Installation and Deployment Guide
InfoConnect Desktop

Micro Focus® InfoConnect®

MICRO FOCUS®

Installation and Deployment Guide

InfoConnect Desktop

Version 16.0

MICRO FOCUS

Copyrights and Notices

Trademarks

Third-Party Notices

This product contains software from third party suppliers.

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

Specific notice applicable to the optional PKI Manager module:

RSA (now EMC) - BSAFE Crypto-J

Includes RSA BSAFE cryptographic or security protocol software from RSA.

Additional third-party copyrights and notices, including license texts and other materials passed through in compliance with third party license terms, can be found in a `thirdpartynotices.txt` file in the program installation folder.

1 Key Concepts

This guide describes how to install, customize and deploy InfoConnect Desktop. There are a number of options available to help administrators install customized versions of the product that make end-user tasks easier and less error-prone. Before you dive into the details, we recommend that you review these key concepts to get an overview the options available to you:

You can use the links provided for each concept to find additional information and procedures to help you get started. As you work through the procedures, you can also use the context-sensitive product Help for further detail.

The Setup Program (Setup.exe)

Users can install InfoConnect using the Setup program (`setup.exe`) directly from a download. Administrators can also customize the installation and run setup.exe from a command line.

- **Running Setup directly**

  When users run Setup directly, they can select which features to install, specify the program installation location, and set data folder locations.

  Use the **Features** tab to select which features to install. The features available to you depend on your InfoConnect Product. See "Feature Selection" on page 11 for a list of which features are available.

  Use the **Data Location** tab to configure where InfoConnect stores data. See "Data Location" on page 12.

  NOTE: The **Data Location** tab is not visible if you are installing InfoConnect Desktop on a system with an earlier version of InfoConnect. After an upgrade, InfoConnect Desktop continues to use your existing data locations.

- **Using the Setup program's administrative features**

  Using the **Advanced** tab you can create an administrative installation image on a network server. This network location can be used by deployment tools to access and create packages that are deployed to workstations. See "Choose the type of Installation" on page 13. You can also use this tab to set logging options. See "Set logging options" on page 13.

  Launching `Setup.exe` in admin mode starts the Installation Customization Tool, a powerful tool from customizing your installations. See "The Installation Customization Tool" on page 39 and "Deploy using the Setup Program" on page 69.

- **Running Setup from the command line**

  You can use the Setup program command line to install InfoConnect from the distribution image, or from an administrative installation image. You can also include command-line options in a batch file to preset installation parameters, and limit user interaction while InfoConnect is installing. You can suppress installation dialog boxes to provide an unattended installation. See “Deploy using the Setup command line” on page 70.

Customizing InfoConnect Desktop

InfoConnect uses a variety of files to store customized data. Administrators can simplify the user experience by preconfiguring and installing customized files.

- **Paths**

  Information required for connecting to ALC, UTS, and T27 hosts is configured in paths, which are saved in the InfoConnect database. You can include a customized database as part of your installation. See “Paths” on page 17.

- **Session documents and customization files**

  By default, InfoConnect saves basic terminal session configuration in a session document, which includes connection and terminal settings. Additional customizations are saved by default to separate customization files that can be associated with one or more terminal sessions. These customization files include theme files (for customizing color and font), keyboard maps, mouse maps, hotspots, customized ribbons, and QuickPads. For information about customizing InfoConnect, see “Session Documents” on page 22. For a complete list of files used by InfoConnect, see “Files Used by InfoConnect” on page 80.

- **Compound session documents**

  You can create a compound session document that includes all the settings in any associated theme, keyboard map, mouse map, hotspot, ribbon, or QuickPad file. This option enables you to deploy session files with all required customizations included in a single file. See “Compound Documents” on page 23.

- **Templates**

  Templates provide default configurations for connecting to specified file types. InfoConnect Desktop ships with default templates for each of the supported session types included with your product. You can also create and deploy custom templates designed to meet the needs of your users. See “Session Templates” on page 24.

- **Workspace settings**

  Workspace settings affect all terminal sessions. Configure these from the Workspace Settings dialog box and deploy them using a custom `Application.settings` file. See “Workspace Settings” on page 25.

- **Layouts**

  Layouts are saved Workspace arrangements. You can open and arrange multiple host sessions, then save your configuration as a layout. When you open the layout, all of the sessions in the layout open in the arranged configuration. You can include custom layout files (`*.rwsp`) as part of your deployment.

Configuring Security

- **Encrypted connections**

  InfoConnect sessions support a number of encryption options, including SSL/TLS, SSH, and Kerberos. To see which options are available with each connection type, see “Secure Connections” on page 31.

- **Reflection Certificate Manager**

  InfoConnect includes the Reflection Certificate Manager, which you can use to manage PKI certificates for use by InfoConnect sessions. See “Digital Certificates and Reflection Certificate Manager” on page 31.

- **Deploying PKI and SSH settings**

  If you configure certificate authentication using the Reflection Certificate Manager, settings are saved to a `.pki` folder in the user folder. If you configure non-default Secure Shell connections, settings are saved to a `.ssh` folder in the user data folder. These settings are not included in compound documents.

- **Trusted locations**

  A trusted location is a directory that is designated as a secure source for opening files. By default, InfoConnect allows users to open documents only in directories specified as trusted locations. Settings to modify these defaults are available from the **Workspace Settings** dialog box. See “Configure Trusted Locations” on page 36.

- **Information Privacy**

  Information Privacy features allow you to configure Reflection so that the sensitive data is not displayed on the screen or in productivity features, such as Screen History. It also allows you to require secure connections. See “Configure Information Privacy” on page 36.

- **API and Macro Security**

  Settings limiting API and macro functionality are available from the **Workspace Settings** dialog box. See “Configure API and Macro Security” on page 38.

Installation Customization Tool

The Installation Customization Tool is a special mode of the Setup program (setup.exe). You can use the Installation Customization Tool to create transforms to customize the installer (`*.mst`) and companion installer packages to install additional files (`*.msi`).

- **Working with the Installation Customization Tool**

  To run the Installation Customization Tool, create an administrative installation point, then run setup from the command line using this syntax `setup.exe /admin`. You’ll be prompted to choose which mode you want to run in. Detailed help is available from the tool for each panel. For more information about setting up your administrative workstation to work with this tool, see “Setup for Customized Deployments Using the Installation Customization Tool” on page 39.

- **Setup customization files (transforms)**

  To create a transform file, choose **Create a new Setup customization** when you launch the Installation Customization Tool. Use this option to select which features to install, to customize start menu shortcuts, and to configure programs to run automatically before or after `Setup.exe`. See “Create Setup Customization Files (Transforms)” on page 42.

- **Companion installers**

  To create a companion installer, choose **Create a new Companion installer**. when you launch the Installation Customization Tool. Use this option to install additional files. You can specify where to install the files (for individual users or all users) and configure shortcuts to launch files. You can use the **Modify user settings** option to launch InfoConnect on your administrative workstation, create custom files, and include them in your companion file. This approach automatically installs the files to the correct location. See “Use Companion Packages to Install Customized Settings” on page 45.

  You can deploy companion installers to users by using the Installation Customization Tool to configure the Setup program to run these programs automatically before or after the InfoConnect install. See “Create a Chain Installation to Run Additional Programs” on page 44

  If you have set up a Management and Security Server, you can use it to deploy companion installers. See “Deploy MSI Packages from Management and Security Server” on page 65.

Micro Focus Management and Security Server

Micro Focus Management and Security Server is a management tool available separately. Using Management and Security Server, an administrator can create, configure, secure, and monitor terminal client sessions from one central location.

- **Centralized session management**

  Create and manage InfoConnect sessions using the Administrative WebStation. Sessions that you create this way are saved to the server and can be made available to users from the server. When you manage sessions this way, you can limit session access to specific users or groups using a directory server (LDAP/Active Directory). See “Create Sessions using the Administrative WebStation” on page 56 and “Deploy Sessions Saved to the Management Server” on page 58.

- **Security Proxy**

  The Security Proxy acts as a proxy for terminal sessions and provides token-based access control, routing encrypted network traffic to and from user workstations. The Security Proxy enables you to create SSL/TLS encrypted sessions even if your host is not configured with an SSL/TLS server. See “Connect to Hosts using the Security Proxy” on page 59.

- **ID Management**

  Use the Terminal ID Manager to configure and monitor a pool of resource IDs that can be used to establish a host session. This eliminates the need to configure a terminal ID (GPID or LU) for each and every client. See “Configure Sessions to use ID Manager to Assign Terminal IDs” on page 64.

- **Deploy companion packages to users or groups**

  Use the Package Manager to upload companion install packages (`*.msi`) to the Management and Security Server for deployment to specified users or groups. For example, use these packages to install customized sessions and Workspace settings. Packages assigned to a user are automatically deployed to a user's desktop when the user logs on to the Management and Security Server or starts an InfoConnect Workspace session with Centralized Management enabled. See “Deploy MSI Packages from Management and Security Server” on page 65.

- **Usage metering**

  Use the Metering Server to track InfoConnect sessions and determine how many client workstations use the product. Metering can also be used to limit the number of concurrent users that can access a host at any given time. See “Enable Usage Metering” on page 66.

Deployment Options

InfoConnect uses standard Windows installer technology (MSI) and supports a number of deployment options.

- **Deploy using the Setup program**

  The Setup program (`setup.exe`) is the recommended tool for installing and deploying InfoConnect. You can have end users run Setup themselves, or you can use the Setup on the command line to manage customized automated installations. See “Customize the Setup installation” on page 69 and “Deploy using the Setup command line” on page 70.

- **Deploy MSI packages using msiexec.exe**

  You can deploy InfoConnect directly from the MSI command line. You can also deploy companion `.msi` files that you have created to contain your custom configuration files. See “Deploy InfoConnect from MSI Command Line” on page 71 and “Deploy a Companion MSI File from the MSI Command Line” on page 72.

- **Deploy using standard Microsoft tools**

  See “Publish with Active Directory” on page 75 and “Deploy with System Center Configuration Manager” on page 76.

2 The InfoConnect Setup Program

You can install InfoConnect Desktop using the Setup program (`setup.exe`) which is available after you expand your download package.

For workstation installs, the Setup program provides a user interface that enables users to select where to install the program files, which features to install, and where to store user data. This chapter covers the options available in this user interface. For information about running `setup.exe` from a command line, see “Deploy using the Setup command line” on page 70.

The Setup program can also be run in an administrative mode. This mode launches the Installation Customization Tool, which can be used to customize the installation and to install additional files. For information about working with this tool, see “The Installation Customization Tool” on page 39.

In this Chapter

Related Topics

- “Deploy using the Setup Program” on page 69
- “Upgrading from Earlier Versions of InfoConnect” on page 15

Feature Selection

Use the **Features Selection** tab of the Setup program to select which features to install. The features available to you depend on your InfoConnect Product. The following table summarizes the features for each of the following:

- InfoConnect Desktop for Unisys
- InfoConnect Desktop for Unisys Pro
- InfoConnect Desktop for Airlines
- InfoConnect Desktop for Airlines Pro

Features in **[brackets]** are included in a default installation.

Feature	Unisys	Unisys Pro	Airlines	Airlines Pro
Unisys Transports	X	X		
[TCPA], **[INT1]**, MATIP for UTS, CCF				
Airline Transports			X	X
[INT1], **[MATIP for ALC]**, MATIP for UTS, ATSTCP, UDPFRAD (with TCPFRAD), SABRE, Airlines Gateway, PEPGate (with add-on)				

Feature	Unisys	Unisys Pro	Airlines	Airlines Pro
3270/5250		X		X
Compatibility: **[Legacy EXTRA!]**, IBM Personal Communications, **[Rumba]**, OpenText Host Explorer, Jolly Giant QWS				
[UNIX and OpenVMS]		X		X
Compatibility: **[Legacy EXTRA!]**, Legacy KEA!, Rumba, OpenText Host Explorer				
HP with NS/VT		X		X
Options Pack	X	X	X	X
GraphX, Automation Development Kit, Connectivity Services Development Kit				
Productivity: **[Screen History**, **Office Tools**, **Auto Complete, Auto Expand, Spell Check, Recent Typing**, **Scratch Pad]**	X	X	X	X
[Visual Basic for Applications]	X	X	X	X
Quick Launch	X	X	X	X
Web Browser	X	X	X	X
[FTP Client]	X	X	X	X
Utilities: **[Kerberos Manager**, **Key Agent]**	X	X	X	X

The following utilities do not appear in the Setup program feature tree. They are installed as follows:

- The Database Editor and InfoConnect Manager are installed with all InfoConnect products.
- T27 Printer Services are installed with both Unisys products.
- PTR Printing can be added to the Airlines products as an add-on.
- The Reflection IBM Printer is installed when you install the 3270/5250 feature, which is available with Unisys Pro and Airlines Pro.

Data Location

Use the **Data Location** tab in the Setup program to configure where InfoConnect stores data. This tab includes two options—a user data location and an application data location.

NOTE: The **Data Location** tab is not visible if you are installing InfoConnect Desktop on a system with an earlier version of InfoConnect. After an upgrade, InfoConnect Desktop continues to use your existing data locations.

- **User data**

  The user data location is used for session documents, customization files (such as themes and keyboard maps), macros, translation tables, Secure Shell configuration, Reflection Certificate Manager configuration, and FTP Client settings.

The default is user-specific: `C:\Users\username\Documents\Micro Focus\InfoConnect`. You can modify this to use the Public Documents folder, or specify an alternate location of your choice.

- **Application data**

  The application data location is used for the InfoConnect database, PTR configuration, and trace files.

  The default location is shared by all users: `C:\Users\Public\Documents\Micro Focus\InfoConnect`. You can modify this to a user-specific location in the Documents folder, or specify an alternate location of your choice.

Advanced Tab

The Advanced tab includes options for creating an administrative installation point and for managing the installation log.

Choose the type of Installation

Two choices are available.

- **Install to this PC**

  Use this option to install InfoConnect.

- **Create an administrative install image on a server**

  Use this option to create an administrative install image, typically on a network server. 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.

NOTE: An administrative install image is not a working installation of the product. If you want to install all available features on an administrative workstation, select **Install to this PC**, and use the **Feature Selection** tab to configure installation of all features.

Set logging options

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` and uses a `.log` extension. To open this directory, launch the **Start** menu **Run** command and enter `%tmp%`.

Related Topics

- “Stage the Installation Files on a Server” on page 39

3 Upgrading from Earlier Versions of InfoConnect

You can install and use InfoConnect Desktop 16 on systems running earlier versions of InfoConnect. When you install using the Setup program:

- The installer will remove your prior version software before installing the new version.
- The installer does not remove existing session, macro, or scheme files. After the upgrade, you can continue to use your legacy files.
- The installer will not remove any product specific registry settings in HKCU.
- When you upgrade an existing system InfoConnect continues to use your existing locations for application and data files. (When you install on a new system, InfoConnect Desktop uses new default locations for these files.)

NOTE: If you are upgrading from InfoConnect version 8.1 SP1 or later, you may need to move some files manually after the upgrade. If you configured any of the following, see "Managing FTP Client and Shared Security Settings after an Upgrade" on page 83.

- FTP Client settings.
- Secure Shell known hosts and non-default Secure Shell settings.
- Certificates and settings configured using the Reflection Certificate Manager.

Working with Your Files After an Upgrade

You can continue to connect to hosts and work with host screens using your existing session files and customized settings. In most cases you can continue to use your prior version files with no modification. Changes are always saved to new files using the new format; your prior version files are never changed.

Working with these files...	After the upgrade...
Terminal session files (`*.adp`, `*.edp`, `*.idp`)	You can open your existing session files from the InfoConnect Desktop Workspace (which replaces the Accessory Manager), or by opening the files from the Windows file explorer. (If you configured a non-default file extension for you earlier version session files, you can also open these files from the Workspace.) When you save your session after opening a legacy file, a new session document is created using the new format and a new file extension. The legacy session file remains unchanged. InfoConnect Desktop introduces a new level of security by configuring trusted locations and requiring that session files be in a designated trusted location. Your Windows Documents folder is configured to be a trusted location by default, so legacy files in that folder will open successfully. If you saved files to a different location, you may need to add that location to the trusted location list.

Working with these files...	After the upgrade...
Layouts (`*.aww`)	You can open your existing layout files from the InfoConnect Desktop Workspace or directly from the Windows file explorer. New and modified layouts are saved using the new format and file extension (`*.rwsp`).
Keyboard maps (`*.ekm`)	InfoConnect Desktop supports your existing keymap files (`*.ekm`). You can attach new InfoConnect Desktop sessions to current-version keyboard map files (`*.xkb`) or legacy keyboard map files (`*.ekm`).
QuickPads (`*.eqp`) and Toolbars (`*.etb`)	InfoConnect Desktop supports your existing QuickPad and toolbar files. (Toolbars are imported as QuickPads docked on the top of the session window.) Modifications to existing QuickPads are saved using the new format and file extension (`*.rqpx`).
InfoConnect database (`ic32.cfg`)	After an upgrade, InfoConnect continues to use your existing database in its current location. All path configuration in the database continues to be used for existing session files and can be used to create new session files in the new format. If you install on a new system, the database is created by default in a new location.
Hotspots (`*.ehs`)	Legacy hotspot schemes are migrated to current version hotspot file format (`*.xhs`).
Extra! macros (`*.ebm`)	You can continue to run and edit most Extra! Basic macros. For details, see “EXTRA! Macros” in the InfoConnect product Help.
CASL macros (`*.xwc`, `*.xws`)	You can continue to run and edit your CASL macros. For details, see “CASL Macros” in the InfoConnect product Help.

