory on the server.
```

**Examples**

This command changes to the directory "Asian Artists" on a UNIX system:

```
CD Asian Artists
```

This command changes directories on a VAX/VMS system:

```
CD SYS$USERS:[ARNOLD.DOCS]
```

**CHMOD**

**Syntax:** chmod <numeric permission mask> <server file or directory>

FTP Command Index (page 825) SFTP Command Index (page 858)

The `CHMOD` command changes the permissions associated with a file or directory.
**Example**

This command sets attributes to `-rw-r--r--` for the specified file.

```plaintext
chmod 644 myfile.htm
```

**CLOSE**

**Syntax:** close

FTP Command Index (page 825)

The **CLOSE** command closes the connection to the FTP server.

You can also use **EXIT** or **QUIT** as a synonym for **CLOSE**.

**CONNECT**

**Syntax:** connect [servername]

FTP Command Index (page 825)

The **CONNECT** command initiates a connection to an FTP server. If no site is specified, a dialog box will prompt for this information. Unlike "OPEN" on page 839, this command does not prompt for user name and password. This information must be entered manually. For example, the following command sequence would connect you to an FTP server that does not use a passthrough server (firewall):

```plaintext
CONNECT <server>
USER <username>
PASS <password>
```

Note that passwords appear as text on screen when you enter them directly in the command window. Because the **OPEN** command prompts for passwords with dialog boxes that do not display password text, this command is preferable for most connections. Use **CONNECT** if you are troubleshooting connections through a firewall.

**CONTINUE**

**Syntax:** continue [on | off]

FTP Command Index (page 825)

The **CONTINUE** command instructs Reflection FTP to ignore errors that occur during a wildcard file transfer initiated at the FTP command line. File transfer proceed as though no error occurred, until all files satisfying the wildcard specification have been transferred.

**CONTINUE** with no arguments tells Reflection FTP to ignore an error in the next "MGET" on page 837 or "MPUT" on page 838 command only.
The **CONTINUE** command only applies to the series of commands that comprise an **MGET** or **MPUT** block (such as **LIST**, **GET**, **PUT**, **CD**). If an error is encountered in any of the commands in the series, the script will stop after it finishes the complete **MGET** or **MPUT** command series. To allow the script to process further commands, change **SET-ABORT-ON-ERROR** (page 845) to NO.

The **CONTINUE** command does not apply to drag-and-drop file operations.

**Example**

This sequence of commands instructs Reflection FTP to ignore any error in the next **MPUT** command. Without **CONTINUE**, the **MPUT** command aborts if an error occurs during the transfer.

```
CONTINUE
MPUT ACCT*.TXT
```

See “**ABORT-ON-ERROR Script Sample**” on page 856 for an additional example.

**CPDIR**

**Syntax:** `cpdir <server directory> [ <pc-path> ] [ askuser | cancel | overwrite | skip ]`

**FTP Command Index (page 825)**

The **CPDIR** command copies the specified server directory to the PC. If a PC directory is not specified, the server directory is copied to the current PC path.

```
server directory  Specifies the name of the server directory.
pc-path           Specifies the PC drive and folder.
askuser | cancel | overwrite | skip           Specifies what to do if the target folder already exists. ASKUSER is the default.
```

**DELETE**

**Syntax:** `delete <serverfile>`

**FTP Command Index (page 825)**

The **DELETE** command deletes a file matching the given filespec on the FTP server.

**NOTE:** If the **SET parameter** (page 845) **CONFIRM-DELETE** is set to YES, the user is prompted for confirmation before deleting.

```
<serverfile> Specifies the name of a server file to delete. This can include a full directory path to the file. On some systems such as UNIX FTP servers, case is important when specifying directories and file names.
```

**Examples**

This command deletes **MEMO.DOC** from the current server directory:

```
DELETE MEMO.DOC
```
The next command deletes the budget.new file from the /users/jill jones directory on a UNIX FTP server:

DELETE /users/jill jones/budget.new

**DIR**

**Syntax:** dir [server filespec]

FTP Command Index (page 825)

The **DIR** command displays a detailed listing of server files matching the given file specification. (Compare this to the “LS” on page 862 command, which displays a less detailed listing.)

<server filespec> Specifies a directory, file, or group of files on the FTP server. If this option is not used, the contents of the current server directory are displayed. The syntax for <server filespec> varies according to your FTP server.

**Example**

This command displays a list of executable files in the current directory on a VAX/VMS FTP server:

DIR *.exe

**DISCONNECT**

**Syntax:** disconnect

FTP Command Index (page 825)

The **DISCONNECT** command closes the connection to the FTP server.

You can also use **CLOSE**, **EXIT**, or **QUIT** as a synonym for **DISCONNECT**.

**DISPLAY**

**Syntax:** display <string>

FTP Command Index (page 825)

The **DISPLAY** command displays data in the command window as if it had been received from the FTP server.

<string> The <string> parameter can be any string of characters.

The character string displays on a single line. If the specified character string exceeds the width of the Reflection FTP window, characters at the end of the string will be hidden; the string will not wrap to the next line. For example, if the window is sized to 50 columns wide and the <string> is 60 characters long, the last 10 characters of the string will be hidden.

**Example**

You can use the **DISPLAY** command to do such things as display a message or reminder about the current process. For example, the following command displays a message that a logon process occurs next:

DISPLAY Next process is logon to bigben.timer.london
EXIT

Syntax: exit

FTP Command Index (page 825)  SFTP Command Index (page 858)

The EXIT command closes the connection to the server.

GET

Syntax: get <serverfile> [to] [<clientfile>] [append | askuser | cancel | overwrite | skip | unique]

FTP Command Index (page 825)  SFTP Command Index (page 858)

The GET command transfers a file from the server to the PC. Wildcards are not supported with the GET command—they are treated as ordinary characters and are assumed to be part of the file name. To transfer multiple files, use “MGET” on page 837.

Before using the GET command, if necessary, use the “ASCII” on page 859, “BINARY” on page 828, “TENEX” on page 868, or “SMART” on page 868 command to override the default file transfer method setting specified on the Tools menu.

A variety of site-specific SET parameters can affect the transfer operation. Click here (page 855) for more information.

<serverfile> Specifies the name of the server file.

to <clientfile> Specifies the name of the PC file to be created. If this option is omitted, the client file receives the same name as the server file. The TO keyword is optional.

append | askuser | cancel | overwrite | skip | unique Specifies what to do if the destination file already exists. If this option is omitted, the active TRANSFER-DISPOSITION (page 845) setting is the default.

Examples

The following example transfers the server file MEMO.DOC from the server to the PC, giving the PC file the same name:

GET MEMO.DOC

This example transfers the VAX/VMS FTP server file MORTGAGE.PAPERS to the PC, giving the PC file the name MORTGAGE.TXT:

GET MORTGAGE.PAPERS MORTGAGE.TXT

HELP

Syntax: help [<command>]

FTP Command Index (page 825)

HELP displays a short summary of FTP commands. You can type HELP <command> at the FTP command line to see information on a specific FTP command. For a listing of FTP commands without descriptions, enter HELP at the command line.
With many FTP servers, you can enter `QUOTE HELP` at the command line for a list of commands the server recognizes. Entering `QUOTE HELP <command>` sometimes gives more detailed information about the command. See “QUOTE” on page 842 for more information.

**NOTE: HELP** displays the FTP command list even if you have made an SFTP connection. Click here (page 858) for a list of commands available during SFTP sessions.

**LCD**

**Syntax:** `lcd [pc drive/folder] | ..`

The **LCD** command opens another folder on the PC.

If no `<folder>` is specified, **LCD** displays the path for the current PC folder.

To change folders, type the folder at the FTP command line, for example, type `LCD F:\Documents` and press Return.

```plaintext
<pc drive/folder> Specifies the drive (if other than the current drive) and folder to change to.
.. Specifies that you want to change to the parent folder.
```

**Example**

This command changes your current folder to the China folder within the Asian Travel folder on drive D:

```
LCD d:\Asian Travel\China
```

**LCPDIR**

**Syntax:** `lcpdir <pc drive/folder> [server folder] [askuser | cancel | overwrite | skip]`

The **LCPDIR** command copies the specified PC folder to the server. If a server folder is not specified, the PC folder is copied to the current server path.

```plaintext
cpc drive/folder Specifies the local folder. Use quotation marks if the file or path includes spaces. For example: lcpdir "d:\Asian Travel\China"
<server folder> Specifies the server folder.
askuser | cancel | overwrite | skip Specifies what to do if the target folder on the server already exists. ASKUSER is the default.
```

**LDEL**

**Syntax:** `ldel <pc filespec>`

The **LDEL** command deletes the specified file on the PC. Wildcards are not supported.
NOTE: If the SET parameter (page 845) CONFIRM-DELETE is set to YES, the user is prompted for confirmation before deleting.

<pc filespec> Specifies the name of a PC file to delete. The filespec can include a full directory path to the file.

Example
This command deletes Map.bmp from the France folder within the European Travel folder on the PC:
LDEL \European Travel\France\map.bmp

LDIR
Syntax: ldir [<pc filespec>]
FTP Command Index (page 825)
The LDIR command displays a listing of PC files matching the given filespec.

<pc filespec> Specifies a folder, a file, or a group of files on the PC. If this option is not used, the contents of the current PC folder are displayed.

Example
This command displays a listing of all the files in the specified PC folder that have the name Old Data and end with any extension:
LDIR D:\Results\Old Data.*

LMD
Syntax: lmd <pc directory>
FTP Command Index (page 825)
The LMD command creates a folder on the PC.

<pc folder> Specifies the drive where you want to create the folder (if other than the current drive) and the folder name.

Example
This command creates the folder Music on the current PC drive:
LMD \Music

LRD
Syntax: lrd <pc directory>
FTP Command Index (page 825)
The LRD command deletes a PC folder and all the files and folders it contains.
You can also use LRDALL as a synonym for LRD.
NOTE: If the SET parameter (page 845) CONFIRM-DELETE is set to YES, the user is prompted for confirmation before deleting.

<pc folder> Specifies the location and name of the folder you want to delete. The <folder> specification must follow PC conventions

Example

This command deletes the folder "Trial Dates" from within the "Cases" folder on the J drive:

LRD J:\Cases\Trial Dates

LRDALL

Syntax: lrdall <pc folder>

FTP Command Index (page 825)

The LRDALL command deletes a PC folder and all the files and folders it contains.

You can also use LRD as a synonym for LRDALL.

NOTE: If the SET parameter (page 845) CONFIRM-DELETE is set to YES, the user is prompted for confirmation before deleting.

<pc folder> Specifies the location and name of the folder you want to delete.

Example

This command deletes the folder "Trial Dates" from within the "Cases" folder on the J drive:

LRD J:\Cases\Trial Dates

LRENAME

lrename <pc filename> <new filename>

FTP Command Index (page 825)

The LRENAME command changes the name of a local file to the new name specified.

<pc filename> Specifies the name of the PC file you want to rename. The specification can include the PC drive and folder where the file is located. If the file location or name contains spaces, the specification must be enclosed with quotation marks. For example: "D:\To do\Monthly tasks".

<new filename> Specifies the name you want to give the file. If the file to be renamed does not exist on the active local drive and folder, you must include the location in the <new filename> specification. Use quotation marks if the file or path includes spaces. For example, "D:\To do\Work assignments".

Example

From the current folder on the C drive, this command renames a file in the folder "Archive" on the D drive, changing the name from "Stories.txt" to "Fairy tales":

LRENAME D:\Archive\Stories.txt "D:\Archive\Fairy tales"
LS

Syntax: `ls [server filespec]`

FTP Command Index (page 825)  SFTP Command Index (page 858)

The LS command displays a simple listing of server files matching the given filespec. (Compare this to the "DIR" on page 831 command, which displays a more detailed listing.)

`<server filespec>` Specifies a folder, file, or group of files on the server. If this option is not used, the contents of the current server folder are displayed.

Example

In this example, the names of all files in the current folder on a UNIX FTP server are listed:

`LS *.*`

LTYPE

Syntax: `ltype <clientfile>`

FTP Command Index (page 825)

The LTYPE command displays the contents of a PC file in the FTP command window.

`<clientfile>` Specifies the location and name of the PC file. This specification cannot contain wildcards.

Example

The following command displays the content of the file Com.doc in the Subjects folder on the J drive on the PC:

`LTYPE J:\Subjects\Com.doc`

MD

Syntax: `md <server folder>`

FTP Command Index (page 825)

The MD command creates a folder on the server.

`<server folder>` Specifies the name and location of the new folder.

Example

This command creates the folder Films within the current folder on the current FTP UNIX server drive:

`MD Films`

MDEL

Syntax: `mdel <server filespec>`

The MDEL command deletes one or more files matching the given filespec on the FTP server.
**MDEL** differs from “DELETE” on page 830 in that **MDEL** supports multiple file deletions from the server using server wildcard characters. Your FTP server must support wildcards for multiple file deletions.

**NOTE:** If the **SET** parameter (page 845) CONFIRM-DELETE is set to YES, the user is prompted for confirmation before deleting.

<server filespec>  Specifies one server file or (using server wildcards) multiple server files. This can include a full directory path to the file. On some systems such as UNIX FTP servers, case is important when specifying directories and file names.

**Examples**

This command deletes all files from the current server directory:

```
MDEL *
```

This command deletes all files ending with ".htm" from the current server directory:

```
MDEL *.htm
```

See “ABORT-ON-ERROR Script Sample” on page 856 for an example.

**MGET**

**Syntax:**