NOTE: Security Files (`*.esf`) which were used by the Accessory Manager frame to limit access, are not used by InfoConnect Desktop. There are other means of limiting access to InfoConnect Desktop features. See “Locking Down Settings” on page 27.

4 Customize InfoConnect

InfoConnect uses a variety of files to store customized data. Administrators can simplify the user experience by preconfiguring and installing customized files.

This chapter reviews how to customize InfoConnect using an installation running on your a Workstation.

In this Chapter

Paths

An InfoConnect path is a named collection of configuration settings that allows you to connect to a host. Paths are required for connections to ALC, T27 and UTS terminal sessions. In the Airlines products, paths are also used for holding the settings-specific device access in PTR. Path configuration information is stored in the InfoConnect database. After an administrator has configured paths and deployed InfoConnect with the required transports and a customized database, end users can create sessions using the preconfigured paths.

Configuring Paths

You can create and manage paths using the Path Wizard, the Database Editor, or the InfoConnect Manager. All three tools save changes to the InfoConnect database. Use the procedures below to launch these tools.

You can create a separate connection path for each host connection. Or, if you have purchased the Micro Focus Management and Security Server and configured the Terminal ID Manager Add-On, you can create a pooled connection path and specify multiple terminal IDs for a single path. See "Configure Sessions to use ID Manager to Assign Terminal IDs" on page 64.

NOTE: Some tasks in the Database Editor and the InfoConnect Manager require an administrator logon. By default the administrator account login is an empty string. This configurable password-protection for these tools does not use the Windows administrator logon.

Path Wizard

The wizard takes you through configuration steps in the correct order to ensure that you specify settings in the correct order.

To start the Path Wizard

1. Start the **InfoConnect Workspace**.
2. Open the **Create New Document** dialog box. (page 22)

3 Select an ALC, UTS, or T27 terminal template and click **Create**.

4 Click **Create Path**.

Database Editor

You can start the Database Editor from the InfoConnect Workspace or from the Windows Start menu.

To launch the Database Editor from the Windows Start menu

1 From the Windows Start menu, go to **Micro Focus InfoConnect** > **Utilities**.

2 Click **Database Editor**.

To launch the Database Editor from the Workspace

1 Open **InfoConnect Workspace Settings** dialog box. (page 25)

2 Click **Manage Path**.

3 Click **Create new Path** or **Modify the selected path**.

-OR-

1 Open the **Create New Document** dialog box. (page 22)

2 Select an ALC, UTS, or T27 terminal template and click **Create**.

3 Right-click in the list of paths and select **Modify path** or **DB Editor**.

InfoConnect Manager

The InfoConnect Manager is an administrative tool that you can use to create and configure paths, as well as to perform additional administrative functions.

NOTE: InfoConnect Manager is an updated version of "INFOConnect Manager 32-bit" in earlier InfoConnect products.

To start the InfoConnect Manager

1 From the Windows Start menu, go to **Micro Focus InfoConnect** > **Utilities**.

2 Click **InfoConnect Manager**.

Deploying the Database

When you deploy InfoConnect, ensure that you have included all the required transports and deploy your modified database to the InfoConnect application data folder. This folder location is configurable using the **Data Location** tab during installation. The default is `C:\Users\Public\Documents\Micro Focus\InfoConnect`. You can also configure a per-user location for the database.

Because the database stores everything that you've configured up to this point, it can capture and store settings that aren't relevant to or beneficial for all users. If you deploy to a user-specific location, you can create a user-specific database by starting with a clean database each time you configure paths to deploy to individual users. You can do this by moving or renaming your existing InfoConnect database files before you start InfoConnect. That way, the database only includes information relevant to the user.

An alternate approach to deploying the database directly is to deploy an `.ini` file that you have created using the Export/Import Utility described below. You can use the Utility or the `expimp32.exe` command line to import the `.ini` file into the database after product installation. (One option for running commands automatically after the install is to use the Installation Customization Tool. See "Create a Chain Installation to Run Additional Programs" on page 44.)

Two tools are available for managing and moving database content—the Export/Import Utility and the Copy ICS Database Utility.

NOTE: If you configure and deploy settings using the Management and Security Server, path configuration is included with each downloaded session and these path settings are automatically added to the user's database. This eliminates the need to configure and deploy the database as a separate step. For details, see "Create Sessions using the Administrative WebStation" on page 56 and "Deploy Sessions Saved to the Management Server" on page 58.

Export/Import Utility

You can use the InfoConnect Export/Import Utility to export data from any InfoConnect database into a text (`*.ini`) or comma-separated value (`*.csv`) and to import data from either of these file formats into an InfoConnect database. You can also create a detail file that provides information about each field in the exported files (such as the maximum number of bytes allowed in each field, the type of data that each field can contain, etc.)

You can use this utility to perform a number of tasks:

- Create a backup copy of your InfoConnect database so that you can easily restore it should your original database become deleted or corrupted.
- Edit InfoConnect paths in an exported `.ini` or `.csv` file that you can subsequently import into an InfoConnect database.
- Export path information from multiple InfoConnect databases and then import the data into a single master database.

To launch the Export/Import Utility User Interface

- Run `expimp32.exe`. You can run this program by entering `expimp32` in the "Search programs and files" box in the Windows Start menu or from a Command window.

To run the Export/Import utility from the command line, run `expimp32.exe`. It supports the following command line parameters.

NOTE

- Unless you include the /S parameter, the Export/Import Utility dialog box appears, displaying the values specified by the command line parameters.
- All tables in the database are included by default.
- Unless you specify otherwise, an `ini` file is the default format, empty tables are not included in the data file, and a detail file is not created.

`/D` *filename*	Export the specified data file. The file is created in the current directory unless you specify a different drive and directory. A file extension is not needed.You can include either the **/D** or the **/I** command line parameter. If you include both, only the **/D** command line parameter is used.

`/I filename`	Import the specified data file. The file is imported from the current directory unless you specify a different drive and directory. A file extension is not needed. You can include either the **/D** or the **/I** command line parameter. If you include both, only the **/D** command line parameter is used.
`/A directory`	Specifies the location of the InfoConnect database to be exported or imported. If you omit this command line parameter, the database specified by the Windows registry is used.
`/FC`	Use csv format for the data file.
`/FI`	Use ini format for the data file.
/OD	Create a detail file. If you include the **/S** command line parameter, you must include both the **/D** and the **/OD** command in order to create a detail file. The detail file will have the same name as the data file, but will have a `*.dtl` extension.
`/OE`	Include empty tables in the data file.
`/OT`	Include empty tables in the detail file.
`/S`	Run in silent mode (no dialog box or message box appears). To run the utility in silent mode, you must also include either the **/D** or the **/I** command line parameter.
`/B1`	Use a 16-bit INFOConnect database.

For example, the following command exports the current database. It shows no user interface and creates a file called `icdata.ini`.

```
expimp32 /S /D c:\icdata.ini
```

The following command imports content from the icdata.ini file into the current database

```
expimp32 /S /I c:\mypath\icdata.ini
```

Copy ICS Database Utility

Getting there

- Run `copics32.exe`. You can run this program by entering `copics32` in the “Search programs and files” box in the Windows Start menu or from a Command window.

Use the Copy ICS Database Utility to create a copy of an InfoConnect database that is identical to the original database except for the name of the location of the executable files. This can be helpful if you share your InfoConnect products on multiple file servers and want a copy of the same database on each server, with the only difference being the name of the server where the executable files are located.

You can use this utility in conjunction with the Export/Import Utility to help install your InfoConnect products throughout a large network. For example, once you install the products on one file server, you can use the Copy ICS Database Utility to create multiple databases that include only information about the products that have been installed. Then you can use the Export/Import Utility to add appropriate path information to each of the databases. In this way, an administrator in one central location can create databases for multiple file servers.

NOTE: For the Copy ICS Database Utility to work properly, each InfoConnect library registered in the database must exist in the location that you want to specify for the executable files. In other words, the target location must be a mapped directory on the PC running this utility *and* it must contain all of

the libraries registered in the InfoConnect database.To determine the names of the registered libraries, run the InfoConnect Manager and click **Libraries** on the left, select a library in the list, and then click **Examine**.

To copy an InfoConnect database

1. Run the Copy ICS Database Utility.

   You can run this program by entering `copics32` in the “Search programs and files” box in the Windows Start menu or from a Command window.
2. If **InfoConnect Database To Copy** does not display the name of the database that you want to copy, click **Browse** and select the desired database from the local drive or any available network location.
3. Specify the location where you want the database to be copied by clicking **Browse** next to **Destination For InfoConnect Database**.
4. In the **New InfoConnect Directory** text box, type the location (that is, drive and folder or UNC name) of the executable files that you want to use in the copy of the database that you are creating.
5. Click **Copy**.
6. Repeat steps 2 through 6 for each database that you want to copy.

Related Topics

- “Running Copy ICS Database from the Command Line” on page 21

Running Copy ICS Database from the Command Line

Run Copy ICS Database from the command line using `copics32.exe`, which is installed to the InfoConnect program folder. It supports the following command line parameters.

NOTE: If **/D** and **/N** are both included on the command line, the Copy ICS Database Utility dialog box does not appear when you run the executable file.

Parameter	Function
`/I` *filename*	Specifies the name of the InfoConnect database to copy. Be sure to include the correct drive and folder. If you omit the /I parameter, the database associated with the Windows system running this utility is used automatically.
`/D` *destination*	Specifies the folder where the copy will be created.If you omit the /D parameter, the Copy ICS Database Utility runs, displaying the values for any other command line parameters that you have specified.
`/N` *newdir*	Specifies the location of the executable files that will be specified in the copy of the database.If you omit the /N parameter, the Copy ICS Database Utility runs, displaying the values for any other command line parameters that you have specified.
`/B1`	Uses a 16-bit InfoConnect database.If you omit the /B1 parameter, the 32-bit database is used automatically.

Example

To copy your own database to the `USER1` directory on file server F: and change the location of the executables to `F:\INFOCONNECT`, you would type the following on the command line:

```
COPICS32.EXE /D F:\USER1 /N F:\INFOCONNECT
```

Session Documents

Terminal session settings are saved to session documents. Session documents are specific to each terminal type (`*.ialc`, `*.iuts`, `*.it27`, `*.rd3x`, `*.rd5x`, or `*.rdox`). (The options available depend on your InfoConnect Desktop product.)

For ALC, UTS, and T27 sessions, session documents include a link to a path that includes required connection information. Path definitions are saved in the InfoConnect database.

For 3270, 5250, and VT sessions, the session documents include all host connection information.

In addition to basic connection information, a number of session customization options are available. These include themes (to change display options such as font and color), keyboard maps, mouse maps, hotspots, quickpads, and ribbon (or menu) customization. By default these customizations are saved to separate files and a pointer to the customization file is saved to the session document. It is also possible to save sessions as compound documents that include these customizations.

- "Document Settings" on page 22
- "Compound Documents" on page 23
- "Session Templates" on page 24

Document Settings

Document settings are specific to each terminal type and can be configured from the **Document Settings** dialog box.

To open the Document Settings dialog box

1. Start a terminal session.
2. Open the **Document Settings** dialog box.

   The steps depend on your user interface mode:

Ribbon or InfoConnect Browser	With a session open, from the **Quick Access Toolbar**, click  .
TouchUX	With a session open, tap the Gear icon  and then select  **Document Settings**.
Classic MDI	With a session open, go to **Options** > **Settings**

The Document Settings options available depend on your session type.

Changes you make to the following are always saved in the session document: **Host Connection**, **Terminal Configuration**, **File Transfer**, **Productivity**, **Printer Settings**.

Changes you make to the following are saved by default to separate customization files: **Themes**, **QuickPads**, **Hotspots**, **Ribbon**, **Keyboard Map**, **Mouse Map**. These settings are included in the session document if you save it as a compound document.

Session documents are saved to the InfoConnect user data folder (page 86). Associated customization files are saved to subfolders in the user data folder.

Deploying session settings

To ensure that users can find their sessions and that these sessions include all customizations, save your sessions as compound documents and install them to the InfoConnect user data folder (page 86). When you deploy session documents to this folder, users will see the sessions listed when they open documents from the Workspace without having to browse their file system.

- If you deploy session documents to a non-default location, ensure that you have configured it as a trusted location. You can provide easy access to these files by configuring shortcuts to launch the sessions directly.
- If you do not save session settings in compound documents, all required customization files must be deployed along with your session files to the correct folder location(s).

Deploying sessions using the Installation Customization Tool

You can use the Installation Customization Tool to create a companion package that installs your session documents and optionally creates shortcuts to launch the sessions. See “Create a Companion Package to Install Customized Settings Files” on page 46.

An advantage of deploying settings using the Installation Customization Tool is the ability to modify the Setup program to include your customizations. See “Customize the Setup installation” on page 69.

Deploying sessions using the Management and Security Server

If you have installed the Micro Focus Host Access Management and Security Server, you can use it to manage and deploy session documents. Deploying this way provides several advantages:

- Manage sessions centrally and update session settings as needed.
- Limit session access to specific users or groups using a directory server (LDAP/Active Directory).
- Use the Security Proxy to encrypt session data and enforce access control.

See “Manage Sessions using the Management and Security Server” on page 55.

Compound Documents

When you save a session as a compound document all customizations are included in a single file. This means that your compound file will include all the settings in any associated theme, keyboard map, mouse map, hotspot, ribbon, or QuickPad file. This option enables administrators to deploy session files with all required customizations included in a single file.

NOTE: If you do not save session settings in compound documents, all required customization files must be deployed along with your session files to the correct folder location(s).

To save an individual session as a compound document

1. Open a terminal session and make the modifications you want to include with this session.
2. Open the **Save As** dialog box.

   The steps depend on your user interface mode.

User Interface Mode	Steps
Ribbon	From the **File** menu, select **Save As**.
InfoConnect Browser	From the **InfoConnect** menu, select **Save As**.
TouchUX	Under **FILE**, tap **Save As**.
Classic MDI	From the **File** menu, select **Save As**.

3 For **Save as type**, select the compound option for your session type, then click **Save**.

To save all sessions as compound documents

1 Open the **Workspace Settings** dialog box. (page 25)
2 Click **Configure Workspace Defaults**.
3 Under **Workspace**, select **Save session as compound document**.

Session Templates

After you configure a session document, you can share and reuse your settings by saving the document as a template. Templates provide an untitled copy of the original, giving you a quick and easy way to create pre-configured documents, while ensuring that your original file remains unchanged.

To create a session template

1 Open the session document that you've configured.
2 Save the session as a template.

The steps depend on your user interface mode.

Ribbon	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**.
Classic MDI	From the **File** menu, select **Save As Template**.

3 Name the template file with an `.rsft` extension.

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.

Deploying templates

Deploy templates in the same way you deploy session documents. (See "Deploying session settings" on page 23.) Install these files to the `Templates` folder:

InfoConnect user application data folder`\Templates\`

Templates saved to this location appear in the **Create New Document** dialog box, under **User-defined**.

Related Topics

- “Where to Deploy Customized Files” on page 47
- “Files Used by InfoConnect” on page 80
- “Deploy Sessions Saved to the Management Server” on page 58

Workspace Settings

Workspace settings affect all terminal session and Web page documents opened in the InfoConnect Workspace. For example, you can:

- Select the user interface mode.
- Specify what actions occur when users open the InfoConnect Workspace and when they close a session.
- Specify which help system to use (locally installed or on the web).
- Configure trusted locations.
- Configure privacy filters.
- Configure Centralized Management using the Micro Focus Management and Security Server.

To configure Workspace settings

- Open the **Workspace Settings** dialog box.

  The steps depend on your user interface mode.

Ribbon	From the **File** menu, click **InfoConnect Workspace Settings** (under the Recent Documents list).
InfoConnect Browser	On the InfoConnect menu, choose **Settings** and then **InfoConnect Workspace Settings**.
TouchUX	Tap the Gear icon and then select **InfoConnect Workspace Settings**.
Classic MDI	From the **Options** menu, select **Global Preferences**.

Most Workspace settings are controlled by the `Application.settings` file. Options in the Information Privacy dialog box are controlled by `PCIDSS.settings` and `PrivacyFilters.xml`. Default files are installed to:

InfoConnect program folder`\Configuration\`

Customizations you make are saved to the following location, and these override the default:

InfoConnect user application data folder`\`

For example, you could use the following procedure to deploy InfoConnect using the Classic MDI user interface.

To configure an installation that uses classic menus

1. Open the **InfoConnect Workspace Settings** dialog box.
2. Click **Configure User Interface**.
3. For **User interface mode**, select **Classic MDI** and click OK.

This saves your changes to the `Application.settings` file in your InfoConnect user application data folder (page 86).

4. Close and reopen the Workspace to view the change.
5. Include the modified `Application.settings` file in your deployment.

Deploying Workspace Settings

To deploy user-specific Workspace settings install `Application.settings` to the InfoConnect user application data folder (page 86).

To deploy Workspace settings for all users, install `Application.settings` to the InfoConnect global application data folder (page 86). The installed settings file is copied to the user application data folder when the user opens the Workspace.

Deploying Workspace settings using the Installation Customization Tool

You can use the Installation Customization Tool to create a companion package that installs the `Application.settings` file. Two options for creating companion packages are available:

- "Create a Companion Package to Install Customized Settings Files" on page 46. Use this procedure to add files to a companion package. This option allows you to install existing files that you have already created and tested. With this approach, you manually set the destination location for the installed files.
- "Use "Modify User Settings" to Configure Workspace Settings" on page 52. Use this procedure to start the InfoConnect Workspace from the Installation Customization Tool. You can then configure your custom settings. When you click **OK** in the Workspace dialog box, the Workspace window closes and the modified settings are added to the companion package you are creating. With this approach the Installation Customization Tool automatically determines the correct location for installing the files.

An advantage of deploying settings using the Installation Customization Tool is the ability to modify the Setup program to include your customizations. See "Customize the Setup installation" on page 69.

Deploying Workspace settings using the Management and Security Server

If you have installed the Micro Focus Host Access Management and Security Server, you can use the Package Manager to upload companion install packages that you have created using the Installation Customization Tool or other MSI creation tools. This tool enables you to designate which packages to install for specific users or groups in your directory server (LDAP/Active Directory).

See "Deploy MSI Packages from Management and Security Server" on page 65.

Related Topics

- "Configure Trusted Locations" on page 36
- "Protect Data and Information Privacy" on page 36
- "Where to Deploy Customized Files" on page 47
- "Files Used by InfoConnect" on page 80

Locking Down Settings

You can restrict user access to almost any of the InfoConnect settings or controls. For example, you can prevent users from changing the host address that a session connects to, or from running a macro. Individual permissions are merged in the following order (from highest to lowest):

- Group Policy – user
- Group Policy – machine
- Local access files (`*.access`)

In this Section

Restrict Access using Permissions Manager

You can use the InfoConnect Permissions Manager to restrict access to InfoConnect features. After you select the features you want to disable using this tool, your specifications are saved in `*.access` files that you can deploy to users. You can run Permissions Manager directly, or by launching it from the Installation Customization Tool.

Access file templates installed to InfoConnect program folder`\Configuration`. The list of available templates depends on which InfoConnect product you have installed.

This File	Controls access to…
`actions.access`	InfoConnect actions
`application.access`	InfoConnect Workspace settings
`ialc.access`	ALC terminal settings
`it27.access`	T27 terminal settings
`iuts.access`	UTS terminal settings
`rd3x.access`	3270 terminal settings
`rd5x.access`	5250 terminal settings
`rdox.access`	VT terminal settings

To set access with Permissions Manager

1. On a workstation to which you have installed InfoConnect, log on as administrator and in the InfoConnect install folder, run `AccessConfig.exe`.
2. When prompted to create a new permission file, or edit an existing one, choose **Create new permission file**.
3. When prompted with a list of access file templates, choose the type of permission file to create.
4. Under **Groups**, select the type of setting to control access to.
5. In the **Items** box, in the **Accessibility** field set the security level you want for the selected feature.

   Full - All users can configure the item.

Restricted - Only Administrators of the system can configure the item. These items have the Windows user access shield added to their icons: 

Read-only - No users of the system can configure this item. These items appear grayed-out in the user interface.

6 If you are configuring terminal session access you will see a pane with **Additional security options**. Select how to control session file encryption.

7 Deploy the customized `*.access` files.

Deploying Permissions Manager access files

To deploy user-specific access settings, install your customized `*.access` file(s) to the InfoConnect user application data folder (page 86). User-specific deployment is available for all `*.access` files. You can use the Installation Customization Tool to create a companion package to install these files. See “Create a Companion Package to Install Customized Settings Files” on page 46.

You can install some access configuration (actions and Workspace settings) for all users of the system. To do this install `actions.access and/or application.access` file(s) to the InfoConnect global application data folder (page 86). Settings files in this location are copied to the user application data folder when the user opens the Workspace. To make these changes from the Installation Customization Tool you can use the **Modify User Settings** feature. When you use this approach, the tool automatically determines the correct location to install the required files. See “Use “Modify User Settings” to Change Access Settings” on page 54.

NOTE

- Be sure to set file permissions on `*.access` files that you deploy to prevent users from deleting, replacing, or editing them.
- To deploy files to the *version* folder, your deployment tool must allow you to install the companion installer package as the user.
- Setting session encryption options in an `*.access` file affects only the associated session type. For example, limiting users to opening only encrypted session files in `rd3x.access` only affects 3270 terminal session files, and not 5250 session files.
- When accessing a setting via an API, such as executing a macro, a setting with restricted access cannot be modified. (When attempting to set a restricted setting via an API, an error is logged.)

Control Access with Group Policy

As an administrator, you can limit users' ability to modify their workspace or session documents by setting permissions from the Microsoft Group Policy Management Console using group policy templates.

InfoConnect installs a set of group policy templates (ADM and ADMX files) to the following directory:

InfoConnect program folder`\Configuration\GroupPolicy`

ADM files contain the Group Policy definitions and resource strings in the same file. Reflection provides the following ADM Group Policy files.

This file	Controls access to
`ACTIONS.adm`	Actions
`APPLICATION.adm`	InfoConnect Workspace
`ReflectionWorkspace.adm`	Root-level ADMX file

NOTE: This directory also includes the `ReflectionPCIDSS.adm` file. This file is used to configure information privacy through Group Policy and is not used to control access. If you have installed a Pro product, you will also see files for configuring 3270, 5250, and VT sessions.

ADMX files are divided into language-neutral files (`.admx`) and language-specific resource files (`.adml`), available to all Group Policy administrators. These factors allow Group Policy tools to adjust their UI according to the administrator's configured language. (In InfoConnect Desktop, only US English files are included.)

Install and Test Group Policy Settings

Before you deploy group policy definitions, set and test them on a local test machine.

To install ADM files on a local test machine

1. Copy all `.adm` files

   From:

   InfoConnect program folder`\Configuration\GroupPolicy\ADM\`

   To:

   `C:\Windows\inf`
2. Open Group Policy Object Editor (`gpedit.msc`)
3. Under either **User Configuration** or **Computer Configuration**, Right-click on **Administrative Templates** and select **Add/Remove Templates**.
4. Click **Add**, select the ADM files you need to add, and then click **Open**.

   The added ADM files are listed in the Add/Remove Templates dialog box, in the **Current Policy Templates** list. Click **Close**.
5. Under either **Computer Configuration** or **User Configuration**, browse to **Administrative Templates** | **Classic Administrative Templates (ADM)** | **Reflection Desktop**.
6. In the Group Policy Management Editor, navigate to the setting or feature you want to configure.
7. Enable the Group Policy settings to which you want to restrict access.

NOTE: Registry keys are added when policy settings are **Enabled**. When **Not Configured**, no key is present. When a setting is **Disabled**, the key is still present, and it's data is set to 0x00000000. The data is 0x00000004 when enabled.

For more about using ADM files to set group policy, see *Add or remove an Administrative Template (.adm file)* (http://technet.microsoft.com/en-us/library/cc739134.aspx).

5 Configure Security

Secure Connections

InfoConnect supports a number of secure protocols. The protocols available, depend on you session type.

	ALC	T27	UTS	IBM 3270	IBM 5250	VT	HP	FTP Client
FIPS Mode	X	X	X	X	X	X	X	X
PCI DSS	X	X	X	X	X	X		
SSL/TLS	X	X	X	X	X	X	X	X
SSH						X	X	X
Kerberos		X	X	X	X	X	X	X
SOCKS				X	X	X	X	X

This topic provides information about deploying configuration for some encrypted connection types. For additional information, see Secure Connections in the InfoConnect product help.

In this Section

Digital Certificates and Reflection Certificate Manager

You can configure certificate authentication for both Secure Shell and SSL/TLS connections.

- 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.
- 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.

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.

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.

You can 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, 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 Manager Store**

  This store is used only by Micro Focus 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.

Reflection Certificate Manager

Use the Reflection Certificate Manager to manage configure certificates for use exclusively by InfoConnect. Settings and certificates are saved to files in Windows personal documents folder\Micro Focus\Infoconnect\.pki.

You can deploy certificates and settings per-user or for all users of the system. These settings are not included in compound documents

- User-specific location: Windows personal documents folder`\Micro Focus\InfoConnect\.pki\`
- Global location: `\ProgramData\.pki`

The procedures for opening the Certificate Manager depend on your product and session type.

NOTE: For InfoConnect Airline products that run Windows services (this includes some Airline transports, PTR, and Airlines Gateway), the certificates need to be accessible from the SYSTEM account. This means that these certificates must be in a public documents location rather than a user-specific one.

From the Secure Shell Settings dialog box

1. Open the **Reflection Secure Shell Settings** dialog box.
2. On the **PKI** tab, click **Reflection Certificate Manager**.

From the Security Properties dialog box

1. Open the **Security Properties** dialog box.
2. On the **SSL/TLS** tab, select **Use SSL/TLS Security**.
3. Click **Configure PKI**.
4. Click **Reflection Certificate Manager**.

From the InfoConnect TCP/UDP Path Options dialog box

1. Set **Security type** to something other than **No Security**.
2. Click **PKI Settings**.
3. Click **Reflection Certificate Manager**.

SSL/TLS Connections

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.

- In ALC, UTS, and T27 sessions, the SSL/TLS connection settings are included in the path.
- In 3270, 5250, and VT sessions, SSL/TLS connection settings are saved to the session document.
- In the FTP Client, SSL/TLS connection settings are saved to the FTP Client settings file (`*.rfw`).

To configure SSL/TLS in most ALC, UTS, and T27 sessions

1. Open the **TCP/UDP Path Options** dialog box for the path used for the connection.
2. Set **Security type** to the version you require.
3. Click **PKI Settings** to open the **PKI Settings** dialog box. From this dialog box, you can configure certificate revocation settings, and whether host name matching is required. You can also use it to access the **Reflection Certificate Manager** to configure host and user certificates for the connection.

To configure SSL/TLS in ALC or UTS sessions that use the MATIP transport

1. Open the **MATIP Host Configuration** dialog box for the path used for the connection.
2. Set **Security type** to the version you require and configure certificate revocation settings, and whether host name matching is required.
3. Click **Reflection Certificate Manager** to configure host and user certificates for the connection.

To configure SSL/TLS in 3270, 5250, or VT terminal sessions

1. Open the **Create New Document** dialog box, select a session template and click **Create**.
2. Select **Configure additional settings,** and then click **OK**.
3. 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**.
4. From the **Security Properties** dialog box, select the **SSL/TLS** tab, and select **Use SSL/TLS security**.
5. Click **Configure PKI** to configure certificate settings.

To configure SSL/TLS in FTP Client Sessions

1. Start the FTP Client.

2. In the **Connect to Site** dialog box, select a site and click **Security**.
3. Click the **SSL/TLS** tab and select **Use SSL/TLS security**.
4. Click **Configure PKI** to configure certificate settings.

Secure Shell Connections

Secure Shell connections are available for VT terminal sessions and to configure SFTP transfers using the FTP Client.

By default, Secure Shell connections use public key authentication for the host and username/password authentication for the user. If you configure non-default settings, they are saved for each host (or ssh configuration scheme) to the ssh configuration file. This file is used for all connections (VT sessions and the FTP Client). You can deploy these settings per-user or for all users of the system. These settings are not included in compound documents.

- User-specific configuration: Windows personal documents folder`\Micro Focus\InfoConnect\.ssh\config`
- Global configuration: `\ProgramData\Micro Focus\InfoConnect\ssh_config`

To configure a secure terminal session using Secure Shell (SSH)

1. Open the **Create New Document** dialog box, select the **VT Terminal** template and click **Create**
2. In the **Create New** dialog box, under **Connection**, select **Secure Shell** and click **OK**.
3. Click **OK**.

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.
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**.

   When you click **OK**, changes to the default settings are saved in the Secure Shell `config` file in Windows personal documents folder`\Micro Focus\Infoconnect\.ssh`

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. Under **Host Connection**, click **Configure Connection Settings**.
3. Under **Connection Options**, select **Handle SSH user authentication in terminal window**.

Known Hosts

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. If you select Always in response to this prompt, the host key is saved in a file called `known_hosts`, which is created in Windows personal documents folder`\Micro Focus\Infoconnect\.ssh`. After the host key is added, InfoConnect Desktop can authenticate the server without requiring user confirmation, and the unknown host prompt does not appear again.

To prevent end-users from seeing the unknown host message you can deploy a known hosts file per-user or for all users of the system. These settings are not included in compound documents

- User-specific file: Windows personal documents folder\Micro Focus\InfoConnect\.ssh\known_hosts
- Global file: \ProgramData\Micro Focus\InfoConnect\ssh_known_hosts

PKI Auto Sign-on

You can configure VT and UTS terminal sessions to use the PKI Auto Sign-on Add-On Client product, which allows the use of a Common Access Card (CAC) or other smart card for authentication.

To use PKI Auto Sign-on, the PKI Auto Sign-on host module must be installed on your host server. This module can be used to verify that a client is in control of a CAC or other smart card, and to extract the Distinguished Name (DN) from the certificate used for authentication. The DN, or some substring contained in the DN, can then be used to provide service to the authorized user. PKI Auto Sign-on is designed to provide a validated identity even via a shared host login, that is, the identity comes from the smart card itself, not from the host user ID.

When a session is configured to use PKI Auto Sign-on:

- System administrators can set up sessions to use a shared log-on that provides the host application with a strongly validated identity directly from a CAC.
- Host programmers can get the strongly validated DN of a user in control of a CAC. The programmers can then extract information from the DN and use it as an identifier to authorize access (for example, to the CAC-bearer's health records).

Prerequisites

- The PKI Auto Sign-on host module must be installed on the host server.

To create an SSH-enabled VT session that uses PKI Auto Sign-on

1. Create a new VT session document.
2. Click **Configure additional settings** and then click **OK**.
3. In the **Settings** dialog box, under **Host Connection**, select **Set up Connection Security**.
4. On the Reflection Secure Shell Settings dialog box **General** tab, under **User authentication**, deselect Public Key.
5. On the **PKI** tab, click **Reflection Certificate Manager**.
6. On the **PKCS #11** tab, click **Add**.
7. In the **PKCS #11 Provider** dialog box, browse to the Provider DLL required to access your CAC.
8. In the `.ssh/config` file for this session document, add the appropriate PKIC prompt string configured on the server. The following example shows an entry for a prompt “Starting PKI Validation...”

   ```
   PKICPrompt "Starting PKI Validation..."
   ```

   When you are done, the file should look like this:

   ```
   Host myHostNameRSAAuthentication noPubkeyAuthentication noconnectionReuse
   noPKICPrompt "Starting PKI Validation..."#EndHost
   ```

Protect Data and Information Privacy

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.

What do you want to do?	See
Define locations from which you can safely open (and store) documents.	“Configure Trusted Locations” on page 36
Mask sensitive data (such as credit card numbers) with privacy filters.	“Configure Information Privacy” on page 36
Control access to the Reflection API and control the execution of actions invoked by a macro or API call.	“Configure API and Macro Security” on page 38

Configure Trusted Locations

A trusted location is a directory that is designated as a secure source for opening files. By default, InfoConnect allows users to open documents only in directories specified as trusted locations. The default trusted locations are the InfoConnect program directory, the user’s personal documents directory, and the InfoConnect user application data folder.

To change the default trusted locations

1. Open the **InfoConnect Workspace Settings** dialog box. (page 25)
2. Click **Specify Trusted Locations**.

   This opens the **Specify Trusted Locations** dialog box, which you can use to add additional trusted locations.
3. Edit the trusted locations list and click **OK**. Changes you make using this dialog box are saved to the `Application.settings` file.
4. Deploy the modified `Application.settings` file (page 26).

Configure Information Privacy

With InfoConnect Information Privacy, you can protect sensitive data such as credit card Primary Account Numbers (PANs), phone numbers, and US Social Security numbers. Information Privacy allows you to configure InfoConnect so that the sensitive data is not displayed on the screen or in productivity features, such as Screen History. It also allows you to require secure connections.

To set up Information Privacy using Workspace Settings

1. Start the InfoConnect Workspace and open the Workspace Settings dialog box (page 25).
2. Under Trust Center, click **Set Up Information Privacy**.
3. 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 P**rivacy Filter Redaction Rules** and **Privacy Filters**.
Redact credit card Primary Account Numbers (PANs) to meet PCI DSS requirements. 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.	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**.

4 When you have finished configuring Information Privacy, click **OK**.

Edits to privacy filters are saved to `PrivacyFilters.xml`. All other **Set Up Information Privacy** settings are saved to `PCIDSS.settings`. These files are saved to the same location as the `Application.settings` file and deployed in the same way.

5 Deploy the modified files (page 26).

To set up Information Privacy with Group Policy

1 Copy the following files to the central store as follows:

Copy these files	To

`ReflectionPCIDSS.admx`
 	
`ReflectionWorkspace.admx`
 	
in
 	
InfoConnect program folder`\Configuration\GroupPolicy\ADMX`
	`%systemroot%\PolicyDefinitions`

`ReflectionPCIDSS.adml`
 	
`ReflectionWorkspace.adml`
 	
in:
 	
InfoConnect program folder`\Configuration\GroupPolicy\ADMX\en-US`
	`%systemroot%\PolicyDefinitions\en-US`

2 Open the Group Policy Object Editor (`gpedit.msc`).

3 Under either the Computer Configuration or User Configuration branch, browse to **Administrative Templates** | **Reflection Workspace** | **Information Privacy**.