```
mget <server filespec> [to] [<pc filespec>] [append | askuser | cancel | overwrite | skip | unique]
```

**FTP Command Index** (page 825) **SFTP Command Index** (page 858)

The **MGET** command transfers one or more files matching the given filespec from the FTP server to the PC. You can use wildcards to transfer multiple files. Most servers support wildcards in the `<serverspec>`. However, if your server doesn't support wildcards in an "LS" on page 862 command, using **MGET** with a wildcard specification may result in a transfer of all files in the current directory.

**NOTE:** The Reflection client supports **MGET** in SFTP sessions, however you should test transfers that use wildcard characters because the SFTP server may not interpret wildcard specifications correctly.

Before using the **MGET** command, if necessary, use the “ASCII” on page 859, “BINARY” on page 828, “TENEX” on page 868, or “SMART” on page 868 command to override the default file transfer method setting specified on the Tools menu.

A variety of site-specific **SET** parameters can affect the transfer operation. Click here (page 855) for more information.
Examples

This example transfers all files with a .Doc extension from the FTP server to the PC, placing the files in the current PC directory:

MGET *.Doc

This example adds the letter A to the transferred files. For example, test.txt becomes Atest.txt.

MGET *.* A*.*

See "ABORT-ON-ERROR Script Sample" on page 856 for an additional example.

MPUT

Syntax: mput <pc filespec> [to] [<server filespec>] [append | askuser | cancel | overwrite | skip | unique]

FTP Command Index (page 825)  SFTP Command Index (page 858)

The MPUT command transfers one or more files matching the given filespec from the PC to the FTP server. You can use wildcards to transfer multiple files.

NOTE: The Reflection client supports MPUT in SFTP sessions, however you should test transfers that use wildcard characters because the SFTP server may not interpret wildcard specifications correctly.

Before using the MPUT command, if necessary, use the "ASCII" on page 859, "BINARY" on page 828, "TENEX" on page 868, or "SMART" on page 868 command to override the default file transfer method setting specified on the Tools menu.

A variety of site-specific SET parameters can affect the transfer operation. Click here (page 855) for more information.
Examples

The following example transfers files in the Meeting Notes folder within the current folder on the PC that have a .Doc extension, placing the files in the current server folder. Source PC files that have the same name as files in the destination server folder are not transferred.

MPUT "Meeting Notes\*.Doc" skip

The following example adds the letter "A" to the front of files transferred to the server. For example Sample.htm becomes ASample.htm.

MPUT *.htm A*.htm

The final example removes file extensions from PC files copied to the server:

MPUT *. *.

OPEN

Syntax: open [<servername> [<username> [<password> [<account>]]]]

FTP Command Index (page 825)

The OPEN command connects to the FTP server and attempts to log in using the server name, username, and password specified. For case-sensitive servers, be sure to use the appropriate case when typing parameter values. If no parameters are specified with the OPEN command, the user is prompted for login information.

When only one parameter is present, it must be <servername>. If you add a second parameter it must be <username>. If you use three parameters, the third must be <password>.

NOTE: If you use a passthrough server to log into FTP servers, use the “PASSTHRU” on page 840 command to open a server connection.


Examples

This command opens an anonymous connection to the FTP server, supplying an e-mail address for the password:

```
OPEN ftp.acme.com anonymous jackie@mycompany.com
```

The following command opens a connection to the Headquarters FTP server for user Jackie. A password parameter wasn't specified, so the user will be prompted to enter a password during the login process.

```
OPEN Headquarters Jackie
```

PASSTHRU

Syntax 1: `passthru <passthrough servername> <username>@<servername> <password>`

Syntax 2: `passthru <passthrough servername> <passthrough username> <passthrough password> <username>@<servername> <password>`

Syntax 3: `passthru <passthrough servername> <passthrough username> <passthrough password> <servername> <username> <password>`

FTP Command Index (page 825)

The PASSTHRU command opens a connection to the FTP server using the passthrough server specified. Two styles of passthrough servers are supported. Reflection FTP sends different commands to log into the passthrough server and connect to an FTP server, based on the PASSTHRU syntax you specify.

When using any form of the PASSTHRU command, all parameters are required. If you specify `""` (a null value) for a parameter, the FTP Client displays a dialog box prompting for that value. For case-sensitive servers, be sure to use the appropriate case when typing parameter values.

**NOTE:** If the FTP server you connect to with the PASSTHRU command requires an account name, use the “ACCOUNT” on page 827 command to tell the FTP server which account you want to use.

Syntax 1

Use this type of PASSTHRU command if your passthrough server is a `username@servername` style server that does not require a passthrough password (that is, it does not perform authentication).
This form of the **PASSTHRU** command sends the current FTP server user name and server name in the format `username@servername` to the passthrough server specified in `<passthrough servername>`. The passthrough server uses this information to open a connection to the specified FTP server.

**Syntax 2**

Use this type of **PASSTHRU** command if your `username@servername` style passthrough server is set up to authenticate the user on the passthrough server prior to opening a connection to an FTP server.

This form of the **PASSTHRU** command allows you to log into a `username@servername` style passthrough server that will open the connection to the FTP server. The command logs into the passthrough server specified in `<passthrough servername>`. The login command provides the username and the password on the passthrough server, based on `<passthrough username>` and `<passthrough password>`. Once the user is authenticated on the passthrough server, the FTP `<username>` and FTP `<servername>` are sent to the passthrough server. This information is specified in the format: `username@servername`. The passthrough server uses this information plus the FTP server `<password>` to open a connection to the FTP server.

**Syntax 3**

This form of the **PASSTHRU** command allows you to log into a SITE servername style passthrough server that will open the connection to the FTP server.

Reflection FTP sends a command to log into the passthrough server specified in `<passthrough servername>`. The login command provides the username and the password on the passthrough server, based on `<passthrough username>` and `<passthrough password>`. Once a connection is opened, a site command is sent to the passthrough server, passing the settings needed to connect to the FTP server (`<servername>`, `<username>`, and `<password>`). The passthrough server uses this information to open a connection to the FTP server.

**PUT**

**Syntax:**

```
put <clientfile> [to] [<serverfile>] [append | askuser | cancel | overwrite | skip | unique]
```

**FTP Command Index (page 825)** **SFTP Command Index (page 858)**

The **PUT** command transfers a file from the PC to the server.

Wildcards are not supported with the **PUT** command; to transfer multiple files using wildcards, use “MPUT” on page 838.
Before using the `PUT` command, if necessary, use the “ASCII” on page 859, “BINARY” on page 828, “TENEX” on page 868, or “SMART” on page 868 command to override the default file transfer method setting specified on the `Tools` menu.

A variety of site-specific `SET` parameters can affect the transfer operation. Click here (page 855) for more information.

```plaintext
<clientfile>                           Specifies the name of the PC file. Use quotation marks if the file or path includes spaces.
to <serverfile>                       Specifies the name of the server file to be created. If the server file name is omitted, the server file is given the same name as the PC file. The TO keyword is optional.
append | askuser | cancel | overwrite | skip | unique                      Specifies what to do if the destination file already exists. If this option is omitted, the active `TRANSFER-DISPOSITION` (page 845) setting is the default.
```

**Examples**

The following example transfers the file Memo.doc from the PC to the server:

```plaintext
PUT Memo.doc
```

This example transfers the file HAPPY.ME from a PC to a VAX/VMS FTP server, giving the VMS file the name HAPPY.BIRTHDAY:

```plaintext
PUT HAPPY.ME TO HAPPY.BIRTHDAY
```

See “ABORT-ON-ERROR Script Sample” on page 856 for an additional example.

**PWD**

**Syntax:** `pwd`

`FTP Command Index (page 825) SFTP Command Index (page 858)`

The `PWD` command shows the server folder that is currently open. The name and location of the folder display in the FTP command window.

**QUIT**

**Syntax:** `quit`

`FTP Command Index (page 825) SFTP Command Index (page 858)`

The `QUIT` command closes the connection to the server.

---

**NOTE:** When you run a script from the Windows command line using the `/RFS` switch and the script ends in with a `QUIT` command, the FTP client shuts down automatically when the script is complete.

**QUOTE**

**Syntax:** `quote <string>`

`FTP Command Index (page 825)`

The `QUOTE` command sends a string to the FTP server. Use `QUOTE` to issue commands to the FTP server that are not implemented by the Reflection FTP Client.
With many FTP servers, you can type `QUOTE HELP` for a list of commands the server recognizes. Typing `QUOTE HELP <command>` sometimes gives more detailed information about the command.

`<string>` Specifies the string to send to the server. Valid strings you can use with the `QUOTE` command depend entirely on the FTP server; check your server documentation for details.

**Example**

To create the subdirectory FIFE on a VAX/VMS FTP server, you could use this command:

`QUOTE MKD MAYBERRY$USERS: [BARNEY.FIFE]`

**RD**

**Syntax:** `rd <server folder>`

FTP Command Index (page 825)

The `RD` command deletes an empty folder on the server.

Note: If the `SET` parameter (page 845) `CONFIRM-DELETE` is set to YES, the user is prompted for confirmation before deleting.

`<server folder>` Specifies the location and name of the folder you want to delete. Before you can delete a folder, you must delete the files and folders within it.

**Example**

This command deletes the folder Articles from the current server folder:

`RD Articles`

**RDALL**

**Syntax:** `rdall <server folder>`

FTP Command Index (page 825)

The `RDALL` command deletes a folder and all the files and folders within it on the server.

**NOTE:** If the `SET` parameter (page 845) `CONFIRM-DELETE` is set to YES, the user is prompted for confirmation before deleting.

`<server directory>` Specifies the location and name of the directory you want to delete. On some systems such as UNIX FTP servers, case is important when specifying directories.

**Examples**

This command deletes the directory Maps from the current server location:

`RDALL Maps`

This command deletes the folder "Destinations" from the "Travel/Europe" folder:

`RDALL /Travel/Europe/Destinations`
REGET

Syntax: reget <serverfile> [to] [<clientfile>]

FTP Command Index (page 825)

The REGET command directs the FTP Client to automatically resume an incomplete file transfer from
the FTP server to the PC. The Client automatically completes the file transfer from the point at which
the download was interrupted.

If the Client does not find a partial file locally, it performs a "GET" on page 832 to do a complete
transfer of the specified server file. If the local folder already contains a file with the same name as
the file being transferred, the local file is overwritten.

NOTE: The REGET command works only for BINARY file transfers. Before using the REGET
command, if necessary, use the “BINARY” on page 828 command to override the default file transfer
method setting specified on the Tools menu.

<serverfile> 
Specifies the name of the server file to transfer to the PC.

to <clientfile> 
Specifies the name of the PC file to be created.

For most REGET operations, you can omit this option. When this option is
omitted, the client file receives the same name as the server file.

If the interrupted file transfer specified that the downloaded file be given a new
name on the PC, be sure to use that name as the <clientfile> specification.
This ensures that the Client can find the partial local file and successfully resume
the transfer.

The TO keyword is optional.

RENAME

Syntax: rename <server filename> <new filename>

FTP Command Index (page 825) SFTP Command Index (page 858)

The RENAME command changes the name of a server file to the new name specified. On some
servers, you can use RENAME to specify both a new name and a new location for the file. In this
case, the file is moved to the new location and given the new name specified.

<server filename> 
Specifies the name of the server file you want to rename. The specification
can include the name of the server folder where the file is located. Use
quotation marks if the file or path includes spaces. For example: "Maps/ 
North America".

<new filename> 
Specifies the name you want to give the file. Use quotation marks if the file
or path includes spaces. For example:

"D:\To do\Work assignments".

On some servers, if you omit the path to the file you are renaming, the file is
moved to the current server folder and given the new name. If you want to
use RENAME to move a file, specify a new location and file name.

Example

In the current folder on the server, this command renames the file "Map of Canada" to "Canada":

RENAME "Map of Canada" Canada

From the "Maps" folder on the server, this command renames a file in the folder "Europe", changing the name from "England" to "Great Britain".

RENAME /Maps/Europe/England "*/Maps/Europe/Great Britain"

**SET**

**Syntax:** `set <set parameter> <value>`

**FTP Command Index (page 825)  SFTP Command Index (page 858)**

Use the **SET** command to configure Reflection. See the **SET Parameters (page 845)** for a list of available options.

**Examples**

These commands initialize various file transfer parameters:

```
SET TABS-TO-SPACES NO
SET TRANSFER-DISPOSITION Overwrite
SET TRANSFER-METHOD Ascii
SET TRANSLATE-FILES NO
```

**Related Topics**

- “**SET Parameter Reference**” on page 845
- “**SET Parameters and Equivalent Interface Settings**” on page 852
- “**Site-Specific File Transfer SET Parameters**” on page 855

**SET Parameter Reference**

The following parameters are for use with the “**SET**” on page 868 command. Settings are site-specific unless otherwise stated.

<table>
<thead>
<tr>
<th>SET Parameter</th>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABORT-ON-ERROR</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td>ACCOUNT</td>
<td>&lt;string&gt;</td>
<td>Specifies the name of the account to log into on an FTP server. This setting does not apply to SFTP connections.</td>
</tr>
<tr>
<td>ANONYMOUS</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td>ASCII-CLIENT-TYPE</td>
<td>&lt;value&gt;</td>
<td>When TRANSLATE-FILES and/or TRANSLATE-DIRECTORY-LISTING is YES, specifies the character set to use on the client PC during ASCII file transfers. Possible values are: PC-ENGLISH (IBM PC extended characters), PC-SLAVIC (DOS 852 code page), WINDOWS, WINDOWS-ANSI, WINDOWS-LATIN-2, WINDOWS-CYRILLIC, WINDOWS-GREEK, YUASCII. This setting does not apply to SFTP connections.</td>
</tr>
<tr>
<td>SET Parameter</td>
<td>Values</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ASCII-SERVER-TYPE</td>
<td>&lt;value&gt;</td>
<td>When TRANSLATE-FILES and/or TRANSLATE-DIRECTORY-LISTING is YES, specifies the FTP server character set to use during ASCII file transfers. Possible values (page 855). This setting does not apply to SFTP connections.</td>
</tr>
<tr>
<td></td>
<td>(Default: DEC Supplemental)</td>
<td></td>
</tr>
<tr>
<td>AUTO-SERVER-UPDATE</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td></td>
<td>(Default: YES)</td>
<td></td>
</tr>
<tr>
<td>CLIENT-HOME-DIRECTORY</td>
<td>&lt;string&gt;</td>
<td>Specifies the path to a home (default) directory for the local PC. If this setting is not set, the global Default local home directory setting is used.</td>
</tr>
<tr>
<td>CONFIRM-DELETE</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td></td>
<td>(Default: YES)</td>
<td></td>
</tr>
<tr>
<td>CREATE-SERVER-UPPER</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td></td>
<td>(Default: NO)</td>
<td></td>
</tr>
<tr>
<td>CREATE-8.3-FILenames</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td></td>
<td>(Default: NO)</td>
<td></td>
</tr>
<tr>
<td>CTRL-Z-EOF</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td></td>
<td>(Default: NO)</td>
<td></td>
</tr>
<tr>
<td>DELETE-TRAILING-SPACES</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td></td>
<td>(Default: NO)</td>
<td></td>
</tr>
<tr>
<td>EMAIL-ADDRESS</td>
<td>&lt;string&gt;</td>
<td>This global parameter specifies your Internet email address. When opening a connection, most anonymous FTP sites ask you to supply your email address, which is used as the password for your guest login. Anonymous connections are not available for SFTP sessions.</td>
</tr>
<tr>
<td></td>
<td>(there is no default value)</td>
<td></td>
</tr>
<tr>
<td>FULL-TO-HALF-FROM-SERVER</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td></td>
<td>(Default: NO)</td>
<td></td>
</tr>
<tr>
<td>HALF-TO-FULL-TO-SERVER</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td></td>
<td>(Default: NO)</td>
<td></td>
</tr>
<tr>
<td>SET Parameter</td>
<td>Values</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ISO7-TO-ROMAN8</td>
<td>YES</td>
<td>NO (Default: NO)</td>
</tr>
<tr>
<td>KANJI-AUTO-DETECT</td>
<td>YES</td>
<td>NO (Default: NO)</td>
</tr>
<tr>
<td>MCS-TO-NRC</td>
<td>YES</td>
<td>NO (Default: NO)</td>
</tr>
<tr>
<td>NATIONAL-REPLACEMENT-SET</td>
<td>&lt;value&gt;</td>
<td>(Default: USASCII)</td>
</tr>
<tr>
<td>NRC-TO-MCS</td>
<td>YES</td>
<td>NO (Default: NO)</td>
</tr>
<tr>
<td>PASSIVE</td>
<td>YES</td>
<td>NO (Default: YES)</td>
</tr>
<tr>
<td>PASSTHROUGH-AUTHENTICATION</td>
<td>YES</td>
<td>NO (Default: NO)</td>
</tr>
<tr>
<td>SET Parameter</td>
<td>Values</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>PASSTHROUGH-</td>
<td>&lt;string&gt; (there is no default value)</td>
<td>You must be connected to a site to change this global passthrough server property. This setting specifies your password on the passthrough server on your local network. For case-sensitive servers, you must use the appropriate case when you enter this value.</td>
</tr>
<tr>
<td>PASSWORD</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PASSTHROUGH-</td>
<td>&lt;value&gt;</td>
<td>You must be connected to a site to change this global passthrough server property. The FTP Client sends different commands to log into the passthrough server and connect to an FTP server, based on the style of server (page 750) you specify.</td>
</tr>
<tr>
<td>SERVER-STYLE</td>
<td>(Default: SITE-SERVERNAME)</td>
<td></td>
</tr>
<tr>
<td>PASSTHROUGH-</td>
<td>&lt;string&gt; (there is no default value)</td>
<td>You must be connected to a site to change this global passthrough server property. This setting specifies the name of the passthrough server on the local network that you use to log on to an FTP server.</td>
</tr>
<tr>
<td>SERVERNAME</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PASSTHROUGH-</td>
<td>&lt;string&gt; (there is no default value)</td>
<td>You must be connected to a site to change this global passthrough server property. Use this setting to specify a valid user name registered on the passthrough server for your local network. For case-sensitive servers, you must use the appropriate case when entering the PASSTHROUGH-USERNAME value.</td>
</tr>
<tr>
<td>USERNAME</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PASSWORD</td>
<td>&lt;string&gt; (there is no default value)</td>
<td>Specifies your password on the current FTP server.</td>
</tr>
<tr>
<td>PORT-NUMBER</td>
<td>0 - 65535</td>
<td>Specifies a non-standard TCP service port number or socket for FTP. The default value 0 (zero) directs the FTP Client to use the standard service port for FTP, which is 21. This setting does not apply to SFTP connections.</td>
</tr>
<tr>
<td>(Default: 0)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PRESERVE-FILE-</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td>DATE</td>
<td>(Default: NO)</td>
<td></td>
</tr>
<tr>
<td>PROXY-SERVER</td>
<td>&lt;value&gt;</td>
<td>This is a read-only parameter that indicates whether the FTP Client connects to this site using a passthrough server or SOCKS proxy server. The possible values are PROXY SERVER and SOCKS PROXY.</td>
</tr>
<tr>
<td>QUIET-STATUS</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td></td>
<td>(Default: NO)</td>
<td></td>
</tr>
<tr>
<td>SET Parameter</td>
<td>Values</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>RESUME-PARTIAL-TRANSFERS</td>
<td>ALWAYS</td>
<td>NEVER</td>
</tr>
<tr>
<td>ROMAN8-TO-ISO7</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td>SAVE-PASSWORD</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td>SAVE-PASSTHROUGH-PASSWORD</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td>SERVER-HOME-DIRECTORY</td>
<td>&lt;string&gt;</td>
<td>Specifies the path to a home (default) directory for the FTP or SFTP site to which you are currently connected. When a connection to the FTP or SFTP site is opened, the server working directory is set automatically to the specified home path. If no value is specified, the user home directory is used.</td>
</tr>
<tr>
<td>SERVERNAME</td>
<td>&lt;string&gt;</td>
<td>(there is no default value)</td>
</tr>
<tr>
<td>SMART-ASCII-TYPES</td>
<td>&lt;string&gt;</td>
<td>(DEFAULT: txt,bat,htm,html,ini)</td>
</tr>
<tr>
<td>SMART-BINARY-TYPES</td>
<td>&lt;string&gt;</td>
<td>(DEFAULT: exe,gif,jpg,wav)</td>
</tr>
<tr>
<td>SET Parameter</td>
<td>Values</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SMART-TENEX-TYPES</td>
<td>&lt;string&gt; (there is no default value)</td>
<td>This global parameter specifies all the file extensions used to identify files that should be transferred using the Tenex (Local 8) transfer method when TRANSFER-METHOD is set to SMART. To specify a list of file extensions, separate each extension with a comma. For example: SET SMART-TENEX-TYPES edd,gol,mmd,lad</td>
</tr>
<tr>
<td>SMART-TYPE-DEFAULT</td>
<td>ASCII</td>
<td>This global parameter specifies a default transfer method to use when TRANSFER-METHOD is set to SMART and the source file has an extension that has not been defined as either SMART-ASCII-TYPE, SMART-BINARY-TYPE, or SMART-TENEX-TYPE. During file transfers, if the source file uses an extension that has not been associated with a file transfer method, Smart File Transfer uses the transfer method specified for SMART-TYPE-DEFAULT.</td>
</tr>
<tr>
<td></td>
<td>BINARY</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TENEX</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ASK USER</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(Default: ASK USER)</td>
<td></td>
</tr>
<tr>
<td>SPACES-PER-TAB</td>
<td>1-20</td>
<td>Applies to ASCII file transfers. Specifies the number of consecutive spaces that are converted to a single tab character (for SPACES-TO-TABS) or the number of spaces that a single tab character is converted into (for TABS-TO-SPACES). This setting does not apply to SFTP connections.</td>
</tr>
<tr>
<td></td>
<td>(Default: 8)</td>
<td></td>
</tr>
<tr>
<td>SPACES-TO-TABS</td>
<td>YES</td>
<td>Applies to ASCII file transfers from the host. When receiving ASCII files, you can replace consecutive spaces with tabs by setting this parameter to YES. The number of spaces that are converted to a single tab is controlled by the SPACES-PER-TAB parameter. This setting does not apply to SFTP connections.</td>
</tr>
<tr>
<td></td>
<td>NO</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(Default: NO)</td>
<td></td>
</tr>
<tr>
<td>TABS-TO-SPACES</td>
<td>YES</td>
<td>When set to YES, tab characters in local files are converted to space characters in server files during ASCII transfers to the server. The FTP Client replaces each tab character with the number of spaces necessary to fill out to the next tab stop, as specified by the SPACES-PER-TAB parameter. This setting does not apply to SFTP connections.</td>
</tr>
<tr>
<td></td>
<td>NO</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(Default: YES)</td>
<td></td>
</tr>
<tr>
<td>TIME-LOGGED-IN</td>
<td>(Read-only)</td>
<td>This is a read-only parameter that indicates the time when you logged into the server. The current time format specified in the International dialog box in the Windows Control Panel determines how time data displays.</td>
</tr>
<tr>
<td>TIME-SINCE-LOGIN</td>
<td>(Read-only)</td>
<td>This is a read-only parameter that indicates how long you have been logged into the server. The current time format specified in the International dialog box in the Windows Control Panel determines how time data displays.</td>
</tr>
<tr>
<td>TIMEOUT-CONNECT</td>
<td>0 - 65535</td>
<td>Specifies how long (in seconds) the client should continue trying to establish a server connection before it gives up. Setting this parameter to 0 (zero) prevents the FTP Client from ever timing out on a connection attempt. This setting does not apply to SFTP connections.</td>
</tr>
<tr>
<td></td>
<td>(Default: 120)</td>
<td></td>
</tr>
<tr>
<td>SET Parameter</td>
<td>Values</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>TIMEOUT- SESSION</td>
<td>0 - 65535 (Default: 120)</td>
<td>Specifies the maximum number of seconds to wait for data packets being transferred to or from the host. If nothing is received within the period specified, a timeout error displays and the transfer is aborted. Setting this parameter to 0 (zero) prevents the FTP Client from ever timing out when waiting for a response. This setting does not apply to SFTP connections.</td>
</tr>
<tr>
<td>TRANSFER-8.3- CASE</td>
<td>LOWER</td>
<td>UPPER</td>
</tr>
<tr>
<td>TRANSFER-DISPOSITION</td>
<td>&lt;value&gt; (Default: OVERWRITE)</td>
<td>This global parameter specifies a file transfer mode that tells the client what to do if the client or server file being transferred already exists at the destination. The possible values are APPEND, PROMPT, CANCEL, OVERWRITE, SKIP, UPDATE, UNIQUE. UPDATE directs the client to overwrite the destination file only if the file being transferred is newer than the destination file. UNIQUE directs the client to create a new unique name.</td>