4 In the **Information Privacy** panel, select and edit the policy settings.

NOTE: If you want to include the default regular expressions used for Custom Detection Rules and Custom Exception Expressions, you must add these expressions through the Group Policy editor. For detailed instructions, see Technical Note 2576 (http://support.attachmate.com/techdocs/2576.html): Adding Regular Expressions for Custom Detection Rules and Custom Exception Expressions to Group Policy.

Configure API and Macro Security

Settings limiting API and macro functionality are available from the **Workspace Settings** dialog box.

To set up API and macro and security

1. Start the InfoConnect Workspace and open the Workspace Settings dialog box (page 25).
2. Under **Trust Center**, click **Set Up API and Macro Security**.
3. Configure the **API settings** as follows:

To	Select
Prevent custom applications from accessing this installation.	**Disable .Net API**
Determine if legacy macros are supported, and to determine which legacy API has preference for the GetObject() method used to retrieve API COM objects. (Reflection supports multiple APIs, but can accept GetObject() calls for only one type of legacy API object at a time.)	**Legacy API preference**

4. Under **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.

To	Select
Control restricted actions with User Account Control (UAC).	**Require elevated rights; do not execute on XP**
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.	**Execute the action**

5. When you have finished configuring the API and macro security settings, click **OK**. Changes you make using this dialog box are saved to the `Application.settings` file.
6. Deploy the modified `Application.settings` file (page 26).

6 The Installation Customization Tool

The Micro Focus Setup Program uses standard MSI-based deployment technologies for Windows systems. The Setup Program provides a standard user interface. You can also use Setup to run the Installation Customization Tool, which provides tools to:

- Customize the installation using transforms (`*.mst`)

  Because multiple transforms can be created for a given install package, you can create customized installations for separate departments or groups of users, each represented in a transform file.

- Create companion installation packages (*.msi) to install additional files.

  Use companion packages to install any of the customized files described in Chapter 4, “Customize InfoConnect,” on page 17.

  NOTE: Using the **Modify user settings** feature, you can launch InfoConnect directly from the Installation Customization Tool and configure your custom settings. Settings added this way are automatically installed to the correct location.

  Companion packages show up as independent entries in the Windows list of installed applications, and can be installed and uninstalled independently of InfoConnect.

In this Chapter

Setup for Customized Deployments Using the Installation Customization Tool

To create customized deployments using the Installation Customization Tool, set up as follows:

1. Stage the Installation Files on a Server.
2. Install InfoConnect on Your Administrative Workstation (page 40)
3. Set Up a Shortcut to the Installation Customization Tool (page 41)

Stage the Installation Files on a Server

To set up the installation files on a server:

- Copy the package files that you extract from the download site.

  -OR-

- Use the Setup program to create an administrative installation point.

When you create an administrative installation point, the files required by the installer are copied to the location you designate and expanded so you can see the file content.

NOTE: An administrative installation point is the recommended format for applying service packs, updates, and hotfixes using the patch utility. When you run the patch utility, it asks for your administrative installation path. If you apply the patch to the original compressed package, the utility won't overwrite the uncompressed files.

You can create an administrative image using the Setup program user interface or from a command line. If you have already installed InfoConnect on your workstation, you must use the command line to create the Administrative installation. When you start Setup on a system that already has InfoConnect installed, the Setup program detects your installation and presents you with options to repair, reinstall, or remove the product—the option to create and administrative install image is not available

To create an administrative install point using the Setup user interface

---

NOTE: For this procedure, use only the **Advanced** and **File Location** tabs. Configurations made from other tabs will be ignored.

---

1. Double-click `setup.exe` file to start the installation program.
2. Review and accept the license agreement and click **Continue**.
3. From the **Advanced** tab, select **Create an Administrative install point on a server**.
4. Click **Continue**. This opens the File Location tab. Browse to the location to use for the administrative installation image.

   Specify the path to a network share as a UNC path. For example: `\\share_name\administrative_install_point`.
5. Click **Install Now**.

To create an administrative installation point using the command line

1. Open a Command window.
2. Run `setup.exe` using the following syntax:

   `path_to_setup_file``\Setup.exe /install /admin TARGETDIR=`*`UNC_path_to_administrative_installation_point`*

   For example:

   ```
   c:\icpackage\setup.exe /install /admin TARGETDIR=\\teamshare\infoconnect
   ```

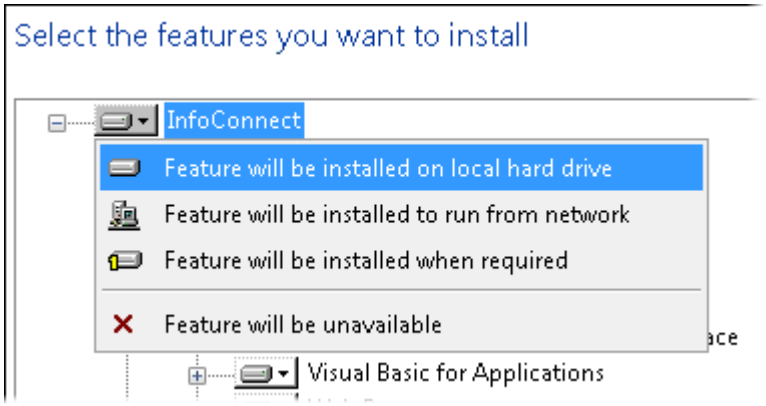
Install InfoConnect on Your Administrative Workstation

You can install InfoConnect by running Setup from your original download location or your administrative installation point.

To install InfoConnect on your workstation

1. Double-click `setup.exe` file to start the installation program.
2. Review and accept the license agreement and click **Continue**.

3 Use the **Feature Selection** tab to select the features you want to install. To install all features, you can click the arrow on the **InfoConnect** icon (the top item in the tree) and select **Feature will be installed on local hard drive**. After you determine which features users require can use the Installation Customization Tool to customized Setup on your installation point to install just those features.



4 Click **Install Now**.

NOTE: For this installation, use the default installation option to **Install to this PC**.

Set Up a Shortcut to the Installation Customization Tool

By default, the Installation Customization Tool can be opened only from a command line. To save yourself time starting this tool, you can optionally create a desktop shortcut and set the shortcut properties to open it.

To set up a desktop shortcut

1 On your administrative installation point, right-click on the `setup.exe` file and choose **Create Shortcut**.

2 Right-click on the shortcut and choose **Properties**.

3 In the **Target** field, add the /admin option to the end of the command line. For example:

```
\\myServer\adminInstallPoint\setup.exe /admin
```

NOTE: Make sure that the path in the Target field is referenced with a Uniform Naming Convention (UNC) format. Do not use drive letters in the path name. Using drive letters can cause problems when you try to use the shortcut on other workstations.

---

4 Rename the shortcut and save it on the desktops of your workstation and on the server that you are using for your administrative installation point.

Create Setup Customization Files (Transforms)

Setup customization files are standard MSI transform files (*.mst). Transforms can be used with any installation that starts with setup.exe or with command-line installs (used by many deployment tools).

You can use transforms to:

- Specify which features will be installed.
- Customize start menu shortcuts.
- Run additional programs (such as companion installation packages) automatically before or after `Setup.exe`.

To create transforms using the Installation Customization Tool, start the tool using your shortcut (page 41), or use the following syntax on a command line:

path_to_setup`\setup.exe /admin`

This displays a **Select Customization** dialog box. To create a transform, choose **Create a new Setup customization file for the following product**. To edit an existing transform, choose **Open an existing Setup customization file or Companion installer**.

In this Section

Create a Transform that Specifies which Features to Install

You can specify which features are installed to your end users by using the Installation Customization Tool to create a transform file that modifies the installation. In addition, you can choose from three options for not installing an item; advertising it, not installing it, and permanently blocking it so that users can not install it later.

To select features, components, and languages to install

1. From your administrative installation point, open the Installation Customization Tool from a shortcut (page 41) or by typing the following command line:

   `path_to_setup``\setup.exe /admin`
2. Select **Create a new Setup customization file for the following product**.
3. Under **Features**, choose **Set Feature Installation States**.
4. Use the feature tree to configure each feature's installation state as follows:

Choose	To do this
Feature will be installed on local hard drive	Add a feature to the installation.
Feature will be installed when required	Advertise a feature.
Feature will be unavailable	Leave a feature uninstalled. End users will still be able to select the item and install it from Windows **Programs and Features** or **Add/Remove Programs**.
Feature will be hidden from view	Leave a feature uninstalled and hidden. End users will not be able to install the item, and it will not be visible in the Windows **Programs and Features** or **Add/Remove Programs**.

5 Click **File** > **Save As.**

Your changes are saved to a transform (*.mst) file.

6 Apply the transform to your installation (page 45).

Modify Setup Properties

You can modify existing INFOConnect setup properties, such as setting the default application folder, or add your own properties to the install. An example of an installer property is ARPHELPLINK, which sets the URL used by the support link in Windows Programs and Features. For a list of installer properties, see “InfoConnect MSI Properties” on page 72.

Yu can modify installer properties in both transforms (`.mst`) and companion installers (`.msi`). The procedure below describes creates modifications in a transform file.

CAUTION:

- InfoConnect uses two properties to configure the user data location. If you configure a non-default user data location, you must set both `USERDATALOC_CUSTOM_PATH` and `WRQ_USERDIR` to the same path.
- Do not overwrite existing properties unless you fully understand how the changes affect your install. Setting properties to improper values can break the install.

To modify installation properties

1 From your administrative installation point, open the Installation Customization Tool from a shortcut (page 41) or by typing the following command line:

path_to_setup\setup.exe /admin

2 Select **Create a new Setup customization file for the following product**.

3 On the Installation Customization Tool navigation pane, select **Modify setup properties**.

4 In the **Name** box, use the drop-down list to select commonly-used public properties that are standard to the Windows Installer. Select an item in the list to see a brief description of the selected property. For additional information about Windows Installer properties, see Microsoft's Windows Installer Guide (http://msdn.microsoft.com/en-us/library/windows/desktop/aa372845(v=vs.85).aspx). Some Micro Focus products.

InfoConnect supports. additional properties that do not appear in the drop-down list. You can configure these properties by manually entering the property name. See “InfoConnect MSI Properties” on page 72.

5 From the **File** menu, choose **Save As**.

6 Apply the transform to your installation (page 45).

Create a Chain Installation to Run Additional Programs

Use this procedure to set up a chain install that automatically runs companion install packages (`*.msi`) before or after the primary installation, or that launches other scripts or programs.

To chain installations and programs

1 From your administrative installation point, open the Installation Customization Tool from a shortcut (page 41) or by typing the following command line:

```
path_to_setup\setup.exe /admin
```

2 Select **Create a new Setup customization file for the following product**.

3 From the Installation Customization Tool navigation pane, choose **User Interface**, then select **Use this customization with interface installs using setup.exe**.

4 From the Installation Customization Tool navigation pane, choose **Add installations and run programs**.

5 Click **Add**.

The **Add/Modify Program Entry** dialog box opens.

6 In the **Target** list, enter or select the folder where the program `.exe` file or the `.msi` file resides, and then enter the executable to run; for example:

```
msiexec.exe
```

7 Under **Arguments**, enter the command-line arguments to execute; for example:

```
/i My_installation.msi
```

8 Choose one of the following options to specify when to run the program.

- Run this program after the base product has been installed.
- Run this program before the base product has been installed.

NOTE: For most cases, select **Run this program after the base product has been installed**. If you select this option before the base product has been installed and the program fails, INFOConnect is not installed.

---

9 Repeat these steps to add other programs or `.msi` files.

10 To change the execution sequence, use the arrows next to Move (at the bottom left area of the pane. To remove a program from the list, select it in the list and click **Remove**.

11 Save your transform and apply this transform to your installation (page 45).

Apply a Transform to your Installation

You will need to deploy your transform with the primary installation. Transforms can be used with any install started with the InfoConnect Setup program (`setup.exe`) or with command-line installs (used by many deployment tools). The installer can only apply transforms during an installation. The following procedure describes how to add your transform file to installations started with the InfoConnect Setup program.

To add the transform to an install started with setup.exe

1. From your administrative installation point, open the Installation Customization Tool from a shortcut (page 41) or by typing the following command line:

   path_to_setup\setup.exe /admin

2. Select **Open an existing Setup customization file or Companion installer**, and then click **OK**.
3. In the **Open** dialog box, browse to select your transform (`.mst`) file.
4. Click **User interface** and select **Use this customization with interactive installs using setup.exe**.

   When you save your transform with this option selected, the Installation Customization Tool automatically updates the `setup.ini` file to apply your transform to the InfoConnect installation by adding the following line to the `[Setup]` section:

   ```
   CustomTransform=<your_transform.mst>
   ```

5. From the **File** menu, click **Save**. (If **Save** appears dimmed, click **Exit** and you will be prompted to save the file.)

   The transform can now be deployed to end users via the `setup.exe` file. (Users can run `setup.exe`, the `setup.exe` file can be called from a script, or `setup.exe` can be initiated from a command line.)

Related Topics

- “Deploy using the Setup command line” on page 70
- “Create Setup Customization Files (Transforms)” on page 42
- “Deploy InfoConnect from MSI Command Line” on page 71

Use Companion Packages to Install Customized Settings

Companion packages are standard MSI files (`*.msi`). Use this option to install InfoConnect customization files or other files required by end users.

To create transforms using the Installation Customization Tool, start the tool using your shortcut (page 41), or use the following syntax on a command line:

path_to_setup\setup.exe /admin

This displays a **Select Customization** dialog box. To create a companion package, choose **Create a new Companion installer**. To edit an existing transform, choose **Open an existing Setup customization file or Companion installer**.

In this Section

- “Create a Companion Package to Install Customized Settings Files” on page 46

- “Where to Deploy Customized Files” on page 47
- “Predefined System Folders” on page 51
- “Use “Modify User Settings” to Configure Workspace Settings” on page 52
- “Use “Modify User Settings” to Change Access Settings” on page 54

Create a Companion Package to Install Customized Settings Files

You can use the Installation Customization Tool to install customized InfoConnect settings. To do this, you will create one or more companion installer packages to install your custom settings files on end-user systems.

Before you begin

- Configure, test, and save the settings you want to deploy to users. (See “Customize InfoConnect” on page 17.)
- Create an administrative installation image (page 39).

To create your companion installer package

1. From your administrative installation point, open the Installation Customization Tool from a shortcut (page 41) or by typing the following command line:

   `path_to_setup\setup.exe /admin`
2. From the **Select Customization** dialog box, select **Create a new Companion installer** (or open an existing MSI), and then click **OK**.
3. From the navigation pane, click **Specify package information**. Use this panel to specify the program name your package will use in the Windows **Programs and Features** or **Add or Remove Programs** list. Also specify your organization name.
4. From the navigation pane, click **Specify install locations**. Specify whether you want to install files for all users (the default) or just the user who installs the package you are creating.
5. From the navigation pane, click **Add Files**, browse to the file, and click **Open.**
6. To change the default location of the added file, select it from the list, and from the **Add Files To** drop-down menu, select from the available locations. These locations are determined by the specified **Installation type** on the **Specify install locations** pane.

   For a list of common files and file locations used by InfoConnect, see “Where to Deploy Customized Files” on page 47.

   For an explanation of available folder options (such as [CommonAppDataFolder] and [PersonalFolder]), see “Predefined System Folders” on page 51.
7. (Optional) With the added file selected, select the **Include shortcut** check box to install a shortcut that opens the installed file. For example, if you're adding a UTS Terminal document file (`*.iuts`), you can install a shortcut to the Windows **Start** menu that will open this file and make the connection.

   NOTE: You can use the **Configure shortcuts** pane later to verify or edit the shortcut location.

   ---
8. Choose **File** > **Save As** and enter a name for your installer file (for example `MyCustomSettings.msi`).
9. (Optional) Chain this installer (page 44) to have it run automatically with the Setup program.

Related Topics

- “Where to Deploy Customized Files” on page 47
- “Session Documents” on page 22
- “Workspace Settings” on page 25

Where to Deploy Customized Files

Files are installed either to a global location or a user-specific location, not both. If you want to install files to both locations, you must create two companion installer packages.

Make sure to choose the location from the **Specify install locations** pane *before* adding files to your companion package.

NOTE: The deployment locations below are for default installations.

- “Database and PTR settings” on page 47
- “Workspace settings” on page 48
- “Reflection FTP Client settings” on page 50
- “Shared security settings” on page 50

Database and PTR settings

File Type	Deployment location
InfoConnect database (`ic32.cfg`)	`[CommonDocumentsFolder]\Micro Focus\InfoConnect\`
PTR route configuration (`ptr32.ini`)	`[CommonDocumentsFolder]\Micro Focus\InfoConnect\`

Workspace settings

File Type	Deployment location

Session
`.ialc`
`.iuts`
`.it27`
`.rdox`
`.rd3x`
`.rd5x`
`.urlx`
Layout
`.rwsp`
	For all users
	Use any location you have configured as a trusted location and defined as the default data directory in the InfoConnect workspace (`Application.settings`) file. For example:
	`[CommonAppDataFolder]\Micro Focus\InfoConnect\`
	For the user who installs
	The default user folder is:
	`[PersonalFolder]\Micro Focus\InfoConnect\`

File Type	Deployment location

Workspace settings
`Application.settings`
`PCIDSS.settings`
`PrivacyFileters.xml`
`Frame.settings`
	Note: You can also use **Modify User Settings** to deploy workspace settings.
	For all users
	`[CommonAppDataFolder]\Micro Focus\InfoConnect\Workspace\<version>`
	For the user who installs
	`[AppDataFolder]\Micro Focus\InfoConnect\Workspace\<version>`.