</tr>
<tr>
<td>TRANSFER- ELAPSED- TIME</td>
<td>(Read-only)</td>
<td>This is a read-only parameter that indicates how long the last completed file transfer took to complete. The current time format specified in the International dialog box in the Windows Control Panel determines how time data displays.</td>
</tr>
<tr>
<td>TRANSFER-METHOD</td>
<td>&lt;value&gt; (Default: SMART)</td>
<td>This global parameter specifies the file transfer method for the client. The possible values are ASCII, BINARY, TENEX, SMART.</td>
</tr>
<tr>
<td>TRANSFER- SPEED</td>
<td>(Read-only)</td>
<td>This is a read-only parameter that indicates the speed of the last completed file transfer. This value represents the number of kilobytes transferred per second.</td>
</tr>
<tr>
<td>TRANSLATE- DIRECTORY- LISTING</td>
<td>YES</td>
<td>NO (Default: NO)</td>
</tr>
</tbody>
</table>
SET Parameters and Equivalent Interface Settings

SET parameters are for use with the “SET” on page 868 command. This table lists equivalent settings in the FTP Client user interface.

<table>
<thead>
<tr>
<th>SET Parameter</th>
<th>Equivalent Interface Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>TRANSLATE-FILES</td>
<td>ABORT-ON-ERROR-No equivalent dialog box setting</td>
</tr>
<tr>
<td>USE-PASSTHROUGH-SERVER</td>
<td>ACCOUNT Option on Connection tab in Site Properties dialog box</td>
</tr>
<tr>
<td>USE-SOCKS</td>
<td>ANONYMOUS Option on General tab in Site Properties dialog box</td>
</tr>
<tr>
<td>USERNAME</td>
<td>ASCII-CLIENT-TYPE Client character set in Character Sets dialog box</td>
</tr>
<tr>
<td>WRITE-CTRLZ</td>
<td>ASCII-SERVER-TYPE Server character set in Character Sets dialog box</td>
</tr>
<tr>
<td></td>
<td>AUTO-SERVER-UPDATE Refresh directory automatically check box on the Directories tab in the Site Properties dialog box</td>
</tr>
<tr>
<td></td>
<td>CLIENT-HOME-DIRECTORY Local Home folder box on the Directories tab in the Site Properties dialog box</td>
</tr>
</tbody>
</table>

**SET Parameter Values Description**

**TRANSLATE-FILES**
YES | NO (Default: NO)
Specifies whether to enable translation of ASCII files. When set to YES, character translations occur between the client and the server when a PC file is sent to the server, and when characters sent from the server are written to a client file. Setting this parameter to YES enables the following SET parameters: SET ASCII-CLIENT-TYPE, SET ASCII-SERVER-TYPE, SET NATIONAL-REPLACEMENT, SET ISO7-TO-ROMAN8, SET ROMAN8-TO-ISO7, SET NRC-TO-MCS, and SET MCS-TO-NRC.

This setting does not apply to SFTP connections.

**USE-PASSTHROUGH-SERVER**
YES | NO (Default: NO)
Specifies whether to connect through a passthrough server when opening connections to the current FTP site. When set to YES, the FTP Client uses the following global settings to make the connection to the passthrough server: PASSTHROUGH-SERVER-STYLE, PASSTHROUGH-SERVERNAME, PASSTHROUGH-USERNAME, PASSTHROUGH-PASSWORD, and PASSTHROUGH-AUTHENTICATION.

**USE-SOCKS**
YES | NO (Default: NO)
Specifies whether you want to use a SOCKS proxy server for connections made to the current site. When set to YES, the FTP Client uses a SOCKS proxy server.

**USERNAME**
<string> (there is no default value)
Specifies a valid user name registered on the current server. For case-sensitive servers, you must use the appropriate case when entering the USERNAME value.

**WRITE-CTRLZ**
YES | NO (Default: NO)
Applies to ASCII file transfers from the server. When set to YES, the FTP Client automatically adds an end-of-file marker (^Z) at the end of a received ASCII file.
<table>
<thead>
<tr>
<th>SET Parameter</th>
<th>Equivalent Interface Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONFIRM-DELETE</td>
<td>Confirm file delete check box on the Preferences tab in the Options dialog box</td>
</tr>
<tr>
<td>CREATE-SERVER-UPPER</td>
<td>Set case of 8.3 file names list box on the Transfer tab in the Site Properties dialog box</td>
</tr>
<tr>
<td>CREATE-8.3-FILENAMES</td>
<td>Create Windows file names in 8.3 format check box on the Transfer tab in the Site Properties dialog box</td>
</tr>
<tr>
<td>CTRL-Z-EOF</td>
<td>Read Ctrl-Z as end of file under To server in the Translation tab Site Properties dialog box</td>
</tr>
<tr>
<td>DELETE-TRAILING-SPACES</td>
<td>Delete trailing spaces check box on the Translation tab in Site Properties dialog box</td>
</tr>
<tr>
<td>EMAIL-ADDRESS</td>
<td>Anonymous password box on the General tab in the Options dialog box</td>
</tr>
<tr>
<td>FULL-TO-HALF-FROM-SERVER</td>
<td>Full- to half-width Katakana check box in Character Sets dialog box</td>
</tr>
<tr>
<td>HALF-TO-FULL-TO-SERVER</td>
<td>Half- to full-width Katakana check box in Character Sets dialog box</td>
</tr>
<tr>
<td>ISO7-TO-ROMAN8</td>
<td>Change ISO-7 to Roman-8 check box in Character Sets dialog box</td>
</tr>
<tr>
<td>KANJI-AUTO-DETECT</td>
<td>Detect server Kanji type check box in Character Sets dialog box</td>
</tr>
<tr>
<td>MCS-TO-NRC</td>
<td>Change MCS to NRC check box in Character Sets dialog box</td>
</tr>
<tr>
<td>NATIONAL-REPLACEMENT-SET</td>
<td>ISO-7/NRC set in Character Sets dialog box</td>
</tr>
<tr>
<td>NRC-TO-MCS</td>
<td>Change NRC to MCS check box in Character Sets dialog box</td>
</tr>
<tr>
<td>PASSIVE</td>
<td>Use passive mode check box on Connection tab in the Site Properties dialog box</td>
</tr>
<tr>
<td>PASSTHROUGH-AUTHENTICATION</td>
<td>Use Firewall check box on the Firewall tab in the Security Properties dialog box</td>
</tr>
<tr>
<td>PASSTHROUGH-SERVERNAME</td>
<td>Server name box on the Firewall tab in the Security Properties dialog box</td>
</tr>
<tr>
<td>PASSTHROUGH-USERNAME</td>
<td>User name box on the Firewall tab in the Security Properties dialog box</td>
</tr>
<tr>
<td>PASSWORD</td>
<td>Password box on General tab in the Site Properties dialog box</td>
</tr>
<tr>
<td>PORT-NUMBER</td>
<td>TCP port box on Connection tab in the Site Properties dialog box</td>
</tr>
<tr>
<td>PRESERVE-FILE-DATE</td>
<td>Preserve server file date check box on the Transfer tab in the Site Properties dialog box.</td>
</tr>
<tr>
<td>PROXY-SERVER</td>
<td>Read-only value based firewall and SOCKS configuration in the Security Properties dialog box.</td>
</tr>
<tr>
<td>QUIET-STATUS</td>
<td>Hide progress window check box on the Preferences tab in the Options dialog box</td>
</tr>
<tr>
<td>ROMAN8-TO-ISO7</td>
<td>Change Roman-8 to ISO-7 check box in the Character Sets dialog box</td>
</tr>
<tr>
<td>SAVE-PASSWORD</td>
<td>Save password check box on the General tab in the Site Properties dialog box</td>
</tr>
<tr>
<td>SET Parameter</td>
<td>Equivalent Interface Setting</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SAVE-PASSTHROUGH-PASSWORD</td>
<td>Save password check box on the Firewall tab in the Security Properties dialog box</td>
</tr>
<tr>
<td>SERVER-HOME-DIRECTORY_SERVER_HOME_DIRECTORY</td>
<td>Server Home directory box on the Directories tab in the Site Properties dialog box</td>
</tr>
<tr>
<td>SERVERNAME_SERVERNAME</td>
<td>FTP address box on the General tab in the Site Properties dialog box</td>
</tr>
<tr>
<td>SMART-ASCII-TYPES</td>
<td>File transfer types on the File Types tab in the Options dialog box</td>
</tr>
<tr>
<td>SMART-BINARY-TYPES</td>
<td>File transfer types on the File Types tab in the Options dialog box</td>
</tr>
<tr>
<td>SMART-TENEX-TYPES</td>
<td>File transfer types on the File Types tab in the Options dialog box</td>
</tr>
<tr>
<td>SMART-TYPE-DEFAULT</td>
<td>Transfer method for undefined file types group box on the File Types tab in the Options dialog box</td>
</tr>
<tr>
<td>SPACES-PER-TAB</td>
<td>Spaces per tab box on Translation tab in the Site Properties dialog box</td>
</tr>
<tr>
<td>SPACES-TO-TABS</td>
<td>Change spaces to tabs check box on Translation tab in the Site Properties dialog box</td>
</tr>
<tr>
<td>TABS-TO-SPACES</td>
<td>Change tabs to spaces check box on Translation tab in the Site Properties dialog box</td>
</tr>
<tr>
<td>TIME-LOGGED-IN</td>
<td>Connected at on the Information tab in the Site Properties dialog box</td>
</tr>
<tr>
<td>TIME-SINCE-LOGIN</td>
<td>Connected for on the Information tab in the Site Properties dialog box</td>
</tr>
<tr>
<td>TIMEOUT-CONNECT</td>
<td>Connect box on the Connection tab in the Site Properties dialog box</td>
</tr>
<tr>
<td>TIMEOUT-SESSION</td>
<td>Session box on the Connection tab in the Site Properties dialog box</td>
</tr>
<tr>
<td>TRANSFER-8.3-CASE</td>
<td>Set case of 8.3 file names box under Upload to server options on the Transfer tab in the Site Properties dialog box</td>
</tr>
<tr>
<td>TRANSFER-DISPOSITION</td>
<td>If File Exists command on the Tools menu</td>
</tr>
<tr>
<td>TRANSFER-ELAPSED-TIME</td>
<td>Last transfer time on the Information tab in the Site Properties dialog box</td>
</tr>
<tr>
<td>TRANSFER-METHOD</td>
<td>Transfer Method command on the Tools menu</td>
</tr>
<tr>
<td>TRANSFER-SPEED</td>
<td>Last transfer rate on the Information tab in the Site Properties dialog box</td>
</tr>
<tr>
<td>TRANSLATE-FILES</td>
<td>Translate files check box in Character Sets dialog box</td>
</tr>
<tr>
<td>USE-PASSTHROUGH-SERVER</td>
<td>Controlled by firewall configuration in the Security Properties dialog box</td>
</tr>
<tr>
<td>USE-SOCKS</td>
<td>Controlled by SOCKS configuration in the Security Properties dialog box.</td>
</tr>
<tr>
<td>USERNAME</td>
<td>User box on General tab in the Site Properties dialog box</td>
</tr>
<tr>
<td>WRITE-CTRLZ</td>
<td>Write Ctrl-Z at end of file under From server on Translation tab in Site Properties dialog box</td>
</tr>
</tbody>
</table>
Site-Specific File Transfer SET Parameters

Advanced File Transfer SET Parameters

Transfer options when sending files to the server
- CREATE-SERVER-UPPER
- TRANSFER-8.3-CASE

Transfer options when receiving files from the server
- PRESERVE-FILE-DATE
- CREATE-8.3-FIENAMES

Character Translation SET Parameters for ASCII File Transfer

Character sets used for translations
- ASCII-CLIENT-TYPE
- ASCII-SERVER-TYPE
- NATIONAL-REPLACEMENT-SET

Translation options when sending files to the server
- MCS-TO-NRC
- ROMAN8-TO-ISO7

Translation options when receiving files from the server
- ISO7-TO-ROMAN8
- NRC-TO-MCS

ASCII-SERVER-TYPE SET Parameter Values

The ASCII-SERVER-TYPE SET parameter (page 845) <value> can be any of the following:

<table>
<thead>
<tr>
<th>Value</th>
<th>Value</th>
<th>Value</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEC-SUPPLEMENTAL</td>
<td>ISO-LATIN-2</td>
<td>BIG-5</td>
<td>DEC-Hebrew</td>
</tr>
<tr>
<td>ISO-LATIN-1</td>
<td>ISO-LATIN-5</td>
<td>CCDC</td>
<td>7-Bit-Hebrew</td>
</tr>
<tr>
<td>PC-ENGLISH</td>
<td>ISO-LATIN-6</td>
<td>GB-Chinese</td>
<td>DEC-Cyrillic</td>
</tr>
<tr>
<td>PC-MULTILINGUAL</td>
<td>ISO-LATIN-7</td>
<td>KS-5601-Korean</td>
<td>HP-Turkish</td>
</tr>
<tr>
<td>HP-ROMAN-8</td>
<td>ISO-LATIN-8</td>
<td>HP-Greek</td>
<td>DEC-Turkish</td>
</tr>
<tr>
<td>PC-SLAVIC</td>
<td>ISO-LATIN-9</td>
<td>DEC-Greek</td>
<td>PC-Spanish</td>
</tr>
<tr>
<td>PC-CYRILLIC-855</td>
<td>SHIFT-JIS</td>
<td>PC-Greek</td>
<td>PC-Turkish</td>
</tr>
<tr>
<td>PC-MODERN-TURKISH</td>
<td>JIS-X0208-1990</td>
<td>YUASCII</td>
<td>SBIG-5</td>
</tr>
<tr>
<td>PC-PORTUGUESE</td>
<td>JIS-X0208-1983</td>
<td>PC-Cyrilic</td>
<td>THAI-988-TISO</td>
</tr>
<tr>
<td>PC-ICELANDIC</td>
<td>JIS-C6226-1978</td>
<td>JIS-Katakana</td>
<td>THAI-TISO</td>
</tr>
<tr>
<td>PC-CANADIAN-FRENCH</td>
<td>DEC-1983-KANJI</td>
<td>NEC-N88</td>
<td>THAI-KU</td>
</tr>
<tr>
<td>PC-ARABIC</td>
<td>DEC-1978-KANJI</td>
<td>PC-Hebrew</td>
<td>THAI-PRIME</td>
</tr>
</tbody>
</table>
NATIONAL-REPLACEMENT-SET Parameter Values

The NATIONAL-REPLACEMENT-SET SET parameter (page 845) <value> can be any of the following:

ABORT-ON-ERROR Script Sample

This sample code sets ABORT-ON-ERROR (page 845) to NO before using “MGET” on page 837 and back to YES before using “MDEL” on page 836 or “PUT” on page 841.

SITE

Syntax: site <argument>

FTP Command Index (page 825)

The SITE command allows you to send a recognized SITE command to the server.

To find out what SITE commands are understood by the current FTP server, try entering this command at the FTP command line:

QUOTE help site
If the server supports the *QUOTE* command, it may respond with a list the *SITE* commands that are understood by the server. The server response displays in the command window.