Permissions Manager settings `.access`	Use the same locations as the Workspace settings. Note: You can also use **Modify User Settings** to deploy access settings.

Keyboard map (`.xkb`)
Mouse map (`.xmm`)
Hotspots (`.xhs`)
Custom UI (`.xuml`)
Themes (`.themex`)
QuickPad (`.rqpx`)
	NOTE: If you save your session documents as compound documents, these settings are included and you do not need to deploy them separately.
	For all users
	Install to a folder (`Keyboard Maps`, `Mouse Maps`, `Hotspot maps`, `CustomUI`, or `Themes`) in any trusted location that exists on the users' workstations and is defined as the default data directory in the InfoConnect workspace (`Application.settings`) file. For example:
	`[CommonAppDataFolder]\Micro Focus\InfoConnect\Keyboard Map`
	For the user who installs
	The default keyboard folders is:
	`[PersonalFolder]\Micro Focus\InfoConnect\Keyboard Maps`
	The default mouse folder is:
	`[PersonalFolder]\Micro Focus\InfoConnect\Mouse Maps`
	The default hotspot folder is:
	`[PersonalFolder]\Micro Focus\InfoConnect\Hotspot Maps`
	The default custom UI folder is:
	`[PersonalFolder]\Micro Focus\InfoConnect\CustomUI`
	The default themes folder is:
	`[PersonalFolder]\Micro Focus\InfoConnect\Themes`
	The default QuickPads folder is:
	`[PersonalFolder]\Micro Focus\InfoConnect\QuickPads`

HLLAPI settings (`hllapi.xml`)	**For the user who installs** `[AppDataFolder]\Micro Focus\InfoConnect\Workspace\<version>`.

Reflection FTP Client settings

File Type	Deployment location
rftp.xml	Settings in the .xml settings file are migrated to a settings.rfw file for each user the first time the user runs the FTP Client. Note: You can also use Modify User Settings to deploy FTP Client settings. **For all users** [CommonAppDataFolder]\Micro Focus\InfoConnect **For the user who installs** [PersonalFolder]\Micro Focus\InfoConnect\
settings.rfw	**For the user who installs** The default user folder is: [PersonalFolder]\Micro Focus\InfoConnect\

Shared security settings

File Type	Deployment location
Secure Shell settings	Note that the global filenames are different than the user-specific filenames, although the content may be the same.
	For all users
ssh_config ssh_known_hosts	[CommonAppDataFolder]\Micro Focus\InfoConnect
	For the user who installs
config known_hosts	[PersonalFolder]\Micro Focus\InfoConnect\.ssh
Reflection Trusted Certificate Authorities trust_store.p12 **Reflection Certificate Manager settings** .pki_config	**For all users** [CommonAppDataFolder]\Micro Focus\InfoConnect\.pki **For the user who installs** [PersonalFolder]\Micro Focus\InfoConnect\.pki

File Type	Deployment location

Kerberos settings
`rsckrb5.xml`
	Settings in this location are migrated to the Windows registry for each Windows user the first time the user runs Kerberos Manager or any Reflection client configured to use Reflection Kerberos.
	For all users
	`[CommonAppDataFolder]\Micro Focus\InfoConnect`
	For the user who installs
	`[AppDataFolder]\Micro Focus\InfoConnect\`

Predefined System Folders

When you configure destination locations using Installation Customization Tool, your options include a list of supported Windows system folder properties (http://msdn.microsoft.com/en-us/library/aa372057.aspx?ppud=4). During installation, the Windows installer expands these to show the appropriate location for your operating system. Default system folder locations are shown below.

The list of available folders for adding files to a companion installer depends on whether you are installing for all users (the default) or for individual users. (Configure this option using the **Specify install locations** pane.)

All-user installations

Property name	Default Windows location	Default path using Windows variables
[CommonAppDataFolder]	`C:\ProgramData`	`%programdata%`
[CommonDocumentsFolder]	`C:\Users\Public\Documents`	`%windir%`
[CommonFilesFolder]	`C:\Program Files\Common Files`	`%ProgramFiles%\Common Files`
[ProgramFilesFolder]	`C:\Program Files`	`%ProgramFiles%`
[RootDrive]	`C:\`	`\`
[WindowsFolder]	`C:\Windows`	`%windir%`

Individual user installations

Property name	Default Windows location	Path using Windows variables
[AppDataFolder]	`C:\Users\<user>\AppData\Roaming\`	`%appdata%`
[LocalAppDataFolder]	`C:\Users\<user>\AppData\Local\`	`%localappdata%`
[PersonalFolder]	`C:\Users\<user>\Documents\`	`%userprofile%\documents`
[RootDrive]	`C:\`	`\`
[%UserProfile]	`C:\Users\<user>`	`%userprofile%`

Use “Modify User Settings” to Configure Workspace Settings

You can use the **Modify User Settings** feature in the Installation Customization Tool to deploy Workspace Settings. With this approach, you open the Workspace Settings dialog box from the Installation Customization Tool. The modified settings are automatically saved to your companion file and deployed to the correct directory.

NOTE: You can also create customize the `Workspace.settings` file by launching the Workspace directly, then creating a companion file as described in “Create a Companion Package to Install Customized Settings Files” on page 46.

Before you begin

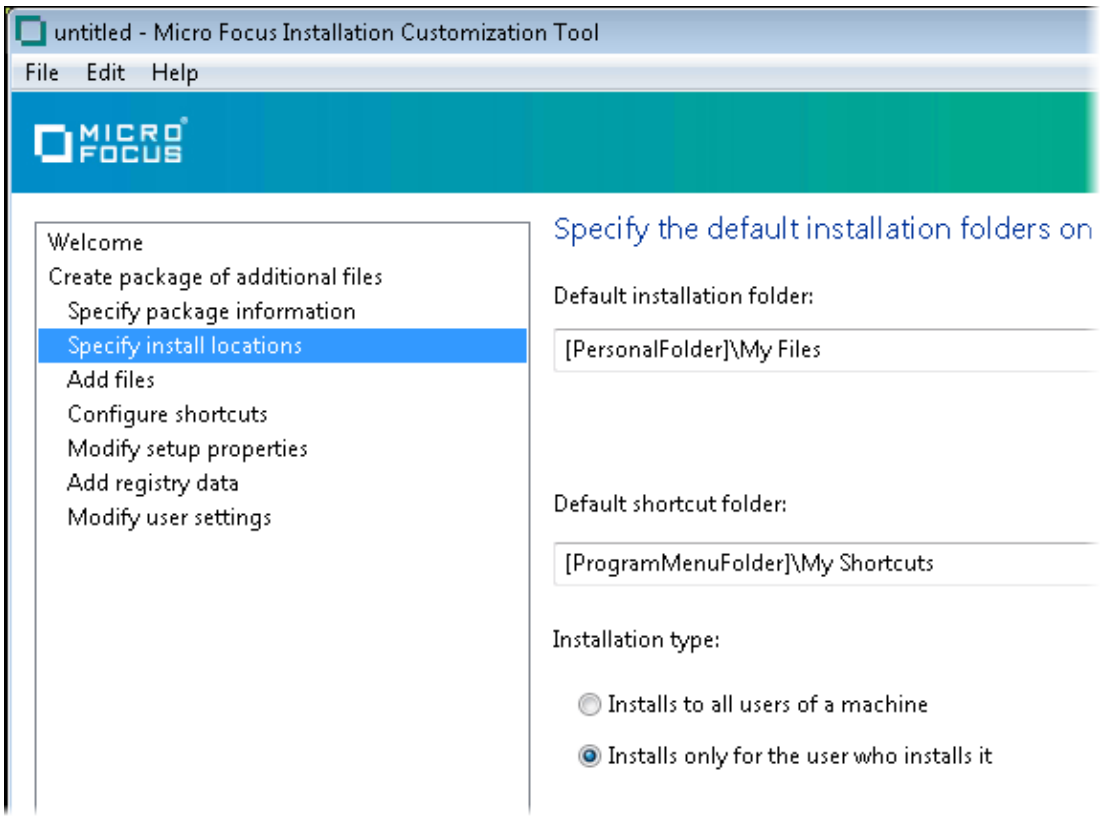
1. Stage the Installation Files on a Server.
2. Install InfoConnect on Your Administrative Workstation (page 40)

To change workspace settings from the Installation Customization Tool

1. From your administrative installation point, open the Installation Customization Tool from a shortcut (page 41) or by typing the following command line:

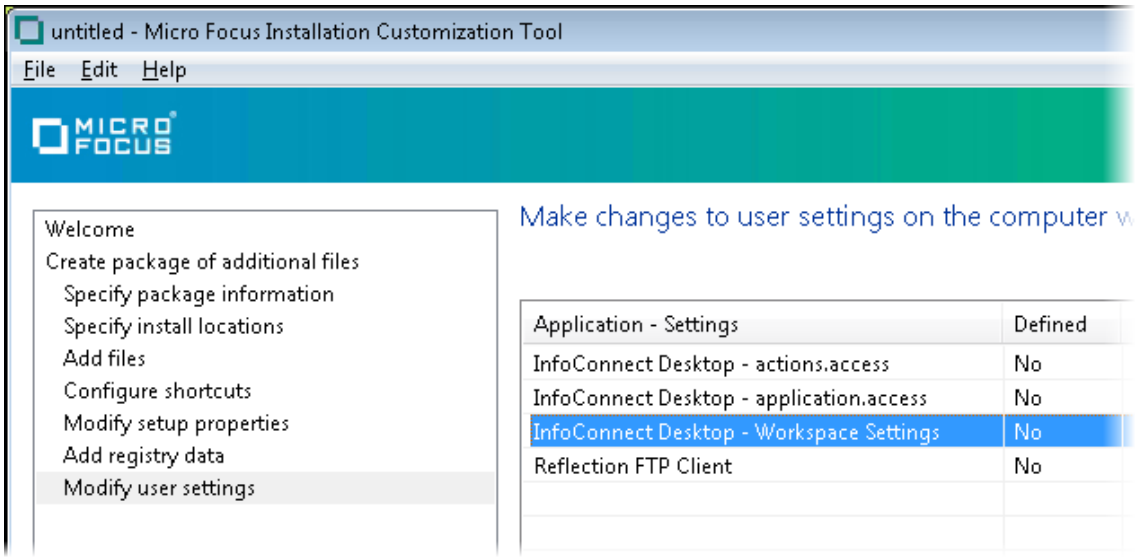
   path_to_setup`\setup.exe /admin`

2. From the **Select Customization** dialog box, select **Create a new Companion installer**, and then click **OK**.
3. From the navigation pane, click **Specify install locations**.



4 Under **Installation type**, select either **Installs only for the user who installs it** (the default), or **Installs to all users of a machine**.

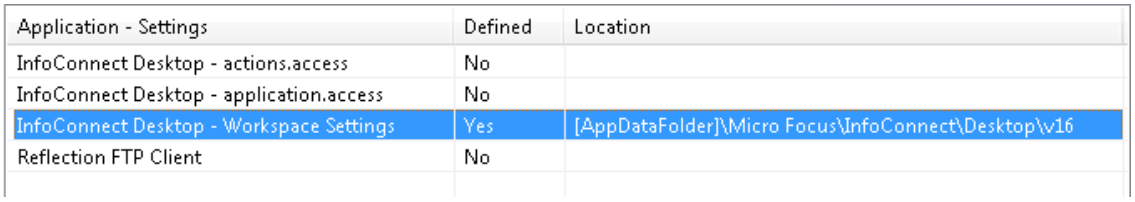
5 On the navigation pane, click **Modify user settings**.



6 From the list of **Application - Settings**, select **InfoConnect Desktop - Workspace Settings** and then click **Define**.

The **InfoConnect Workspace Settings** dialog box opens in a separate window.

7 Select the feature you want to modify. After you make your changes and click **OK**, the Workspace window closes. In the Installation Customization Tool window, under **Location**, you will see where the modified settings will be installed.



8 Repeat steps 6 and 7 to customize additional settings.

9 Save the companion package file (`.msi`) and close the Installation Customization Tool. You can deploy the companion file as it is, or you can edit it to add additional files.

10 (Optional) Use a transform to chain the installation of this package.

Custom settings are automatically saved in the `Application.settings` file. The companion installer file is automatically configured to deploy this file for per-user installs to:

`[AppDataFolder]\Micro Focus\InfoConnect\Desktop\`*`version`*`\`

Or, for all users to:

`[CommonAppDataFolder]\Micro Focus\InfoConnect\Desktop\`*`version`*`\`

Related Topics

- “Workspace Settings” on page 25

Use “Modify User Settings” to Change Access Settings

You can use the **Modify User Settings** feature of the Installation Customization Tool to create a companion package that will lock down access to InfoConnect features. With this approach, you open the Permissions Manager from the Installation Customization Tool. The modified access settings are automatically saved to your companion file and deployed to the correct directory.

NOTE: You can also create your `access` files by launching the Permissions Manager directly, you can deploy them by creating a companion file as described in “Create a Companion Package to Install Customized Settings Files” on page 46.

Before you begin

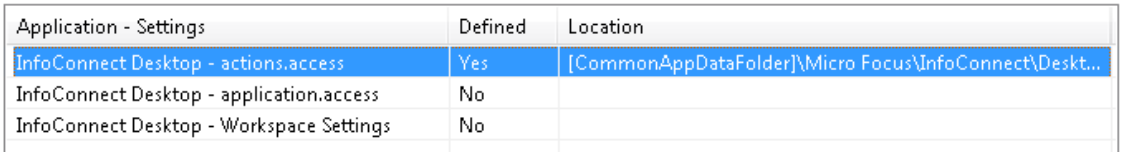
1. Stage the Installation Files on a Server.
2. Install InfoConnect on Your Administrative Workstation (page 40)

To configure access from the Installation Customization Tool

1. From your administrative installation point, open the Installation Customization Tool from a shortcut (page 41) or by typing the following command line:

   path_to_setup\setup.exe /admin

2. From the **Select Customization** dialog box, select **Create a new Companion installer**, and then click **OK**.
3. In the **Select Customization** dialog box, select **Create a new Companion installer**.
4. On the left pane, select **Specify install locations**. Under **Installation type**, select **Installs only for the user who installs it**.
5. In the left pane, select **Modify user settings**. Select one of the `.access` options and click **Define**.
6. Under **Application - Settings**, select the *.access file you want to edit and click De
7. Permissions Manager opens in a separate window. Set the Accessibility level for the features you want to change. When you click **Finish**, Permissions Manager closes. In the Installation Customization Tool window, under **Location**, you will see where the modified `.access` file will be installed. This example shows a companion package that is being configured for all users of the machine.



8. From the **File** menu, choose **Save As** and save the companion installer package.

Custom settings are automatically saved in the `Application.settings` file. The companion installer file is automatically configured to deploy this file for per-user installs to:

`[AppDataFolder]\Micro Focus\Reflection\Desktop\`*`version`*`\`

Or, for all users to:

`[CommonAppDataFolder]\Micro Focus\Reflection\Desktop\`*`version`*`\`

7 Manage Sessions using the Management and Security Server

The Micro Focus Host Access Management and Security Server is a separately available product that provides an administrator the means to centrally manage, secure, and monitor users' access to host connections. Management and Security Server features you can use with InfoConnect include the following:

- **Administrative Server**

  The Administrative Server is the central component of Host Access Management and Security Server that enables you to define terminal emulation sessions, and then manage and configure secure settings for those sessions. The Administrative WebStation is the interface for the Administrative Server, where you configure and save settings.

- **Metering Server**

  Use the Metering Server component to monitor the use of terminal sessions including the ability to track the number of connections and total connection time per user.

- **Security Proxy Add-On**

  The Security Proxy acts as a proxy for terminal sessions and provides token-based access control, routing encrypted network traffic to and from user workstations. The Security Proxy Server can be installed on the same server as the Administrative Server or on another system.

- **Terminal ID Manager Add-On**

  The Terminal ID Manager enables you to pool terminal IDs, track ID usage, and manage inactivity timeout values for specific users, thus conserving terminal ID resources and significantly reducing operating expenses. The Terminal ID Manager can be installed on the same server as the Administrative Server or on another system using either the automated installer or a manual installation.

- **Automated Sign-On for Mainframe Add-On**

  Automated Sign-On for Mainframe enables an administrator to configure a connection to the Digital Certificate Access Server (DCAS) on an IBM z/OS mainframe, and then configure their mainframe sessions so that users can access their entitled sessions using a single login, such as with a smartcard. To add Automated Sign-On for Mainframe, you need to install the activation file and configure settings using the Administrative WebStation. Some configuration is also needed on the mainframe.

NOTE: To manage InfoConnect Desktop sessions you need to install and configure Management and Security Server version 12.2 or later.

In this Chapter

- “Deploy MSI Packages from Management and Security Server” on page 65
- “Enable Usage Metering” on page 66

Create Sessions using the Administrative WebStation

You can create and manage InfoConnect sessions using the Management and Security Server Session Manager, which is available from the Administrative WebStation. Sessions that you create this way are saved to the server and can be made available to users from the server and modified at any time.

Requirements

- InfoConnect must be installed on the administrative workstation and on user computers.
- Java must be enabled in the browser you will use to run the Administrative WebStation.
- Management and Security Server must be installed on a server. You will need to know the administrative credentials to log onto the Management Server.