```<argument>`
Specifies any *SITE* command that the FTP server understands.
```

**Examples**

The following command requests the idle timeout setting for the server:

```
SITE idle
```

The server response shows in the command window. For example:

```
200 Current IDLE time limit is 900 seconds; max 7200
```

This command sets the IDLE timeout to 1800 seconds:

```
SITE idle 1800
```

**SMART**

**Syntax:** `smart`

FTP Command Index (page 825)  SFTP Command Index (page 858)

The *SMART* command changes the current FTP file transfer method to Smart.

Use the Smart transfer method if you want the FTP Client to automatically determine what transfer method to use (ASCII, Binary, or Tenex) based on the type of file that is being transferred. The FTP Client uses the source file extension to determine what type of file is being transferred. To set up for Smart File Transfer, use settings on the *File Types* tab in the *Options* dialog box.

**SYSTEM**

**Syntax:** `system`

FTP Command Index (page 825)

The *SYSTEM* command displays information about the type of operating system used by the current FTP server. The information displays in the FTP command window.

For example, if you entered `SYSTEM` at the FTP command line, the display might look like this:

```
215 UNIX Type: L8
```

**TENEX**

**Syntax:** `tenex`

FTP Command Index (page 825)  SFTP Command Index (page 858)

The *TENEX* command changes the current file transfer method to "local 8." Use this transfer method if you're moving files to or from a server that uses a non-8-bit byte (such as the DECsystem-20).

**TYPE**

**Syntax:** `type <serverfile>`

FTP Command Index (page 825)

The *TYPE* command displays the contents of a server file in the FTP command window.
Example

The following command displays in the command window the file hardware.txt, which is located in the /Users/boris folder on the FTP server:

```
TYPE /Users/boris/hardware.txt
```

**VERIFY**

Syntax: `verify [commands] [set parameter] [changed]`

FTP Command Index (page 825)

The `VERIFY` command displays information about the values of one or more `SET` parameters (page 845). With no parameters, `VERIFY` displays the current value of all Reflection `SET` parameters.

```
<serverfile> Specifies the location and name of the server file. This specification cannot contain wildcards.

<set parameter> Displays the value of a particular `SET` parameter.
```

Examples

This command displays the current national replacement set setting:

```
VERIFY NATIONAL-REPLACEMENT-SET
```

This command creates a complete list of current `SET` parameter values:

```
VERIFY
```

**SFTP commands**

In this Section

- “ASCII” on page 859
- “BINARY” on page 859
- “BYE” on page 859
- “CD” on page 859
- “CHMOD” on page 860
- “EXIT” on page 860
- “GET” on page 860
- “LCD” on page 861
- “LLS” on page 861
- “LMKDIR” on page 862
- “LPWD” on page 862
- “LS” on page 862
- “MGET” on page 863
- “MKDIR” on page 864
ASCII

Syntax: ascii

FTP Command Index (page 825)   SFTP Command Index (page 858)

The ASCII command changes the current file transfer method to ASCII. Use this transfer method to move ASCII text files between the server and your PC.

BINARY

Syntax: binary

FTP Command Index (page 825)   SFTP Command Index (page 858)

The BINARY command changes the current file transfer method to binary (image). Use this transfer method to transfer binary files, such as .EXE files and compressed files, between two PCs (via a server), or between two servers (via a PC).

BYE

Syntax: bye

SFTP Command Index (page 858)

The BYE command closes the connection to the server.

This command is available for SFTP connections only.

CD

Syntax: cd <server directory>

FTP Command Index (page 825)   SFTP Command Index (page 858)

The CD command changes the working directory on the FTP server.

<server directory> Specifies a directory on the server.

Examples

This command changes to the directory "Asian Artists" on a UNIX system:
CD Asian Artists
This command changes directories on a VAX/VMS system:
CD SYS$USERS:[ARNOLD.DOCS]

CHMOD
Syntax: chmod <numeric permission mask> <server file or directory>
FTP Command Index (page 825)  SFTP Command Index (page 858)
The CHMOD command changes the permissions associated with a file or directory.

<numeric permission mask>  Specifies a three digit numeral that is a valid value for the UNIX chmod command. Valid values have digits from 0 to 7.
Tip: To determine what mask to use to set permissions, right click on a server file and select properties. The properties dialog box displays the three digit mask and the permissions associated with it. If you change the permissions, the mask value is updated automatically.

<server file or directory>  Specifies a file or directory on the FTP server. Follow the server's syntax for specifying file and directory names.

Example
This command sets attributes to -rw-r--r-- for the specified file.
chmod 644 myfile.htm

EXIT
Syntax: exit
FTP Command Index (page 825)  SFTP Command Index (page 858)
The EXIT command closes the connection to the server.

GET
Syntax: get <serverfile> [to] [<clientfile>] [append | askuser | cancel | overwrite | skip | unique]
FTP Command Index (page 825)  SFTP Command Index (page 858)
The GET command transfers a file from the server to the PC. Wildcards are not supported with the GET command—they are treated as ordinary characters and are assumed to be part of the file name. To transfer multiple files, use "MGET" on page 837.

Before using the GET command, if necessary, use the "ASCII" on page 859, "BINARY" on page 828, "TENEX" on page 868, or "SMART" on page 868 command to override the default file transfer method setting specified on the Tools menu.

A variety of site-specific SET parameters can affect the transfer operation. Click here (page 855) for more information.
Examples

The following example transfers the server file MEMO.DOC from the server to the PC, giving the PC file the same name:

GET MEMO.DOC

This example transfers the VAX/VMS FTP server file MORTGAGE.PAPERS to the PC, giving the PC file the name MORTGAGE.TXT:

GET MORTGAGE.PAPERS MORTGAGE.TXT

LCD

Syntax: lcd [<pc drive/folder> | ..]

The LCD command opens another folder on the PC.

If no <folder> is specified, LCD displays the path for the current PC folder.

To change folders, type the folder at the FTP command line, for example, type LCD F:\Documents and press Return.

<pc drive/folder> Specifies the drive (if other than the current drive) and folder to change to.

.. Specifies that you want to change to the parent folder.

Example

This command changes your current folder to the China folder within the Asian Travel folder on drive D:

LCD d:\Asian Travel\China

LLS

Syntax: lls [pc filespec]

The LLS command displays a listing of PC files matching the given filespec.

This command is available for SFTP connections only. The FTP equivalent is LDIR.

<pc filespec> Specifies a folder, a file, or a group of files on the PC. If this option is not used, the contents of the current PC folder are displayed.
Example
This command displays a listing of files in the current PC folder that have a .Doc extension:
LLS *.Doc

LMKDIR
Syntax: lmkdir <pc directory>
SFTP Command Index (page 858)
The LMKDIR command creates a folder on the PC.
This command is available for SFTP connections only. The FTP equivalent is LMD.

<pc folder> Specifies the drive where you want to create the folder (if other than the current drive) and the folder name.

Example
This command creates the folder Music on the current PC drive:
LMKDIR \Music

LPWD
Syntax: lpwd [<pc drive/folder> | ..]
SFTP Command Index (page 858)
The LPWD command opens another folder on the PC.
If no <folder> is specified, LPWD displays the path for the current PC folder.
To change folders, type the folder at the FTP command line, for example, type LPWD F:\Documents and press Return.
This command is available for SFTP connections only. The FTP equivalent is LCD.

<pc drive/folder> Specifies the drive (if other than the current drive) and folder to change to.
.. Specifies that you want to change to the parent folder.

Example
This command changes your current folder to the China folder within the Asian Travel folder on drive D:
LPWD d:\Asian Travel\China

LS
Syntax: ls [<server filespec>]
FTP Command Index (page 825) SFTP Command Index (page 858)
The LS command displays a simple listing of server files matching the given filespec. (Compare this to the "DIR" on page 831 command, which displays a more detailed listing.)
Example

In this example, the names of all files in the current folder on a UNIX FTP server are listed:

```
LS *.*
```

### MGET

**Syntax:** `mget <server filespec> [to] [<pc filespec>] [append | askuser | cancel | overwrite | skip | unique]`

The `MGET` command transfers one or more files matching the given filespec from the FTP server to the PC. You can use wildcards to transfer multiple files. Most servers support wildcards in the `<serverspec>`. However, if your server doesn’t support wildcards in an “LS” on page 862 command, using `MGET` with a wildcard specification may result in a transfer of all files in the current directory.

**NOTE:** The Reflection client supports `MGET` in SFTP sessions, however you should test transfers that use wildcard characters because the SFTP server may not interpret wildcard specifications correctly.

Before using the `MGET` command, if necessary, use the “ASCII” on page 859, “BINARY” on page 828, “TENEX” on page 868, or “SMART” on page 868 command to override the default file transfer method setting specified on the Tools menu.

A variety of site-specific `SET` parameters can affect the transfer operation. Click here (page 855) for more information.

#### Examples

This example transfers all files with a .Doc extension from the FTP server to the PC, placing the files in the current PC directory:

```
MGET *.* "C:\My documents\*.doc"
```
**MGET**

*MGET *.*.Doc*

This example adds the letter A to the transferred files. For example, test.txt becomes Atest.txt.

*MGET *.* A*.*

See “ABORT-ON-ERROR Script Sample” on page 856 for an additional example.

**MKDIR**

**Syntax:** mkdir <server folder>

SFTP Command Index (page 858)

The **MKDIR** command creates a folder on the server.

This command is available for SFTP connections only. The FTP equivalent is **MD**.

<server folder> Specifies the name and location of the new folder.

**Example**

This command creates the folder Films within the current folder on the current FTP UNIX server drive:

MKDIR Films

**MPUT**

**Syntax:** mput <pc filespec> [to] [<server filespec>] [append | askuser | cancel | overwrite | skip | unique]

FTP Command Index (page 825)       SFTP Command Index (page 858)

The **MPUT** command transfers one or more files matching the given filespec from the PC to the FTP server. You can use wildcards to transfer multiple files.

**NOTE:** The Reflection client supports **MPUT** in SFTP sessions, however you should test transfers that use wildcard characters because the SFTP server may not interpret wildcard specifications correctly.

Before using the **MPUT** command, if necessary, use the “ASCII” on page 859, “BINARY” on page 828, “TENEX” on page 868, or “SMART” on page 868 command to override the default file transfer method setting specified on the **Tools** menu.

A variety of site-specific **SET** parameters can affect the transfer operation. Click here (page 855) for more information.
File and Data Transfer

**Examples**

The following example transfers files in the Meeting Notes folder within the current folder on the PC that have a .Doc extension, placing the files in the current server folder. Source PC files that have the same name as files in the destination server folder are not transferred.

```plaintext
MPUT "Meeting Notes\*.Doc" skip
```

The following example adds the letter "A" to the front of files transferred to the server. For example, `Sample.htm` becomes `ASample.htm`.

```plaintext
MPUT *.htm A*.htm
```

The final example removes file extensions from PC files copied to the server:

```plaintext
MPUT *.* *.
```

**PROGRESS**

**Syntax:** `progress`

SFTP Command Index (page 858)

Toggles the display of the progress meter.

This command is available for SFTP connections only.

**PUT**

**Syntax:** `put <clientfile> [to] [<serverfile>] [append | askuser | cancel | overwrite | skip | unique]`

FTP Command Index (page 825)  SFTP Command Index (page 858)

The **PUT** command transfers a file from the PC to the server.

Wildcards are not supported with the **PUT** command; to transfer multiple files using wildcards, use "MPUT" on page 838.
Before using the **PUT** command, if necessary, use the “ASCII” on page 859, “BINARY” on page 828, “TENEX” on page 868, or “SMART” on page 868 command to override the default file transfer method setting specified on the **Tools** menu.

A variety of site-specific **SET** parameters can affect the transfer operation. Click here (page 855) for more information.

```plaintext
<clientfile>             Specifies the name of the PC file. Use quotation marks if the file or path includes spaces.
to <serverfile>         Specifies the name of the server file to be created. If the server file name is omitted, the server file is given the same name as the PC file. The TO keyword is optional.
append | askuser | cancel | overwrite | skip | unique                  Specifies what to do if the destination file already exists. If this option is omitted, the active **TRANSFER-DISPOSITION** (page 845) setting is the default.
```

**Examples**

The following example transfers the file Memo.doc from the PC to the server:

**PUT** Memo.doc

This example transfers the file HAPPY.ME from a PC to a VAX/VMS FTP server, giving the VMS file the name HAPPY.BIRTHDAY:

**PUT** HAPPY.ME TO HAPPY.BIRTHDAY

See “**ABORT-ON-ERROR Script Sample**” on page 856 for an additional example.

**PWD**

**Syntax:** `pwd`

**FTP Command Index (page 825)**  **SFTP Command Index (page 858)**

The **PWD** command shows the server folder that is currently open. The name and location of the folder display in the FTP command window.

**QUIT**

**Syntax:** `quit`

**FTP Command Index (page 825)**  **SFTP Command Index (page 858)**

The **QUIT** command closes the connection to the server.

**NOTE:** When you run a script from the Windows command line using the `/RFS` switch and the script ends in with a **QUIT** command, the FTP client shuts down automatically when the script is complete.

**RENAME**

**Syntax:** `rename <server filename> <new filename>`

**FTP Command Index (page 825)**  **SFTP Command Index (page 858)**
The **RENAME** command changes the name of a server file to the new name specified. On some servers, you can use **RENAME** to specify both a new name and a new location for the file. In this case, the file is moved to the new location and given the new name specified.

<server filename> Specifies the name of the server file you want to rename. The specification can include the name of the server folder where the file is located. Use quotation marks if the file or path includes spaces. For example: "/Maps/North America".

=new filename> Specifies the name you want to give the file. Use quotation marks if the file or path includes spaces. For example:

"D:\To do\Work assignments".

On some servers, if you omit the path to the file you are renaming, the file is moved to the current server folder and given the new name. If you want to use **RENAME** to move a file, specify a new location and file name.

**Example**

In the current folder on the server, this command renames the file "Map of Canada" to "Canada":

```
RENAME "Map of Canada" Canada
```

From the "Maps" folder on the server, this command renames a file in the folder "Europe", changing the name from "England" to "Great Britain".