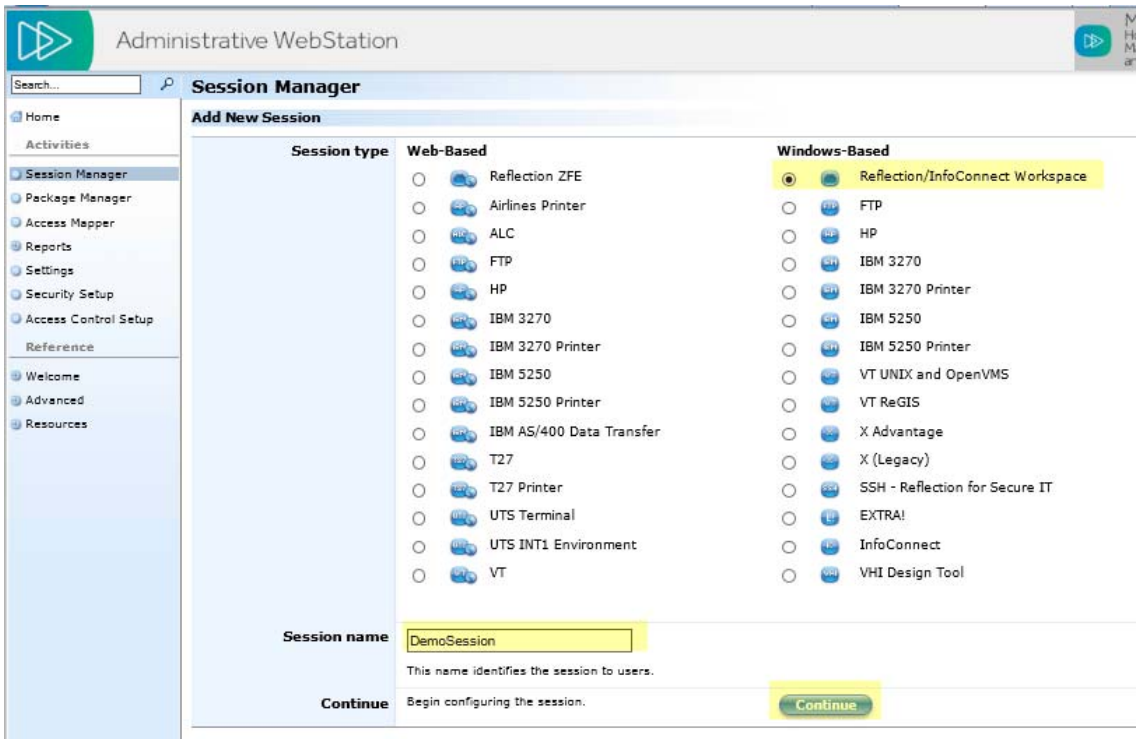
To create a session from the Administrative WebStation

1. From a system running InfoConnect, open a web browser and start Management and Security Server by setting the URL to:

   `http://server:port/mss/AdminStart.html`

   Where *server* and *port* are replaced with the Management Server address. (Port is optional if you installed using the default.)
2. Log in as the server administrator
3. Click **Administrative WebStation**.
4. Select **Session Manager** and click **Add**.

5 From the **Windows-Based** list, select **Reflection/InfoConnect Workspace**. Enter a value for **Session name** and click **Continue**.



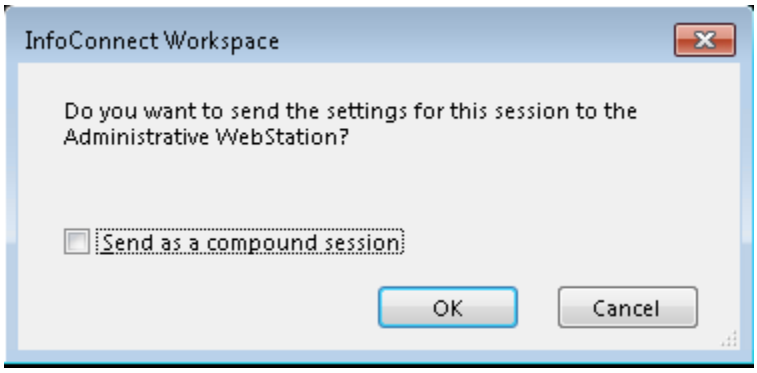
NOTE: The **InfoConnect** option further down in the Windows-Based list is for use with InfoConnect 9.x products.

6 (Optional) Change the defaults for where sessions will be stored on the end user's workstation and whether these files will overwrite existing user files.

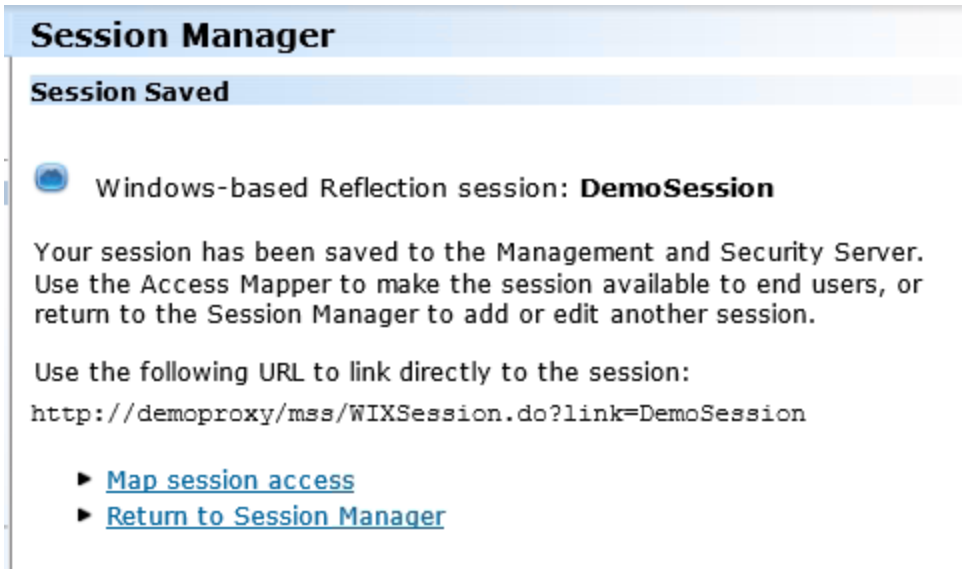
7 Click **Launch**.

InfoConnect opens in Administrative WebStation mode (page 58).

8 Configure your session settings, then save your session. You will see the following prompt asking you if you want to save your settings to the Administrative WebStation. If your session uses associated settings (such as a theme or keyboard map file), select **Send as compound session** to include these settings.



9 Click **OK**, then close the Workspace window. You will see a confirmation that your session has been saved.



10 Click **Map session access** to specify which users have access to the file.

11 Deploy the sessions to end users. See “Deploy Sessions Saved to the Management Server” on page 58.

Administrative WebStation Mode

When you launch InfoConnect from the Management and Security Server Administrative WebStation, the Workspace opens in *Administrative WebStation Mode*. Use this Workspace window to configure sessions for central management.

In Administrative WebStation mode:

- When you save a session, the session is uploaded to the Management and Security Server; it is not saved on your workstation.
- Options to configure the Security Proxy are available; these options are not available when you launch the Workspace directly)

Related Topics

- “Deploy Sessions Saved to the Management Server” on page 58
- “Connect to Hosts using the Security Proxy” on page 59

Deploy Sessions Saved to the Management Server

After you have saved sessions to the Management and Security Server, you can make these sessions available to users who have InfoConnect installed on their workstation. Two options are available: users can obtain sessions by launching a Workspace that is configured for Centralized management, or you can provide web links for users to download and launch sessions.

Before you begin

- Use the Administrative WebStation to create and configure the sessions you want to deploy. (page 55)
- Install InfoConnect on user workstations, including all features required to run the sessions.

To deploy Management Server sessions using Centralized Management

Centralized Management must be configured in the user's Workspace. To do this:

1. Open the Workspace Settings dialog box.
2. Under **Workspace Settings**, click **Configure Centralized Management**.
3. Select **Enable Centralized Management** and specify the **Server URL**. You can use the **Test Connection** button to confirm that the server is running and available

The steps above can be done manually after the installation, or you can include this configuration by deploying customized Workspace settings. (See "Deploying Workspace Settings" on page 26.)

Once Centralized Management has been configured, each time the user opens the Workspace:

- InfoConnect contacts the server and prompts for user credentials (if required by the server).
- New or updates sessions that are available to the user are downloaded to the user data directory.
- For any session that requires path configuration, a session-specific database is downloaded to the user data directory. Path information in this database is added to the InfoConnect database when the user launches the downloaded session.

Users can now launch these sessions the same way they launch locally created sessions.

To deploy Management Server sessions using a web browser

NOTE: To access sessions using a web browser, users must have Java installed and enabled in the browser.

---

1. Point users to a URL to access sessions. The URL can be either of the following:
   - The server URL (for example `http://myserver/mss`).

     With this options, users log in with their credentials, then see a links list showing all sessions available to them. When they open a session on the list, the InfoConnect Workspace starts and opens the selected session.
   - A direct link to the session. (for example `http://myserver/mss/WIXSession.do?link=MySession`).

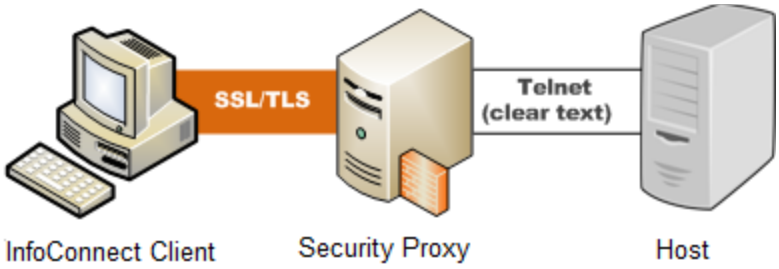
     With this option, users are prompted for required credentials when they click the link. The InfoConnect Workspace then starts and opens the session.

Connect to Hosts using the Security Proxy

The Security Proxy acts provides additional features to authorize users and encrypt session data. Several configuration options are available.

Client Authorization

When using the default configuration for the Security Proxy, users are authorized using security tokens. Transmitted data between the client and the Security Proxy is encrypted; transmitted data between the Security Proxy and the host is not. The Security Proxy server should be installed behind a corporate firewall when used in this mode.

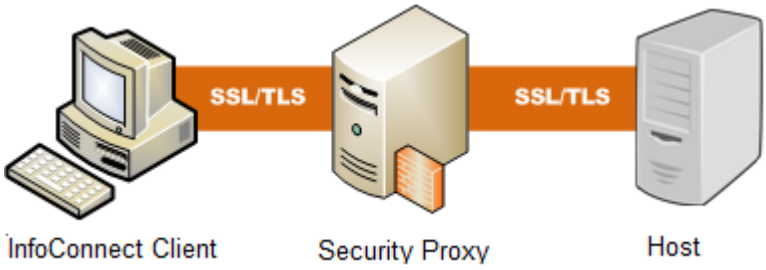


Pass Through

When configured as a Pass Through Proxy, the Security Proxy passes data to the destination host without regard to content (that is, it ignores any SSL handshaking data). You can secure data traffic using SSL between the client and the destination host by enabling SSL user authentication on the destination host. When using a Pass Through proxy, client authorization is not an option.

End-to-End SSL/ TLS Security

This option is available for 3270, UTS, T27, and some ALC sessions. It combines user authorization with SSL security for the entire connection. Single sign-on capability using the IBM Express Logon (page 73) is also supported, provided the host supports SSL.



Create a Session that Connects through the Security Proxy

Use this procedure to create an Reflection emulation session that connects to the Security Proxy and requires a user token for client authorization. Client authorization is a configurable option in Security Proxy that is enabled by default.

This feature is supported for Telnet connected sessions.

Requirements

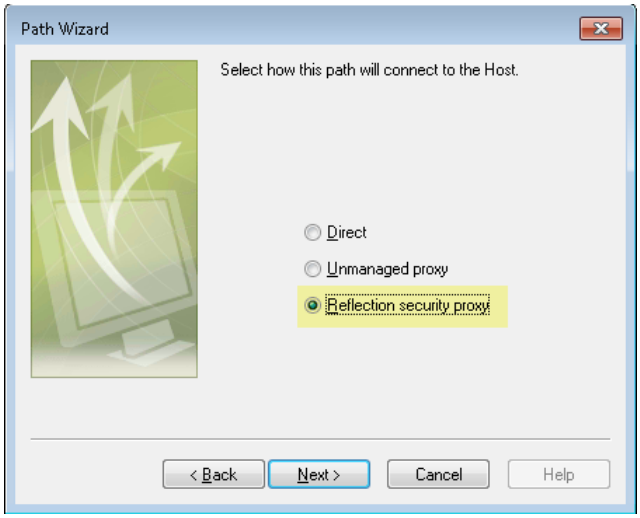
- A Micro Focus Management and Security Server, with a Security Proxy Configured. For end-to-end encryption, the Security Proxy must be configured to require **Client authorization**. (It can optionally be configured to require **Client authentication**. For client authentication, you can use a single certificate or two separate client certificates on each server (Security Proxy and destination host).

- Digital certificates. To successfully establish the SSL/TLS sessions between the client and the Security Proxy, and the client and the destination host, you may need multiple digital certificates. End-to-end connections require two certificates and SSL/TLS handshakes — one for the client/proxy server connection and another for the client/host connection.
- On the administrator's workstation, installation of InfoConnect Desktop and a browser (with Java enabled)

To configure an ALC, UTS, or T27 session to use the Security Proxy

1. Start the Administrative WebStation and launch a session. (See “Create Sessions using the Administrative WebStation” on page 56.)

   InfoConnect opens in Administrative WebStation mode.
2. From the **Create New Document** dialog box, select an ALC, UTS, or T27 terminal template and click **Create**.
3. In the **Create New Document** dialog box, click **Create Path** to start the Path Wizard. Respond to the prompts for your connection type until you see the following dialog box. (These options appear only when you are running in WebStation mode.)



4. Select **Reflection security proxy** and click **Next**. You can use the next dialog box to configure your connection to the host through the proxy.

5 Click **Next** and continue through the wizard to complete the configuration. When you click **Finish**, the session opens in InfoConnect.

6 Finish configuring your session, then save the new session and close the Workspace.

The session file is saved to the Management and Security Server.

Configure an IBM terminal session to use the Security Proxy

1 Start the Administrative WebStation and launch a session. (See "Create Sessions using the Administrative WebStation" on page 56.)

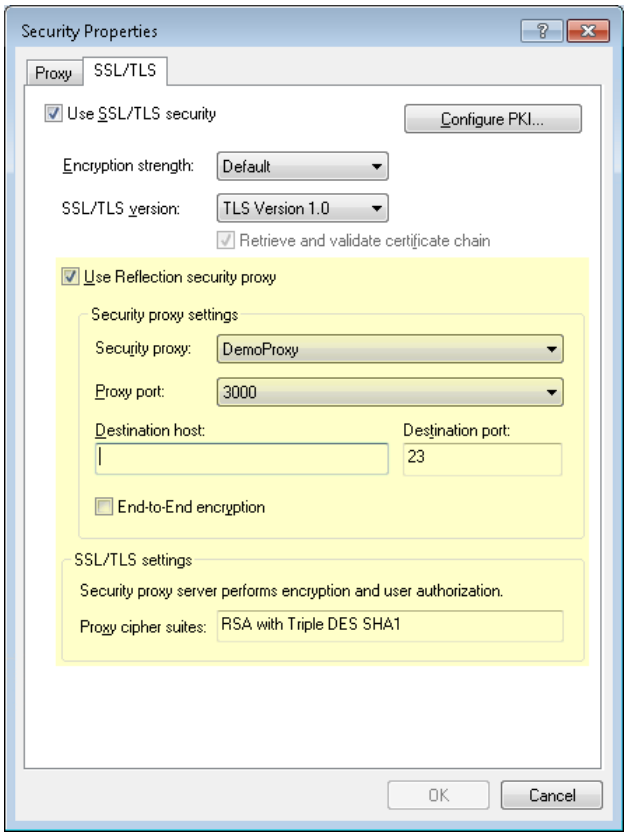
InfoConnect opens in Administrative WebStation mode.

2 From the **Create New Document** dialog box, select a 3270 or 5250 terminal template and click **Create**.

3 Select the check box **Configure additional settings**, and click **OK**.

4 Under **Host Connection**, click **Set Up Connection Security**, then click **Security Settings**.

5 In the Security Properties dialog box, select **Use SSL/TLS security**, then select **Use Reflection security proxy**. Use this dialog box to configure your connection to the host through the proxy.



6 Finish configuring your session, then save the new session and close the Workspace.

The session file is saved to the Management and Security Server.

Related Topics

- “Deploy Sessions Saved to the Management Server” on page 58

About Certificates

Server Certificates

Destination SSL hosts and Security Proxy servers typically have server certificates already installed. Each of these server certificates must be trusted by the client. The client will trust a server certificate if:

- It is signed by the certificate authority that is trusted by the client, or
- It is self-signed and imported into the trusted root certificate store where InfoConnect can find it.

To use a single server certificate for both the destination host and the Security Proxy, do one of the following:

- Configure the InfoConnect session not to enforce having the server name in the certificate match the server in the connection. (In IBM sessions, in the **PKI Configuration** clear **Certificate host name must match host being contacted**, which is enabled by default. For ALC, UTS, and T27 sessions, the setting in the Path Wizard is called **Verify host name against host certificate**, and it is not enabled by default.)
- (Recommended) Create a certificate that uses the destination host address for the **Subject Common Name** and the Security Proxy address for the **Subject Alternative Name**.

Client certificates

Certificates used for client authentication must be signed by a certificate authority that is trusted by both the Security Proxy and the destination host's SSL server.

Express Logon also requires that the client certificate used to authenticate on the TN3270 server be registered with RACF. (For details, see the documentation that came with the 3270 server.)

For more details on configuring SSL and creating certificates on the host, see Technical Note 1759 (http://support.attachmate.com/techdocs/1759.htm) and Technical Note 1760 (http://support.attachmate.com/techdocs/1759.htm).

Configure Sessions to use ID Manager to Assign Terminal IDs

From InfoConnect, you can establish host connections using the ID Manager, provided by Management and Security Server

The ID Manager configures and monitors a pool of resource IDs that can be used to establish a host session. Resource IDs work in place of the required address or identifier for a particular terminal type. This eliminates the need to configure a terminal ID (GPID or LU) for each and every client. You can use ID Manager with 3270, 5250, UTS, ALC and T27 terminal emulation sessions.

When a session is configured to use ID Manager, InfoConnect obtains an ID before the session connects and then holds on to the ID throughout the session. When the session disconnects, the ID is returned to its pool. A different ID may be used the next time the session connects.

Requirements

- A Micro Focus Management and Security Server, with a Terminal ID Manager configured.

- You need to know the complete URL for the ID Manager server. For example, `https://servername:port/tidm`. If you use the default port for http (80) or https (443), the colon and port number are not required.
- You need to know the parameters that the ID Manager requires to allocate an ID (for example the pool name).

To use the Path Wizard to configure ID Management

1. From the InfoConnect Workspace, open the **Create New Document** dialog box.
2. Select an ALC, UTS, or T27 terminal template and click **Create**.
3. Click **Create Path**.
4. When the **Use ID Management** check box appears in the Path Wizard, select it and continue.
5. On the following page, select **Use Reflection ID Management Server** and in the **Reflection ID Management Server URL** box, enter the URL for the ID Manager server.
6. Click **Next** to continue.
7. Under **Obtain ID using**, select the options that are required by the ID Manager to allocate an ID, such as pool name. (Options that aren't supported by InfoConnect are unavailable.)
8. Click **OK** and complete the session creation.

To use the Database Editor or InfoConnect Manager to configure ID Management

1. Open the path configuration dialog box for any of the following Unisys and Airlines transports:
   - ALC (MATIP, UDPFRAD, TCPFRAD or SABREIP)
   - T27 (TCPA)
   - UTS (INT-1 or MATIP)
2. Select the **Use ID Management** check box and click **Configure ID Management**.

To configure ID Management for connections to IBM hosts

1. Open a 3270 or 5250 terminal session.
2. Open the **Document Settings** dialog box.
3. Under **Host Connection**, click **Set Up ID Management**.

Deploy MSI Packages from Management and Security Server

Use the Package Manager to upload companion install packages (`*.msi`) to the Management and Security Server for deployment to specified users or groups. Companion install packages can be created using the Installation Customization Tool or other MSI creation tools.

Packages assigned to a user are automatically deployed to a user's desktop when the user logs on to the Management and Security Server or starts an InfoConnect Workspace session with Centralized Management enabled.

To upload a package

1. From a system running InfoConnect, open a web browser and start Management and Security Server by setting the URL to:

   `http://server:port/mss/AdminStart.html`

Where *server* and *port* are replaced with the Management Server address. (Port is optional if you installed using the default.)

2. Log in as the server administrator
3. Click **Administrative WebStation**.
4. Click **Package Manager** on the left.
5. Click **Add** and then **Browse** to locate the `.msi` file you want to add or update. You can optionally add a description about the package.
6. Click **Save** to upload the package to the Management Server.

To deploy a package to users

Use the Access Mapper to specify users to which the package will be deployed.

- Use **Access Mapper** in the Administrative WebStation to provide access to specific users or groups. If the Management and Security Server has been configured to integrate with your enterprise directory using LDAP, the Access Mapper operates in a different mode. For more information, refer to the documentation included with Management and Security Server.

  After you make the package available to a user, the next time that user accesses the Links List, or launches an InfoConnect Workspace session with Centralized Management enabled, the package contents are copied to the user's computer to the locations specified in the MSI package.

To update or replace a package

To update an MSI package on the Management and Security Server, you essentially replace it with an updated file of the same name.

1. Make your changes to the MSI package and save it using the same name.
2. From Package Manager, click the MSI file that you want to replace.
3. Click **Browse**, select the modified package, and then click **Open**.
4. In the **Description** field, enter a version number or some other indicator that the package contents have changed, and then click **Save**.

Enable Usage Metering

The Management and Security Server Metering Server allows administrators to track InfoConnect sessions and determine how many client workstations use the product. Metering can also be used to limit the number of concurrent users that can access a host at any given time.

Requirements

- A Micro Focus Management and Security Server, with a Terminal ID Manager configured.
- You need to know the complete URL for the Metering server. The syntax is: `http://[host name]:[port]/[metering server context name]/meter.do`. (If you used the default port, you can omit the colon and port number.)

  For example:

  `http:/Myserver.com:80/mssmeter/meter.do`

You can use group policy to enable metering after the product is installed, or use the Installation Customization Tool (page 39) to configure metering as part of the initial installation.

To configure metering via group policy

1. Download the file ReflectionPolicy.zip (http://download2.attachmate.com/fileinfo.asp?filename=ReflectionPolicy.zip) from the download library.
2. Open Group Policy Object Editor (`gpedit.msc`)
3. Under **Computer Configuration**, right-click on **Administrative Templates** and select **Add/Remove Templates**.
4. Click **Add**, select Reflection.adm file. you need to add, and then click **Open**. The added ADM file is listed in the Add/Remove Templates dialog box, in the **Current Policy Templates** list. Click **Close**.
5. Navigate to **Computer Configuration** > **Administrative Templates** > **Classic Administrative Templates** (**ADM**) > **Reflection Settings** > **Client Metering**.
6. Under **Configure Client Metering**, check the **Enabled** radio button.
7. In the **Metering URL** box, enter the URL of your metering server.
8. Select **Require metering** only if you want to prevent users from launching Reflection when the metering server is not available. (Enabling this setting can be useful when you are creating a trial installation and want to test to see if the metering server is running and available.)

To configure metering using the Installation Customization Tool

1. From your administrative installation point, open the Installation Customization Tool from a shortcut (page 41) or by typing the following command line:

   path_to_setup\setup.exe /admin
2. Select **Create a new Setup customization file for the following product**.
3. In the left pane, click **License and session metering**.
4. Select the checkbox to accept the license agreement on behalf of users.
5. Under **Session Metering**, enter the URL of your metering server.
6. (Optional) If you are going to deploy using the `setup.exe` file in your administrative installation point, click **User Interface** in the left pane, then select **Use this customization with interactive installs using setup.exe**.
7. Save the transform.

8 Deploy InfoConnect

This chapter provides instructions on deploying InfoConnect.

Deploy using the Setup Program

The Setup program (`setup.exe`) is the recommended tool for installing and deploying InfoConnect. You can have end users run Setup themselves, or you can use `setup.exe` on the command line to manage customized automated installations.

Customize the Setup installation

When users launch the Setup program, by default they see the user interface described in “The InfoConnect Setup Program” on page 11. You can use the Installation Customization Tool to customize what happens when users run Setup.

To customize Setup using the Installation Customization Tool

1. From your administrative installation point, open the Installation Customization Tool from a shortcut (page 41) or by typing the following command line:

   `*path_to_setup*\setup.exe /admin`
2. In the left-hand navigation pane, select **Create a new Setup customization file for the following product**.
3. Select License and Session metering and click I accept the terms of the Software License Agreement.
4. In the navigation pane, select **User Interface** and click **Use this customization with interface installs using setup.exe**.

   When you save your transform with this option selected, the Installation Customization Tool automatically updates the `setup.ini` file to apply the transform to the installation by adding the following line to the `[Setup]` section:

   `CustomTransform=*your_transform.mst*`

   You must enable this option if you want to add programs to your installation using the **Add installations and run programs** panel. When you save your transform after using that panel, the tool creates a `[RunPrograms]` section in `setup.ini` with a command to run each added program.

The modifications made to `setup.ini` mean that any installation using `setup.exe` (using either the interactive user interface or using `setup.exe` on a command line) will automatically apply your transform and run any added programs.

5 Under **Select a user interface level**, select one of the following:

None - Displays no interface.

Basic - Displays only a progress bar.

Full - Displays the full Setup program interface.

(Optional) Select **No cancel** to set up the install so that it cannot be canceled after it begins.

6 (Optional) In the navigation pane, select **Set feature installation states** to modify the installed features.

7 (Optional) In the navigation pane, select **Add installations and run programs** to run any companion packages automatically before or after the Setup program.

8 Save your transform.

After you have made these changes, running the Setup program from your administrative installation point (using either the user interface or a command line) will automatically install InfoConnect with your customizations.

Related Topics

- “The Installation Customization Tool” on page 39

Deploy using the Setup command line

You can use the Setup program command line to install InfoConnect from the distribution image, or from an administrative installation image. You can also include command-line options in a batch file to preset installation parameters, and limit user interaction while InfoConnect is installing. You can suppress installation dialog boxes to provide an unattended installation.

To see a list of available command-line parameters

```
setup.exe /?
```

To deploy with default settings

```
setup.exe /install
```

To disable user interaction during the installation

To perform an unattended install that displays a progress bar and disables the Cancel button:

```
setup.exe /install /passive
```

To perform a silent install with no display:

```
setup.exe /install /quiet
```

To deploy InfoConnect and a transform

`setup.exe /install TRANSFORMS=` *myCustomInstall*`.mst`

NOTE: An alternate way to apply a transform is to use the Installation Customization Tool as described above in Customize the Setup installation.

To specify a non-default location for program files

Use the INSTALLDIR property. For example:

`setup.exe /install INSTALLDIR=C:\path`

Deploy with MSI

You can deploy InfoConnect directly from the MSI command line. You can also deploy companion `.msi` files that you have created to contain your custom configuration files.

Deploy InfoConnect from MSI Command Line

Use these procedures to install InfoConnect from a command line with MSI.

To customize your installation, specify Windows Installer properties on the command line or pass them in a transform file. For a list of public properties that are standard to the Microsoft Windows Installer, refer to the Microsoft Windows Installer Guide (http://msdn.microsoft.com/en-us/library/windows/desktop/aa372845(v=vs.85).aspx).

Handling prerequisites in command line installs

If you use `setup.exe` for your install, the setup program checks for any prerequisites required by the features you have selected and installs them automatically.

If you use `msiexec.exe` for your install, prerequisites are not installed automatically. You need to install them separately if they are not already on your users' workstations. You can find installers for the required prerequisites in the Prerequisites folder in the distribution media, or in your administrative installation. The prerequisites you need to install depend on which programs and features you are installing:

- All InfoConnect Workspace features require Microsoft .NET Framework 4.5.1. If you attempt an install using msiexec.exe and this prerequisite is not found, a message displays and the installer stops. To install the .NET framework, run the executable file in Prerequisites\DotNet451.
- The Visual Basic for Applications feature requires Microsoft VBA 7.1. Use the core and language-specific *.msi packages in the Prerequisites\VB71 folder.

Handling upgrades in command line installs

If you are upgrading a previous version of InfoConnect, the prior version must be uninstalled before you can install the current version.

If you use `setup.exe` for your install, the setup program checks for a previous versions of InfoConnect and uninstalls it automatically if one is found. It also preserves your existing data folders. For details, see “The InfoConnect Setup Program” on page 11.

If you use `msiexec.exe` for your install, you must first manually uninstall any earlier versions. If you upgrade these products by deploying the `.msi` file directly and have not removed the earlier version, a message displays telling you to uninstall the older software first.

To deploy InfoConnect “out-of-the-box” directly with MSI

- At a command prompt on a test workstation, change to the directory in which the `.msi` file resides and enter:

  `msiexec /i path_to_administrative_installation_point\yourVersion.msi`

  where *yourVersion*`.msi` is the specific version of the InfoConnect MSI that you downloaded.

To deploy InfoConnect and a transform directly with MSI

- At a command prompt, enter:

```
msiexec /i path_to_administrative_installation_point\yourVersion.msi
TRANSFORMS= yourCustomInstall.mst
```

Deploy a Companion MSI File from the MSI Command Line

You can deploy configuration files that are included in a separate companion installation package. This allows you to deploy and maintain these files between InfoConnect software updates without removing InfoConnect.

NOTE: If you use Management and Security Server, you can upload MSI files to the Package Manager and silently deploy them to users' workstations. See “Deploy MSI Packages from Management and Security Server” on page 65.

To deploy a companion installer package directly with MSI

- At a command prompt, enter:

```
msiexec /i path_to_administrative_installation_point\ your_companion_file.msi
```

To remove a companion installer package directly with MSI

- At a command prompt, change to the directory in which the companion installer package file resides and enter:

```
msiexec /x your_companion_file.msi
```

InfoConnect MSI Properties

The following table lists common properties in the InfoConnect `.msi` file, some of which are used to set default values for installation and global options. These properties can be specified on the command line or passed in by way of a transform file (see “Modify Setup Properties” on page 43). If installation values are not specified and the installation dialog boxes are suppressed, the default values are used.

CAUTION: InfoConnect uses two properties to configure the user data location. If you configure a non-default user data location, you must set both `USERDATALOC_CUSTOM_PATH` and `WRQ_USERDIR` to the same path.

Property	Description
`WRQ_USERDIR=`*`path`*	Sets the location for user data. (Also set USERDATALOC_CUSTOM_PATH)
`COMPANYNAME=`*`organization`*	Sets the organization name.
`INSTALLDIR=`*`path`*	Sets the installation path

Property	Description
USERDATALOC_CUSTOM=Yes|No	Default is *No*. This property only works when USERDATALOCATIONMIN and USERDATALOCATIONMINTWO are set to Custom. If USERDATALOCATIONMIN or USERDATALOCATIONMINTWO is set to Custom., set this value to Yes. In all other cases, set it to No.
USERDATALOC_CUSTOM_PATH=*path*	Only works if USERDATALOCATIONMIN and USERDATALOCATIONMINTWO are set to Custom. Specifies a custom location to store user data. If you replace the user-specific portion of the path with the string userid, when the product is run by a user for the first time, the userid portion of the path is replaced with the logged-in user's ID. This property also supports the string %personalfolder%. This string is replaced with the path to the user's My Documents folder.
USERDATALOCATIONMIN=*value*	Sets the location for user data. (Aso set WRQ_USERDIR) **This value** — **Saves data to** MyDocs — \My Documents\Micro Focus\InfoConnect AllUsersDocDataDir — \Users\Public\Documents\Micro Focus\InfoConnect Custom — User-defined value as follows: When you specify custom for the value, you must include the following two properties: USERDATALOC_CUSTOM=Yes USERDATALOC_CUSTOM_PATH=*pathname*
APPDATALOC_CUSTOM=Yes|No	Default is *No*. This property only works if APPDATALOCATION is set to Custom. In that case, include this property and set the value to Yes.
APPDATALOC_CUSTOM_PATH=*path*	This property only works if APPDATALOCATION is set to Custom. In that case, include this property and for *path*, specify a custom location to store application data. This property supports the string %personalfolder%. This string is replaced with the path to the user's My Documents folder.
APPDATALOCATION=*value*	Sets the location where application data is saved. **This value** — **Saves data to** MyDocs — \My Documents\Micro Focus\InfoConnect AllUsersDocuments — \Users\Public\Documents\Micro Focus\InfoConnect

Property	Description
	`Custom` User-defined value as follows: When you specify `Custom` for the value, you must include the following two properties: `APPDATALOC_CUSTOM=Yes` `APPDATALOC_CUSTOM_PATH=`*`pathname`*

Properties for Transports and Options

You can specify transports or options from the command line if you haven't customized your `.msi` file to install specific transports or options. This is most common for silent or group policy installations. If you do not specify any transports or options, the defaults are installed.

NOTE: You can also add or remove transports after the initial product installation.

To install transports and options from a command line, type the feature names exactly as they appear in the following tables as values for Windows Installer properties such as `ADDLOCAL` or `ADDSOURCE`.

Use the MSI feature names with the standard MSI properties and arguments. The `ADDLOCAL=`*`comma_delimited_list`* property would install one or more transports or options locally. For example, to install Sabre and MATIP for UTS locally, you would enter:

```
ADDLOCAL=ICW40_SABRE,ICW40_MATIP
```

Other common properties to set on the command line (but not in a transform) include `REMOVE=`*`comma_delimited_list`*, which uninstalls the feature and `ADDSOURCE=`*`comma_delimited_list`*, which installs the files for that feature to run from a network location.