```
RENAME /Maps/Europe/England "/Maps/Europe/Great Britain"
```

**RM**

**Syntax:** rm <serverfile>

*SFTP Command Index (page 858)*

The **RM** command deletes a file matching the given filespec on the SFTP server.

This command is available for SFTP connections only. The FTP equivalent is **DELETE**.

**NOTE:** If the **SET** parameter (page 845) **CONFIRM-DELETE** is set to YES, the user is prompted for confirmation before deleting.

<serverfile> Specifies the name of a server file to delete. This can include a full directory path to the file. On some systems case is important when specifying directories and file names.

**Example**

This command deletes MEMO.DOC from the current server directory:

```
RM MEMO.DOC
```

**RMDIR**

**Syntax:** rmdir <server folder>

*SFTP Command Index (page 858)*

The **RMDIR** command deletes an empty folder on the server.
This command is available for SFTP connections only.

**NOTE:** If the **SET** parameter (page 845) **CONFIRM-DELETE** is set to YES, the user is prompted for confirmation before deleting.

<server folder> Specifies the location and name of the folder you want to delete. The <server folder> specification must follow the conventions of the server operating system. Before you can delete a folder, you must delete the files and folders within it.

**Example**

This command deletes the folder Articles from the current server folder:

RMDIR Articles

**SET**

**Syntax:** set <set parameter> <value>

Use the **SET** command to configure Reflection. See the **SET Parameters** (page 845) for a list of available options.

**Examples**

These commands initialize various file transfer parameters:

SET TABS-TO-SPACES NO
SET TRANSFER-DISPOSITION Overwrite
SET TRANSFER-METHOD Ascii
SET TRANSLATE-FILES NO

**Related Topics**

- “**SET Parameter Reference**” on page 845
- “**SET Parameters and Equivalent Interface Settings**” on page 852
- “Site-Specific File Transfer SET Parameters” on page 855

**SMART**

**Syntax:** smart

The **SMART** command changes the current FTP file transfer method to Smart.

Use the Smart transfer method if you want the FTP Client to automatically determine what transfer method to use (ASCII, Binary, or Tenex) based on the type of file that is being transferred. The FTP Client uses the source file extension to determine what type of file is being transferred. To set up for Smart File Transfer, use settings on the **File Types** tab in the **Options** dialog box.

**TENEX**

**Syntax:** tenex
The **TENEX** command changes the current file transfer method to "local 8." Use this transfer method if you're moving files to or from a server that uses a non-8-bit byte (such as the DECsystem-20).
Creating and Using Macros

In InfoConnect, you can create and run Visual Basic for Applications (VBA) macros to simplify and automate routine tasks. You can create these macros two ways:

- Click **Record Macro**, perform the tasks you want to automate, and then save the recorded steps in a macro.
  
  Use this method to create simple macros that automate interaction with host applications. (You cannot record interaction with Web applications or interaction with InfoConnect settings.)

- Open the Visual Basic Editor and type in the commands for the macro.
  
  Use this method to create complex macros that perform InfoConnect actions and interact with other applications.

A common approach for creating a macro is to record it and then fine-tune it using the Visual Basic Editor. For more information about editing and programming macros, see the InfoConnect VBA Guide (Help > VBA Guide).

In this Chapter

- “Run a Macro” on page 871
- “Create a Macro in the Visual Basic Editor” on page 873
- “Record a Macro” on page 874
- “Edit a Macro” on page 875
- “Run a Startup Macro” on page 875
- “Set up Macros that run before or after a host connection” on page 876
- “Naming Macros” on page 877
- “Recording Complete Dialog Box” on page 878
- “Using Legacy Macros” on page 878

Run a Macro

Index Term
Primary: running
Secondary: macros
You can run VBA macros created in InfoConnect, and most macros created with legacy Reflection and EXTRA! products. You can also run the majority of macros created with the Micro Focus RUMBA, IBM Personal Communications, OpenText HostExplorer, and Brandon Systems/Jolly Giant QWS3270 products. However, you can only run macros in trusted locations.

Several macro-related actions (such as, Run a Reflection Workspace Macro) are available from the Select Action dialog box.

You can also run a macro by mapping an action to a control. For more information, see “Add a Button to Run a Macro” on page 76.

To run a macro

1 Open the Run Macro dialog box.
   1a The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reflection Ribbon</td>
<td>On the Session ribbon, from the Macros group, click Run Macro.</td>
</tr>
<tr>
<td>Reflection Browser</td>
<td>On the Reflection menu, choose Tools, Macro and then Run Macro.</td>
</tr>
<tr>
<td>TouchUx</td>
<td>Tap the Wrench icon and then under Macro, select Show Run Macro Dialog.</td>
</tr>
</tbody>
</table>

2 From the Run Macro dialog box, select the macro you want to run.

**NOTE:** Legacy macro options are available only if compatibility features are installed. In addition, to run legacy Reflection and EXTRA! macros from external files, you must specify, from the Set Up API and Macro Security dialog box, the type of legacy macro you want to run.

<table>
<thead>
<tr>
<th>Reflection Workspace Macro</th>
<th>Shows macros in the active session document. Select to run macros created in InfoConnect or 2007 (SP1) documents.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>To run a macro in the Common project and other documents, select one of the following options from the Macros in menu:</td>
</tr>
<tr>
<td>Select</td>
<td>To show macros in</td>
</tr>
<tr>
<td>&lt;All Standard&gt;</td>
<td>All open projects and session documents.</td>
</tr>
<tr>
<td>Common</td>
<td>The Common project.</td>
</tr>
<tr>
<td>Project [ &gt; filename ]</td>
<td>The active session document only.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Legacy Reflection Macro in This File</th>
<th>Select to run legacy macros in the active document. These macros include legacy settings files (.rsf, .r2w, or .r4w), and in InfoConnect, session documents (.rd3x, .rd5x, .rdox) that were previously converted from settings files.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Legacy Reflection Macro in Another File</th>
<th>Select to specify and run a macro in a SharedMacro file (.rma) or a settings file (.rsf, .r2w, or .r4w).</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Legacy RB Macro</th>
<th>Select to specify and run a Reflection Basic macro (.rbs).</th>
</tr>
</thead>
</table>

872 InfoConnect 2014 User’s Guide
Creating and Using Macros

Creating and Using Macros

Create a Macro in the Visual Basic Editor

Whenever possible, create macros in Modules. Doing so will add to the integrity and stability of your program. The exception to this rule is event procedures, which are added directly to Reflection objects.

To create a macro in the Visual Basic Editor

1. In InfoConnect, open a session document.
2. Open the Visual Basic Editor.

   The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reflection Ribbon</td>
<td>From the Tools ribbon, click Visual Basic.</td>
</tr>
<tr>
<td>Reflection Browser</td>
<td>On the Reflection menu, choose Tools, Macro and then Visual Basic.</td>
</tr>
<tr>
<td>TouchUx</td>
<td>Tap the Wrench icon and then under Macro, select Visual Basic.</td>
</tr>
</tbody>
</table>

   The session document appears as a project in the Project Explorer; for example, Project (My Session.rd3x).

3. In the Project Explorer, select the project in which you want save the macro, and then choose Insert > Module to create a new module.

4. Double-click the module you created.

   The Code window opens.

5. Choose Insert > Procedure, type a name in the Name box, and then click OK.

   The name you choose must follow the Visual Basic naming conventions for macros. For further information, see "Naming Macros" on page 877.

6. Type code for your macro between the Sub (or Public Sub) and End Sub statements.

   Context-sensitive Help is available for Visual Basic commands. Position the insertion point within a command and press F1.
Record a Macro

Index Term
Primary: recording macros

You can record a macro to automate your interaction with host applications, including:

- Sending data to, or typing text in, a host application.
- Cutting, copying, or pasting text or data from one host application to another.
- Switching tabs to move from one host application to another.

You cannot record:

- Interaction with InfoConnect settings and Productivity features (such as Spell Check, Auto Expand, and Auto Complete).
- Connecting to or disconnecting from a host.
- Interaction with Web applications.
- Cutting or pasting from a host to an external application (for example, Notepad).

To record a macro

1 Select Record Macro.
   The steps depend on your user interface mode (page 120).

   User Interface Mode | Steps
   Ribbon              | On the Tools ribbon, from the Macros group, click Record Macro.
   InfoConnect Browser| On the InfoConnect menu, choose Tools, Macro and then Record Macro.
   TouchUx             | Tap the Wrench icon, and then under Macro, select Record Macro.

2 Perform the task(s) that you want to automate.
3 (Optional) If you need to interrupt the recording to perform another task, click Pause Recording. When you are ready to resume recording, click Pause Recording again.
4 When you are finished recording the macro, click Stop Recording.
   The Recording Complete dialog box appears.
5 Name the macro, choose the location where you want to save it, and then click OK.

NOTE: You can fine-tune recorded macros by using the Visual Basic Editor. For more information, see Edit a Macro. (page 875)

Related Topics

- “Naming Macros” on page 877
- “Edit a Macro” on page 875
- “Recording Complete Dialog Box” on page 878
Edit a Macro

Use the Visual Basic Editor to edit Reflection macros.

To edit a macro

1. Open the Visual Basic Editor.
   The steps depend on your user interface mode (page 120).
   - Reflection Ribbon: From the Tools ribbon, click Visual Basic.
   - Reflection Browser: On the Reflection menu, choose Tools, Macro and then Visual Basic.
   - TouchUx: Tap the Wrench icon and then under Macro, select Visual Basic.

   The Macros dialog box appears.

2. In the Macro name box, select the name of the macro to edit and click Edit.
3. In the Visual Basic Editor, type in or edit the macro commands.
4. From the File menu, choose Save.

Related Topics
- “Editing Legacy Reflection Macros <User Guide>” on page 880
- “Editing Legacy EXTRA! Macros” on page 884

Run a Startup Macro

You can set up a Visual Basic for Applications (VBA) macro to run when a InfoConnect workspace starts, rather than when a session opens and connects to the host.

This allows you to gather information about how users will connect and then use that information to configure session settings.

For example, you can create a startup macro to perform tasks such as:
- displaying a VBA UserForm to gather information from the user before connecting to the host
- reading from an .ini file
- checking for host or router availability
- configuring InfoConnect settings
**CAUTION:** You can configure only macros in the Common project to run when the workspace starts. Do not configure the “Run Reflection Workspace Macro” action to run a macro present in a session document (rd0x, rd3x, rd5x). This prevents InfoConnect from starting properly.

To set up a startup macro

1. Open the **InfoConnect Workspace Settings** dialog box. The steps depend on your **user interface mode** (page 120).

   **User Interface Mode** | **Steps** |
   -------------------- | ---------- |
   Ribbon (Office 2007)  | On the Reflection button , choose **Reflection Workspace Settings**. |
   Ribbon (Office 2010)  | On the **File** menu, choose **Reflection Workspace Settings**. |
   Reflection Browser    | On the Reflection menu, choose **Settings** and then **Reflection Workspace Settings**. |
   TouchUx               | Tap the Gear icon and then select **Reflection Workspace Settings**. |

2. Under **Workspace Settings**, click **Configure Workspace Settings**.
3. Under **Workspace and Documents**, in the **When starting workspace** list, select **Run Startup action**.
4. Click **Select Action**.
5. Under **Action**, select **Run Reflection Workspace Macro**.
6. Under **Action parameters**, choose **Select macro**.
7. In the **Select a macro** box, select the macro you want to run when InfoConnect starts.

**Related Topics**

- “Creating and Using Macros” on page 871
- “Run a Macro” on page 871
- “Set Up a Workspace Startup Action Sequence” on page 176

**Set up Macros that run before or after a host connection**

If you have created a macro for your session or workspace, you can set up the session to run a connection macro.

To set up a connection macro

1. Open the **Document Settings** dialog box. The steps depend on your **user interface mode** (page 120).
On the Settings… dialog box, do one of the following

- (VT) click Configure Connection Settings.
- (3270 or 5250), click Configure Advanced Connection Settings.

3 Under Connection Action, select whether to run the macro before or after the initial connection.

4 Click Select Action and select the macro to run.

### Naming Macros

Observe the following rules when you name Visual Basic macros (including procedures, constants, variables, and arguments):

- Use a letter as the first character. (Names aren't case sensitive, but they preserve capitalization.)
- Use only alphanumeric characters and the underscore character ( _ ). Spaces and other symbols are not allowed.
- Use fewer than 255 characters.
- Avoid names that match Visual Basic or Reflection commands. Or, if you do use a macro name that is the same as a command, fully qualify the command when you want to use it. (To do this, you need to precede the command name with the name of the associated type library. For example, if you had a macro named Beep, you could only invoke the Visual Basic `Beep` statement using VBA.`Beep`.)
- Give unique names to macros within a single module. Visual Basic doesn't allow you to have two macros with the same name in the same code module. However, you can have two macros with the same name if they are in different code modules. For example, although you could not have two macros named StartUp in the same code module, you could have two macros named StartUp if they were in different code modules. To call a macro with a duplicate name that is in another code module, you must fully qualify the macro name. (For example, Module1.StartUp invokes the StartUp macro in Module1.)
Recording Complete Dialog Box

The Recording Complete dialog box automatically appears after you stop recording a macro. From this dialog box, you can name and save the actions you've recorded as a Reflection Workspace macro.

<table>
<thead>
<tr>
<th>Save in the current document's project</th>
<th>Saves the macro in the current session document, which must be opened each time you want to run the macro.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save in the common project</td>
<td>Saves the macro in the Common project, which can be accessed from any session document on the local computer.</td>
</tr>
<tr>
<td>Macro name</td>
<td>Specify a unique name with no spaces. For other tips on naming Visual Basic macros, see “Naming Macros” on page 877. The name you specify appears after the module name in the Run Macro dialog box when you select a macro to run. For example, recorded macros are saved as “Recorded.Macroname.”</td>
</tr>
<tr>
<td>Copy script to clipboard</td>
<td>Saves the macro to the system clipboard, which allows you to paste it in a text file or another application.</td>
</tr>
</tbody>
</table>

Using Legacy Macros

Index Term
Primary: legacy
Secondary: macro support, see also macros

In InfoConnect, you can run VBA macros created in InfoConnect, and most macros created with legacy Reflection and EXTRA! products. You can also run the majority of macros created with the Micro Focus RUMBA, IBM Personal Communications, OpenText HostExplorer, and Brandon Systems/Jolly Giant QWS3270 products.

In addition, you can edit and debug legacy Reflection macros. InfoConnect provides tools for editing EXTRA! Basic and Reflection Basic macros.

For more information, see the InfoConnect Administrator's Reference.

In this Section
- “Legacy Reflection Macros” on page 878
- “Legacy EXTRA! Macros” on page 883
- “RUMBA Macros” on page 884
- “IBM Personal Communications Macros” on page 885
- “Brandon Systems/Jolly Giant QWS3270 Macros” on page 885
- “Hummingbird Basic Macros” on page 886

Legacy Reflection Macros

Index Term
Primary: Reflection, previous versions
Secondary: macro support
InfoConnect supports the following macro file formats:

- Settings files (.rsf,.r2w,.r4w)
- SharedMacros (.rma)
- Reflection Basic scripts (.rbs)
- Reflection Command Line scripts (.rcl)

You can open a settings file in the workspace, or run legacy macros as an external file. You can only run RCL scripts when a VT session document is active in the workspace.

To run a legacy Reflection macro

1. (Recommended) If your legacy macro was created in Reflection 10.x or earlier, save it in Reflection 14.x.

2. Open Workspace Settings.
   
   The steps depend on your user interface mode (page 120).


4. From the Legacy API preference menu, select Reflection, and then click OK.

5. On the Session ribbon, click the Run Macro button.

6. From the Run Macro dialog box, specify the legacy macro that you want to run.

**NOTE:** If the macro contains unsupported objects, its functionality may be limited or it may not run. For a list of unsupported objects and methods, see the InfoConnect VBA Guide (Help > VBA Guide). If your legacy macros use early binding, and if they return compiling errors when you run them, change their Reflection namespace references from Reflection to ReflectionCOM.
Related Topics

- “Run a Macro” on page 871

Adding Macro Data

Index Term
Primary: macros
Secondary: adding data

Index Term
Primary: adding
Secondary: macro data

If you want to enter macro data each time you run a legacy Reflection macro, you can run the legacy macro from an external file by clicking the **Run Macro** button on the Ribbon, and then selecting **Legacy Reflection Macro in Another File**.

Or, you can set up an action to run legacy macros in sessions that are currently open in the workspace. To do this, create a control (such as a button or a keystroke) and associate it with the **Run Embedded Macro with Data** action.

Editing Legacy Reflection Macros <User Guide>

You can edit legacy Reflection macros in the Visual Basic Editor. However, some Session methods and properties are no longer supported. For more information, see the [InfoConnect VBA Guide](#) (Help > VBA Guide).

To edit a legacy Reflection macro

1. Open the settings file that contains the legacy macro.
   - or-
   If you've previously saved a settings file that contains one or more legacy macros to a InfoConnect session document, open the session document.

2. Open the Visual Basic Editor.
   - The steps depend on your [user interface mode](#) (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reflection Ribbon</td>
<td>From the <strong>Tools</strong> ribbon, click <strong>Visual Basic</strong>.</td>
</tr>
<tr>
<td>Reflection Browser</td>
<td>On the <strong>Reflection</strong> menu, choose <strong>Tools</strong>, <strong>Macro</strong> and then <strong>Visual Basic</strong>.</td>
</tr>
<tr>
<td>TouchUx</td>
<td>Tap the Wrench icon and then under <strong>Macro</strong>, select <strong>Visual Basic</strong>.</td>
</tr>
</tbody>
</table>

3. In the Project pane, locate the project named `ProjectLegacy(filename)`, open the appropriate module, and then edit the macro.

   **NOTE:** Edits to legacy macros must be done in the legacy project (`ProjectLegacy`).

---

880    InfoConnect 2014 User’s Guide
4 Save the file as an InfoConnect session document to retain your changes. InfoConnect identifies the macro as a "legacy macro," even though it's in an InfoConnect session document.

**Editing Reflection Basic Macros**

**To edit Reflection Basic scripts**

1. Open the Reflection Basic Editor.
2. Open the Reflection Basic script that you want to edit.
3. Use Application for the Reflection object name.

**Code sample**

4. (Optional) To access information or procedures in other Reflection Basic scripts, use the $Include metacommand, the Declare statement, or the RunScript method.

**Code sample**

**To edit a Reflection Basic macro (script):**

1. Open the Reflection Basic Editor.
2. Open the Reflection Basic script that you want to edit.
3. Optional: To access information or procedures in other Reflection Basic scripts, use the $Include metacommand, the RunScript method, or the Declare statement.

**Example of the $Include metacommand:**

This line of code, (the comment is intended) will make functions in the common.rbs available to the .rbs file.

'include ".\common.rbs"

**Example of the RunScript method:**

This line of code runs the myTestRBScript.rbs script.

Application.RunScript "myTestRBScript.rbs", ""

**Related Topics**

- “Select Action Dialog Box” on page 161

**Run External Legacy Reflection Macro Dialog Box**

**Getting there**

1. Open the Run Macro dialog box.
   The steps depend on your user interface mode (page 120).
From the Run Macro dialog box, click Legacy Reflection Macro in Another File.

From this dialog box, you can run legacy Reflection macros (.rma, .rsf, .r2w, .r4w).

**Settings or macro filename**
- Type the filename for the macro or click Browse to select it.

**Select a macro**
- From the list, select the macro you want to run.

**Macro data**
- Enter any parameters that you want to execute with the macro.

---

**Run Embedded Macro with Data Dialog Box**

**Getting there**

This dialog box opens when you initiate the action Run Embedded Macro with Data. To initiate an action, you must create a custom control, and then map an action to it. When you use the control, the action occurs.

1. Create a control using any of the following features:
   - UI Designer
   - Keyboard Mapper
   - Mouse Mapper
   - Context Menu Editor

2. From the Select Action dialog box, under Action Category, select Macro.

3. From the Action list, select Run Embedded Macro with Data, and then click OK.
   - The action is mapped to the control that you created in step 1.

4. Use the control to execute the Run Embedded Macro with Data action.

From this dialog box, you can run embedded legacy Reflection macros in open session documents.

**Select Macro**
- From the list, specify the legacy Reflection macro that you want to run.

**Macro Data**
- Enter any parameters that you want to execute with the selected macro.

---

**Run Script Dialog Box**

**Getting there**

1. Open the Run Macro dialog box.
   - The steps depend on your user interface mode (page 120).
2 From the Run Macro dialog box, click Legacy RB Macro.

The options are:

File name
Specify the Reflection Basic macro file (.rbs) that you want by selecting it from the list, typing the name in the box, or browsing to select it.

Files of type
The default extension is .rbs. InfoConnect appends the extension .rbs to the filename.

Script arguments
Enter any arguments that you want to execute in the script.

Run
Choose to run the selected macro.

## Legacy EXTRA! Macros

**Index Term**
Primary: macros
Secondary: legacy EXTRA!

**Index Term**
Primary: EXTRA!
Secondary: macro support