INFOConnect Unisys Transports and Options

Transport or option	Feature name
TCPA - A Series TCP/IP Transport (default)	ICW40_ATA
INT1 Transport (default)	ICW40_OIA
MATIP for UTS Transport	ICW40_MATIP
CCF	ICW40_CCF

INFOConnect Airlines Transports and Options

Transport or option	Feature name
INT1 Transport (default)	ICW40_OIA_AIRLINES
MATIP for UTS Transport	ICW40_MATIP
MATIP for ALC Transport (default)	MATIP_ALC_AIRLINES
ATSTCP - Galileo Apollo Travel Services TCP/IP Transport	ICW40_ATS
UDPFRAD and TCPRAD Transports	ICW40_FRAD
Sabre IP Transport	ICW40_SABRE
Airlines Gateway Client Transport	ICW40_AIRGATE

PTR Stand-alone Transport and Options

Transport or option	Feature name
INT1 Transport	ICW40_OIA_AIRLINES
MATIP for ALC Transport (default)	MATIP_ALC_AIRLINES
MATIP for UTS Transport	ICW40_MATIP_AIRLINES
ATSTCP - Galileo Apollo Travel Services TCP/IP Transport	ICW40_ATS
UDPFRAD and TCPFRAD Transports	ICW40_FRAD
Sabre Transport	ICW40_SABRE
Airlines Gateway Client Transport (default)	ICW40_AIRGATE

Publish with Active Directory

To assign and publish your product installation using Microsoft Active Directory, you must meet the following requirements:

- Windows Administrative Tools are installed on your workstation.
- You are a member of **Domain Admins** and **Group Policy Creators and Owners**. (This is required to publish software.)

For more information, see "Active Directory groups" in the Microsoft Management Console help.

To install with Active Directory

1. From the **Active Directory User and Computers Console**, advertise your product installation to members of any organizational units in your Active Directory using appropriate transform modifications.
2. If multiple transforms are specified, make sure that the listed order of the transforms is correct, and click **OK**. (If you need to change the order for any reason after you click **OK**, you will have to start over again.)

NOTE: For more information about assigning and publishing, see "assigning applications" and "publishing applications" in the Microsoft Management Console help.

Deploy with System Center Configuration Manager

You can deploy InfoConnect with Microsoft Systems Center Configuration Manager (or Microsoft Systems Management Server).

To deploy with System Center Configuration Manager

1. Create an administrative install image on your site server.

   This serves as the administrative installation point for deployment.
2. Use the product Package Definition File (`.sms`) to create the product installation package.

   NOTE: The Package Definition File (`.sms`) is created during the administrative installation and can be found at the root of the administrative installation point. Alternatively, you can reference the `.msi` file directly — consult the Microsoft SMS documentation for more information.
3. Advertise the installation packages to your users.

Distribute Software Updates

InfoConnect service packs, updates and hotfixes are distributed as Microsoft `.msp` files. You can deploy these updates with the Micro Focus Patch utility included with your distribution. Patch log files are saved in the user's Windows temporary folder (`%tmp%`) with a generated name, using the form `atmpatchxxxxxx.log`.

To distribute updates with the Micro Focus Patch utility

1. From the distribution image, double-click the self-extracting executable update file.

   The Micro Focus Patch utility opens.
2. Follow the instructions provided by the utility.

   For detailed instructions on upgrading your Micro Focus products, refer to the Micro Focus Patch Utility Help.

To distribute updates from the command line

- To Install to a (clean) workstation and apply a patch:

  `msiexec /i path_to_original.msi PATCH=<path_to_patch.msp> /qb`
- To apply a patch to an administrative installation:

  `msiexec /p path_to_patch.msp /a <path_to_admin.msi> /qb`
- To reinstall to workstation (for example, after applying patch to admin):

  `msiexec /i path_to_admin.msi REINSTALLMODE=vomus REINSTALL=ALL /qb`

Remove an Installation

To remove InfoConnect, you can use the Windows Control Panel, the Setup program user interface, or a command line. To remove a companion installation, you can use the Windows Control Panel or a command line.

NOTE: You must log on with administrator privileges to remove InfoConnect.

To remove an installation using the Windows control panel

1. To open the **Programs and Features** control panel go to **Start** > **Control Panel** > **Programs and Features**. (On older Windows systems, this Control Panel is called Add or Remove Programs.)
2. Select the name of the installation that you want to remove.
3. Click **Uninstall** (or **Remove**).

To remove an installation with the Setup program user interface

1. From an administrative installation image, click the `setup.exe` file.
2. From the tab, select **Remove**, and then click **Continue**.

To remove an installation using setup.exe on the command line

---

CAUTION: If you use the following instructions to find the product code in the registry, make sure you do not change any registry values. Changing these values can damage an installation. If you prefer not to use the registry, you can get the product code by contacting Technical Support.

---

1. Open the registry editor (`regedit.exe`) and find this key:

   32-bit platforms

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
   ```

   64-bit platforms

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall
   ```

   Each key under the **Uninstall key** is the product code or Globally Unique Identifier (GUID) for a product installed on the computer.
2. In the **Uninstall** key, search for Micro Focus InfoConnect to find the Micro Focus InfoConnect product code.
3. Verify that the **DisplayName** includes “InfoConnect”
4. Run setup using the following syntax:

   `setup.exe /uninstall` *`ProductCode`*

   where *`ProductCode`* is the Globally Unique Identifier (GUID) that is the principal identifier for the product.

To remove a companion installer package with MSI directly

- At a command prompt, change to the directory in which the companion installer package file resides and enter:

  `msiexec /x` *`your_companion_file.msi`*

Repair an Installation

If you are experiencing problems with your installation, you can use the **Repair** option, which automatically searches for and replaces missing or corrupted files.

To repair an installation with the Setup program user interface

1. From an administrative installation image, click the `setup.exe` file.
2. Click **Repair,** and then follow the installer instructions.

To repair an installation using Windows Add/Remove

1. From the Windows **Programs and Features** (or the **Add or Remove Programs**) control panel, select the name of the installation that you want to repair, and then click **Change**.
2. From the Setup program, select **Repair**, and then click **Continue**.

To repair an installation using setup.exe on the command line

1. Determine product code or Globally Unique Identifier (GUID) for your InfoConnect product. (See details in “Remove an Installation” on page 77.
2. Run setup using the following syntax:

   `setup.exe /repair ProductCode`

   where *`ProductCode`* is the Globally Unique Identifier (GUID) for your product.

NOTE: Setup also supports `/reinstall ProductCode`.

A Appendix

InfoConnect Product/Feature Table

Use this table to determine which terminal and printer emulation features are available in your InfoConnect product. An **X** indicates that the feature is available.

	InfoConnect Desktop for Unisys	**InfoConnect Desktop Pro for Unisys**	**InfoConnect Desktop for Airlines**	**InfoConnect Desktop Pro for Airlines**
ALC terminal			**X**	**X**
PTR printer			**X** (with add-on)	**X** (with add-on)
UTS terminal	**X**	**X**	**X**	**X**
T27 terminal	**X**	**X**		
T27 printer	**X**	**X**		
IBM 3270 terminal		**X**		**X**
IBM 3270 printer		**X**		**X**
IBM 5250 terminal		**X**		**X**
IBM 5250 printer		**X**		**X**
VT terminal		**X**		**X**
HP terminal		**X**		**X**

Files Used by InfoConnect

This table describes files used by InfoConnect. Not all file types are supported by all InfoConnect products. See “InfoConnect Product/Feature Table” on page 79 to see which features are supported by your InfoConnect product.

* Can be opened directly from the Windows file explorer.

† Must be in a trusted location.

§ Included in the session file when you save the session as a compound document (page 25).

Description	File Name or Extension	Default location and additional notes
InfoConnect database	`ic32.cfg`	InfoConnect application data folder.
ALC session * †	`ialc`	Saved by default to the InfoConnect user data folder.
UTS session * †	`iuts`	Saved by default to the InfoConnect user data folder.
T27 session * †	`it27`	Saved by default to the InfoConnect user data folder.
3270 session * †	`rd3x`	Saved by default to the InfoConnect user data folder.
5250 session * †	`rd5x`	Saved by default to the InfoConnect user data folder.
VT session * †	`rdox`	Saved by default to the InfoConnect user data folder.
Web session * †	`urlx`	Saved by default to the InfoConnect user data folder.
Layout * †	`rwsp`	Saved by default to the InfoConnect user data folder.
HP session *	`r1w`	Saved by default to the InfoConnect user data folder
Template †	`rsft`	Default templates are installed to: InfoConnect program folder`\Built-Ins\Templates` User-defined templates are saved by default to: InfoConnect user application data folder`\Templates`
Workspace settings	`Application.settings`	Default settings are installed to: InfoConnect program folder`\Configuration` User customizations are be saved to: InfoConnect user application data folder Administrators can deploy settings for all users to: InfoConnect global application data folder
Workspace window size and position	`Frame.settings`	Same as `Application.settings`
Permissions Manager	`access`	Same as `Application.settings`.

Description	File Name or Extension	Default location and additional notes

Information Privacy Settings	`PCIDSS.settings`
	
	`PrivacyFilters.xml`
		These files are configured using the **Set Up Information Privacy** dialog box. Edits to privacy filters are saved to `PrivacyFilters.xml`. All other settings in that dialog box are saved to `PCIDSS.settings`.
		
		File locations are the same as `Application.settings`.

Theme §	`themex`	Built-in themes are installed to: InfoConnect program folder`\Built-Ins\Themes` User themes are saved by default to: InfoConnect user data folder`\Themes`
Keyboard map §	`xkb`	Built-in keyboard maps are installed to: InfoConnect program folder`\Built-Ins\Keyboard Maps` User keyboard maps are saved by default to: InfoConnect user data folder`\Keyboard Maps`
Mouse map §	`xmm`	Built-in mouse maps are installed to: InfoConnect program folder`\Built-Ins\Keyboard Maps` User mouse maps are saved by default to: InfoConnect user data folder`\Mouse Maps`
Hotspot §	`xhs`	Built-in hotspots maps are installed to: InfoConnect program folder`\Built-Ins\Keyboard Maps` User hotspots are saved by default to: InfoConnect user data folder`\Hotspots Maps`
Ribbon UI §	`xuml`	Built-in ribbon files are installed to: InfoConnect program folder`\Built-Ins\CustomUI` User customized ribbon files are saved by default to: InfoConnect user data folder`\CustomUI`
QuickPad §	`rqpx`	Predefined QuickPads are installed to: InfoConnect program folder`\Schemes\ENU` User QuickPads are saved by default to: InfoConnect user data folder`\QuickPads`
Screen History †	`rshx`	Saved by default to the InfoConnect user data folder
3270 and 5250 printer *	`rsf`	Saved by default to the InfoConnect user data folder.
PTR route configuration	`ptr32.ini`	InfoConnect application data folder.

Description	File Name or Extension	Default location and additional notes
PTR host filter	`hff`	InfoConnect program folder
T27 Print Services configuration	`atm`	InfoConnect program folder The default is `stdcfg.atm`.
Translation tables	`tbl`, `xlt`	Default samples are installed to the `Translation` subfolder of the InfoConnect user data folder and to the `ENU\Translation` subfolder of the InfoConnect program folder.
HLLAPI settings	`hllapi.xml`	InfoConnect user application data folder If it does not yet exist, this file is created the first time you use the **Configure IHLLAPI Settings** dialog box.
GraphX accessory configuration	`icc.ini`	Saved by default to the InfoConnect user data folder.
GraphX picture files	`grx` (ASCII) `ugp` (binary)	User-selected location
GraphX picture configuration	`ugc`	User-selected location
Reflection FTP Client Settings *	`rfw`	InfoConnect user data folder The default is `settings.rfw`
Reflection Certificate Manager settings	`pki_config`	InfoConnect user data folder`\.pki` This folder also contains certificates you have imported into the Reflection Certificate Manager store. Administrators can deploy these files for all users to: ProgramData\Micro Focus\InfoConnect\
Secure Shell configuration (per user)	`config`	Configuration settings saved by the user are saved to: InfoConnect user data folder`\.ssh`
Secure Shell configuration (all users)	`ssh_config`	Administrators can deploy settings for all users to: `ProgramData\Micro Focus\InfoConnect`
Secure Shell known hosts (per user)	`known_hosts`	Known hosts added by the user are saved to: InfoConnect user data folder`\.ssh`
Secure Shell known hosts (all users)	`ssh_known_hosts`	Administrators can deploy settings for all users to: `ProgramData\Micro Focus\InfoConnect`

Supported Legacy Files

The following legacy InfoConnect and EXTRA! file types also continue to be supported.

Description	File Extensions
InfoConnect session * †	adp, idp
Extra! session * †	edp
Layout * †	aww
HotSpot scheme	ehs
Keyboard map §	ekm
QuickPad §	eqp
Toolbar §	etb
Compiled CASL macro †	xwc
Casl macro source code	xws
EXTRA! Basic macro †	ebm

Managing FTP Client and Shared Security Settings after an Upgrade

If you are upgrading from InfoConnect version 8.1 SP1 or later, you may have some customized information in an `Attachmate\Reflection` subfolder located in your personal documents folder. Information stored in this folder includes:

- FTP Client settings (`\Settings.rfw`)
- Secure Shell known hosts and non-default Secure Shell settings (`\.ssh\*.*`)
- Certificates and settings configured using the Reflection Certificate Manager (`\.pki\*.*`)

Starting with InfoConnect Desktop version 16, these settings are stored in the same user data folder you use for your session documents and other user-configured files.

If you used the features listed above and upgrade your system to InfoConnect Desktop version 16, you will need to copy your settings from the `\Attachmate\Reflection` folder to your user data folder.

For example, if you used the default user data folder before the upgrade (`C:\Users\<user>\Documents\Attachmate\INFOCNEE`), InfoConnect Desktop will continue to use this same location for your user data after the upgrade. If you have any customized content in the `Attachmate\Reflection` folder, you should copy that content (include all subfolders) to your InfoConnect user data folder. You can do this using the Windows file explorer, or with a command line like the following:

```
C:\>robocopy /e C:\Users\myname\Documents\Attachmate\Reflection C:\Users\
myname\Documents\Attachmate\INFOCNEE
```

Glossary of Terms

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).

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.

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.

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.

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.

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.

FCC. Field Control Character. A UTS terminal field attribute.

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.

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.

InfoConnect database. The InfoConnect database (`ic32.cfg`) contains connection settings information for ALC, T27, and UTS terminal sessions. The database contains information about all the InfoConnect packages, path templates and libraries that have been installed, as well the paths that have been created. The InfoConnect packages, path templates and libraries are included based on which product features (emulations and transports) are installed.

InfoConnect application data folder. This folder location is configurable using the **Data Location** tab during installation. The default is `C:\Users\Public\Documents\Micro Focus\InfoConnect`.

InfoConnect program folder. The default on English language systems is `C:\Program Files (x86)\Micro Focus\InfoConnect` on 64-bit systems and `C:\Program Files\Micro Focus\InfoConnect` on 32-bit systems.

InfoConnect global application data folder. Settings here apply to all users of the system. The location is version-specific: `\ProgramData\Micro Focus\InfoConnect\Desktop\`*`version`*.

InfoConnect user application data folder. The default is `\Users\`*`username`*`\AppData\Roaming\Micro Focus\InfoConnect\Desktop\`*`version`*.

InfoConnect user data folder. This folder location is configurable using the **Data Location** tab during installation. The default is `C:\Users\`*`username`*`\Documents\Micro Focus\InfoConnect`.

InfoConnect global ssh data folder. InfoConnect stores global Secure Shell information in the Windows common application data folder. The default is `\ProgramData\Micro Focus\InfoConnect`.

InfoConnect user ssh folder. InfoConnect stores Secure Shell information for individual users in the following location in the Windows personal documents folder. The default is `\Users\`*`username`*`\Documents\Micro Focuse\InfoConnect\.ssh`.

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.

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.

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". Using OCSP removes the need for servers and/or clients to retrieve and sort through large CRLs.

package. An InfoConnect package is a collection of components that provide specific communication capabilities. Transport packages typically consist of one or more external interface libraries (EILs) or service libraries (SLs). For example, the InfoConnect TCP/IP Transport package includes the TCP EIL and the TP0 SL. Accessory packages typically consist of the terminal emulator or file transfer application and other related products. For example, the InfoConnect T27 package includes InfoConnect T27, T27 Print Services, and the T27 Print Services Configuration Utility.

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.

path. An InfoConnect path is a named collection of configuration settings that allows you to connect to a host. Paths are required for connections to ALC, T27 and UTS terminal sessions, and for PTR router connections. Path configuration data is stored in the InfoConnect database.

path template. InfoConnect path template are used as the basis for configuring paths. Each is combination of one or more libraries required for a particular connection type. If a library in the path template can have library channels, the path template can also indicate which library channel to use.

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. All companies who handle credit cards are likely to be subject to this standard.

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.

PTR route. A PTR route configures required information for printing using PTR. It consists of three parts: the host path (configures the communication link between PTR and the host), the host filter (a DLL that initializes the host connection, manipulates the printer data for the selected output device, and sends the data to the output device), and the printer queue path (configures the communication link between PTR and the output device, such as a printer or file).

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.

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.

Screen History. Screen History creates recordings of host screens as you navigate to them. (VT screens are not recorded automatically; they 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.

T27 print services environment. A set of configuration options that represents one host connection and determine how printing operates from that host.

T27 print services configuration file. A file use by T27 Print Services to view and manage host printing. Each configuration file contains settings for up to eight print environments. The default configuration file is `STDCFG.ATM`.

trusted host. A trusted host is one for which you hold the public key.

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 using the Specify Trusted Locations dialog box.

Windows common application data folder. The application data folder is hidden by default. The default is `\ProgramData\`.

Windows personal documents folder. The default on English systems is `\Users\`*`username`*`\Documents\`.

Workspace Menu. The Workspace menu contains layout options, application and document settings, and a list of recent documents. It is accessed by clicking the **File** menu (when using the ribbon user interface).