You can run most EXTRA! macro files (.ebm) in InfoConnect, including encrypted EXTRA! macros.

---

**NOTE:** To use legacy EXTRA! macros in InfoConnect, you must install the Legacy EXTRA! feature when you install InfoConnect. (This feature is available on the Attachmate Installation Program Features tab, under 3270/5250 | Compatibility or UNIX and OpenVMS | Compatibility.)

---

### To run an EXTRA! macro

1 Open the Run Macro dialog box.

1a The steps depend on your user interface mode (page 120).
2 In the **Run Macro** dialog box, click **Legacy EXTRA! Macro**.
3 Browse to select a macro file, and then click **Open**. The macro must be in a trusted location.

**NOTE**
- If the macro contains unsupported objects, its functionality may be limited or it may not run.
- For a list of unsupported objects and methods, see the [InfoConnect VBA Guide](#) (Help > VBA Guide).
- Note: You can significantly improve the performance of your recorded EXTRA! macros by editing these macros to change how InfoConnect detects when the screen is ready for input. (See [Technical Note 2483](http://support.attachmate.com/techdocs/2483.html).)

**Editing Legacy EXTRA! Macros**

If you need to make changes to your legacy EXTRA! macros (.ebm), you can edit them using the EXTRA! Basic Editor.

To start the EXTRA! Basic Editor, you must first associate the Run EXTRA! Basic Editor action with a custom control, such as a button or a keyboard shortcut.

**NOTE:** You can significantly improve the performance of your recorded EXTRA! macros by editing these macros to change how InfoConnect detects when the screen is ready for input.

For more information about how to run legacy EXTRA! macros, set up the Basic editor, edit HostOptions properties, and improve performance of recorded macros, see [Technical Note 2483](http://support.attachmate.com/techdocs/2483.html).

**Related Topics**
- “Select Action Dialog Box” on page 161

**RUMBA Macros**

**Index Term**
Primary: RUMBA macros

**Index Term**
Primary: NetManage RUMBA macros

**Index Term**
Primary: macros
Secondary: RUMBA

**InfoConnect** includes support for Micro Focus RUMBA macros (.rmc).

**NOTE:** To run a RUMBA macro, the Micro Focus RUMBA compatibility feature must be installed. This feature is available on the Attachmate Installation Program Features tab, under 3270/5250 Compatibility.
To run a RUMBA macro

1 Open the Run Macro dialog box.
   1a The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reflection Ribbon</td>
<td>On the Session ribbon, from the Macros group, click Run Macro.</td>
</tr>
<tr>
<td>Reflection Browser</td>
<td>On the Reflection menu, choose Tools, Macro and then Run Macro.</td>
</tr>
<tr>
<td>TouchUx</td>
<td>Tap the Wrench icon and then under Macro, select Show Run Macro Dialog.</td>
</tr>
</tbody>
</table>

2 In the Run Macro dialog box, click RUMBA Macro.
3 Browse to select a macro file, and then click Open.

IBM Personal Communications Macros

InfoConnect includes support for IBM Personal Communications macros (.mac).

**NOTE:** To run a Personal Communications macro, the IBM Personal Communications compatibility feature must be installed. This feature is available on the Attachmate Installation Program Features tab, under 3270/5250 | Compatibility.

To run a Personal Communications macro

1 Open the Run Macro dialog box.
   1a The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reflection Ribbon</td>
<td>On the Session ribbon, from the Macros group, click Run Macro.</td>
</tr>
<tr>
<td>Reflection Browser</td>
<td>On the Reflection menu, choose Tools, Macro and then Run Macro.</td>
</tr>
<tr>
<td>TouchUx</td>
<td>Tap the Wrench icon and then under Macro, select Show Run Macro Dialog.</td>
</tr>
</tbody>
</table>

2 In the Run Macro dialog box, click IBM Personal Communications Macro.
3 Browse to select a macro file, and then click Open.

Brandon Systems/Jolly Giant QWS3270 Macros

InfoConnect supports QWS (.jgs) macros that run against IBM 3270 terminal sessions.

**NOTE:** To run a QWS macro, the Brandon Systems/Jolly Giant QWS3270 QWS compatibility feature must be installed. This feature is available on the Attachmate Installation Program Features tab, under 3270/5250 | Compatibility.
To run a QWS macro

1 Open the Run Macro dialog box.
   1a The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reflection Ribbon</td>
<td>On the Session ribbon, from the Macros group, click Run Macro.</td>
</tr>
<tr>
<td>Reflection Browser</td>
<td>On the Reflection menu, choose Tools, Macro and then Run Macro.</td>
</tr>
<tr>
<td>TouchUx</td>
<td>Tap the Wrench icon and then under Macro, select Show Run Macro Dialog.</td>
</tr>
</tbody>
</table>

2 In the Run Macro dialog box, click QWS Macro.
3 Browse to select a macro file, and then click Open.

Hummingbird Basic Macros

InfoConnect supports OpenText HostExplorer Hummingbird Basic (.ebs) macros that run against IBM 3270 terminal sessions.

NOTE: To run a Hummingbird Basic macro, the HostExplorer compatibility feature must be installed. This feature is available on the Attachmate Installation Program Features tab, under 3270/5250 | Compatibility.

To run a Host Explorer macro

1 Open the Run Macro dialog box.
   1a The steps depend on your user interface mode (page 120).

<table>
<thead>
<tr>
<th>User Interface Mode</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reflection Ribbon</td>
<td>On the Session ribbon, from the Macros group, click Run Macro.</td>
</tr>
<tr>
<td>Reflection Browser</td>
<td>On the Reflection menu, choose Tools, Macro and then Run Macro.</td>
</tr>
<tr>
<td>TouchUx</td>
<td>Tap the Wrench icon and then under Macro, select Show Run Macro Dialog.</td>
</tr>
</tbody>
</table>

2 In the Run Macro dialog box, click HostExplorer Macro.
3 Browse to select a macro file, and then click Open.
authentication. The process of reliably determining the identity of a communicating party. Identity can be proven by something you know (such as a password), something you have (such as a private key or token), or something intrinsic about you (such as a fingerprint).

authentication server (AS). A service of the KDC (Key Distribution Center) that issues authentication credentials for a principal. When a user requests a service that requires Kerberos authentication, the AS consults the Principals database for valid principals and passwords, then issues a set of authentication credentials, which includes a TGT (ticket-granting ticket).

CA (Certificate Authority). A server, in a trusted organization, which issues digital certificates. The CA manages the issuance of new certificates and revokes certificates that are no longer valid for authentication. A CA may also delegate certificate issuance authority to one or more intermediate CAs creating a chain of trust. The highest level CA certificate is referred to as the trusted root.

cipher. A cipher is an encryption algorithm. The cipher you select determines which mathematical algorithm is used to obscure the data being sent after a successful Secure Shell connection has been established.

credentials cache. The location of stored credentials. Credentials consist of session keys, TGTs, and service tickets issued to a client by the KDC. The client uses its credentials to authenticate itself when it requests a service.

credentials file. This file is used by a client to authenticate itself when it requests a service. The credentials file stores the session keys, TGTs, and service tickets issued to the client by the KDC.

If your system administrator has installed a configuration file, Reflection Kerberos Manager automatically sets a default credentials filename and location the first time you start. If not, specify a credentials filename and location in the Initial Configuration dialog box, or use the suggested default (your Windows personal documents folder). You can modify the credential storage location for each principal profile using Kerberos Manager.

CRL (Certificate Revocation List). A digitally signed list of certificates that have been revoked by the Certification Authority. Certificates identified in a CRL are no longer valid.

digital certificate. An integral part of a PKI (Public Key Infrastructure). Digital certificates (also called X.509 certificates) are issued by a certificate authority (CA), which ensures the validity of the information in the certificate. Each certificate contains identifying information about the certificate owner, a copy of the certificate owner's public key (used for encrypting and decrypting messages and digital signatures), and a digital signature (generated by the CA based on the certificate contents). The digital signature is used by a recipient to verify that the certificate has not been tampered with and can be trusted.

encryption. Encryption is the process of scrambling data by use of a secret code or cipher so that it is unreadable except by authorized users. Encrypted data is far more secure than unencrypted data.

hash. Also called a message digest, a hash or hash value is a fixed-length number generated from variable-length digital data. The hash is substantially smaller than the original data, and is generated by a formula in such a way that it is statistically unlikely that some other data will produce the same hash value.

hosts file. A list that maps recognizable host names to Internet addresses, similar to a domain name system. You can use a hosts file whether there is a domain name server on your network.
**Hotspots.** Hotspots are specific areas or text that are associated with host functions, macros, or commands. When enabled, hotspots appear in the terminal area of a display session.

**KDC (Key Distribution Center).** The security server that maintains the database of principal information, uses the information in the database to authenticate users, and controls access to kerberized services in a realm.

**Kerberize.** A host, server, or client application that has been modified to use Kerberos for authentication and encryption.

**Kerberos.** A protocol that uses a trusted third party to enable secure communications over a TCP/IP network. The protocol uses encrypted tickets rather than plain-text passwords for secure network authentication.

**Layout.** A layout is a settings file that you can create to restore your workspace and all open documents. It also restores the workspace position and tab properties of open documents.

**LDAP (Lightweight Directory Access Protocol).** A standard protocol that can be used to store information in a central location and distribute that information to users.

**OCSP (Online Certificate Status Protocol).** A protocol (using the HTTP transport) that can be used as an alternative to CRL checking to confirm whether a certificate is valid. An OCSP responder responds to certificate status requests with one of three digitally signed responses: "good", "revoked", and "unknown". ![Writer's comment. These terms should not be translated.] Using OCSP removes the need for servers and/or clients to retrieve and sort through large CRLs.

**Office Tools.** The Office Tools feature allows you to integrate host data with Microsoft Office applications, if those applications are installed on your computer. You can create Word documents and PowerPoint presentations, send e-mail, schedule appointments, add notes and tasks, and create new contacts.

**Passphrase.** A passphrase is similar to a password, except it can be a phrase with a series of words, punctuation, numbers, white space, or any string of characters. Passphrases improve security by limiting access to secure objects, such as private keys and/or a key agent.

**PKCS.** PKCS (Public Key Cryptography Standards) is a set of standards devised and published by RSA laboratories that enable compatibility among public key cryptography implementations.

Different PKCS standards identify specifications for particular cryptographic uses, for example:

- PKCS#7 can be used to sign and/or encrypt messages. It can also be used to store certificates and to disseminate certificates (for instance as a response to a PKCS#10 message).
- PKCS#10 is a certification request syntax.
- PKCS#11 is a programming interface used for cryptographic hardware tokens.
- PKCS#12 defines the personal information exchange syntax used for storage and transportation of certificates and associated private keys. Files in this format typically use a *.pfx or *.p12 extension.

**Port forwarding.** A way to redirect unsecured traffic through a secure SSH tunnel. Two types of port forwarding are available: local and remote. Local (also called outgoing) port forwarding sends outgoing data sent from a specified local port through the secure channel to a specified remote port. You can configure a client application to exchange data securely with a server by configuring the client to connect to the redirected port instead of directly to the computer running the associated server. Remote (also called incoming) port forwarding sends incoming data from a specified remote port through the secure channel to a specified local port.
principal. Any user, client, network service, application, or host system that is recognized by the Kerberos server. Each principal has a unique name within a realm. The format of a full principal name is:

<principal name>@<realm name>

If the realm name is omitted, the default realm is assumed.

principal profile. A collection of information that defines who you are (your principal and realm names) and which settings you want to use (requested ticket lifetime, how your credentials should be stored, and the name of your profile).

principals database. A database containing valid principals and passwords for a particular realm. Each realm has its own credentials database. This database is part of the KDC (Key Distribution Center).

Privacy Filters. This feature provides a way to filter out sensitive data (for example, Social Security or account numbers), and refrain from displaying it in productivity features, such as Office Tools integration, Screen History, Recent Typing, and Auto Complete, and to obscure data from the Print Screen and Cut/Copy/Paste commands.

product installation folder. The default is \Program Files\Attachmate\InfoConnect.

Public Key Infrastructure (PKI). PKI is a framework of policies, services, and encryption software used for authentication and encryption of sensitive information. The PKI framework depends on trusted third parties called certification authorities (CAs), which issue digital certificates.

public key/private key. Public keys and private keys are pairs of cryptographic keys that are used to encrypt or decrypt data. Data encrypted with the public key can only be decrypted with the private key; and data encrypted with the private key can only be decrypted with the public key.

realm. The name applied to a group of Kerberos principals on a network. All principals in a Kerberos realm are governed by the same Kerberos policies. The realm name is often similar to, or the same as, the domain name. The realm name is case sensitive — typically uppercase in a Kerberos environment.

Recent Typing. Using the Recent Typing gallery or task pane, you can quickly view and select from a list of recently typed items, and send the selected string to the active document. This eliminates the need to manually re-enter information, saving time, and reducing errors when entering commonly-typed commands or field data.

Scratch Pad. Use the Scratch Pad to keep notes associated with a session. From the task pane you can print or save the Scratch Pad notes as .RTF or .TXT files.

Screen History. Screen History creates recordings of IBM 3270 and 5250 host screens as you navigate to them. VT screens can be recorded using manual capture. You can view and/or verify the information from those screens, and send multiple host screens to Microsoft Word, PowerPoint, and Outlook (Email Message and Note only), if they are installed on your computer.

secret key cryptography. In this form of cryptography, which is sometimes referred to as symmetric cryptography, data is encrypted and decrypted using the same key or shared secret quantity.

Secure Shell. A protocol for securely logging onto a remote computer and executing commands. It provides a secure alternative to Telnet, FTP, rlogin, or rsh. Secure Shell connections require both server and user authentication, and all communications pass between hosts over an encrypted communication channel. You can also use Secure Shell connections to forward X11 sessions or specified TCP/IP ports through the secure tunnel.
**service ticket.** To gain access to a service that requires Kerberos authentication, the client application must present a valid service ticket. The KDC issues the service ticket when Reflection Kerberos sends a valid TGT and requests a ticket to the service.

A service ticket typically remains valid for the life of the TGT. A new service ticket is required to log into a different host, or to use a different service on the same host.

**services provider.** A kerberized server that processes the requests of its clients. Services providers are often running as server daemons, such as telnetd or ftplib, on host machines.

**SOCKS.** SOCKS is a software protocol used in conjunction with a firewall host system to provide secure, controlled access to internal and external networks. When you request a network connection from a SOCKS-enabled application, the SOCKS Client software communicates with the SOCKS server software to determine if the connection is allowed. If it is, the connection is established. If it is not, the SOCKS server rejects the connection request.

**SSL/TLS.** The Secure Sockets Layer protocol (SSL) and its compatible successor, the Transport Layer Security protocol (TLS), enable a client and server to establish a secure, encrypted connection over a public network. When you connect using SSL/TLS, the client authenticates the server before making a connection, and all data passed between Reflection and the server is encrypted.[<shared glossary text>]

**template.** A template includes all of the settings specific to documents. When you create a new document based on this template, it is configured identically, except that it prompts the user for a new name.

**TGT request.** A request for a ticket-granting ticket sent by the Reflection Kerberos client application to the KDC (Key Distribution Center).

**ticket lifetime.** Refers to the period of time for which a ticket-granting ticket is valid. The user can request a ticket lifetime value when requesting a ticket-granting ticket. The server determines the maximum ticket lifetime. The default is eight hours (8h).

**ticket-granting server (TGS).** The component of the KDC (Key Distribution Center) that issues service tickets to clients requesting services from a kerberized application. The Reflection Kerberos client sends a request to the TGS containing the identity of the principal. If the TGS verifies that the principal and realm are valid, it sends a TGT and a session key (encrypted using a key derived from the principal's password which is stored on the KDC) to the Reflection Kerberos client.

**ticket-granting ticket (TGT).** The KDC generates a ticket-granting ticket (TGT) when a user requests access to a service that requires Kerberos authentication.

The Reflection Kerberos client uses the TGT to obtain service tickets each time the user requests access to a kerberized application. The user does not have to authenticate again until the ticket-granting ticket expires.

**trusted host.** A trusted host is one for which you hold the public key.

**URI (Uniform Resource Identifier).** A string of characters that represents the location or address of a resource. URIs can be used to locate resources on the Internet or on an LDAP server.

**Windows common application data folder.** The application data folder is hidden by default.

The default is:

- Windows 8, Windows 7, Windows Vista, Windows Server 2008:

  \ProgramData\
Windows personal application data folder. The personal application data folder is hidden by default.

The default personal roaming application data folder is:

- Windows XP, Windows Server 2003:
  \Documents and Settings\all users\Application Data\n
Windows personal documents folder. The default is:

- Windows XP, Windows Server 2003:
  \Documents and Settings\username\My Documents\n
Workspace Menu. The Workspace menu contains layout options, application and document settings, and a list of recent documents. It is accessed by clicking the Reflection button (when using the Office 2007 look and feel) or the File menu (when using the Office 2010 look and feel).

socket. The combination of a host name (IP address or DNS name) and a port number. This creates a unique identifier that a client application uses as an end point of communications.

PCI DSS. PCI DSS (Payment Card Industry Data Security Standard) is a worldwide standard comprising technology requirements and process requirements designed to prevent fraud and is published by PCI Security Standards Council, LLC (https://www.pcisecuritystandards.org/). All companies who handle credit cards are likely to be subject to this standard.

Express Logon Feature (ELF). Also referred to as single sign-on (SSO), express logon is an IBM mainframe feature that lets users log on and connect to the host without entering a user ID and password each time. Express Logon authenticates the user on the mainframe by using her SSL client certificate in lieu of entering a user ID and password.

Reflection ssh folder. Reflection stores Secure Shell information for individual users in the following location in the Windows personal documents folder:

Windows XP, Windows Server 2003:
\Documents and Settings\username\My Documents\Attachmate\Reflection\.ssh

Windows 7, Windows Vista, Windows Server 2008:
\Users\username\Documents\Attachmate\Reflection\.ssh

Comparable files are placed in the $HOME directory on UNIX systems.

Reflection application data folder. Reflection stores Secure Shell information that is available to all users in the following location:

Windows XP, Windows Server 2003:
\Documents and Settings\all users\Application Data\Attachmate\Reflection
Windows 7, Windows Vista, Windows Server 2008:
\ProgramData\Attachmate\Reflection

**Auto Expand.** Use the Auto Expand feature to add acronyms or shortcuts for long words, phrases, or complex repeat commands. The shortcut, when typed and followed by the Spacebar, automatically expands to the full word or phrase.

**APVUFILE.** A file transfer protocol used for transfers to and from double-byte enabled IBM 3270 hosts. Configure APVUFILE transfers from the Mainframe tab of the File Transfer Settings dialog box.

**keyboard map.** A keyboard map is a configuration file that allows you to use your PC keyboard as a host terminal keyboard. Keyboard maps also include definitions for keyboard shortcuts.

**Trusted Locations.** A trusted location is a directory that's designated as a secure source for opening files. By default, InfoConnect allows you to open documents only in directories specified as trusted locations in the InfoConnect settings.

**digital signature.** Used to confirm the authenticity and integrity of a transmitted message. Typically, the sender holds the private key of a public/private key pair and the recipient holds the public key. To create the signature, the sender computes a hash from the message, and then encrypts this value with its private key. The recipient decrypts the signature using the sender's public key, and independently computes the hash of the received message. If the decrypted and calculated values match, the recipient trusts that the sender holds the private key, and that the message has not been altered in transit.