Evaluation Guide
Host Access Management and Security Server

12.4.4
Copyrights and Notices

Copyright

© 2017 Attachmate Corporation, a Micro Focus company. All rights reserved.

No part of the documentation materials accompanying this Attachmate software product may be reproduced, transmitted, transcribed, or translated into any language, in any form by any means, without the written permission of Attachmate Corporation. The content of this document is protected under copyright law even if it is not distributed with software that includes an end user license agreement.

The content of this document is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by Attachmate Corporation. Attachmate Corporation assumes no responsibility or liability for any errors or inaccuracies that may appear in the informational content contained in this document.

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

Third-Party Notices

This product contains software from third party suppliers.

RSA (now EMC) - BSAFE Crypto-J

This software includes RSA BSAFE cryptographic or security protocol software from RSA.

Copyright © 2012 EMC Corporation. All rights reserved. EMC, RSA, the RSA logo, and BSAFE are registered trademarks of EMC Corporation in the United States and/or other countries. Used under private license.

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.
Contents


1 Introduction to Host Access Management and Security Server 12.4.4 7
   Meeting Business Challenges ................................................................. 7
   Product Features ................................................................................... 7
   Add-On Products .................................................................................... 8
   Technical Resources .............................................................................. 8

2 Evaluation Scenario 11
   Company Requirements .......................................................................... 11
   Configuration Overview ......................................................................... 12
       Expected User Experience ................................................................. 12

3 Configuration Steps 13
   Set Up Single Sign-On and Centralized Management ............................ 13
       Step 1. Install the Host Access Management and Security Server evaluation software. ........................................... 13
       Step 3. Install Reflection Desktop version 16.1 evaluation software. .......................................................................... 17
       Step 4. Enable Centralized Management and set the Workspace view. ...................................................................... 18
       Step 5. Install the customized companion package to the workstation. ....................................................................... 21
   Create, Deploy, and Test a TLS 1.2 Session ............................................. 22
       Step 6. Create a Windows-based 3270 session that uses TLS 1.2 ............................................................................... 22
       Step 7. Deploy the session to the domain user's workstation. .................................................................................... 26
       Step 8. Test the deployment ................................................................. 28
   Lock Down the Workstation and Test the User Experience ..................... 29
       Step 9. Update (modify) the security settings ..................................... 29
       Step 10. Upload and deploy the updated companion.msi. .......... 33
       Step 11. Test the domain user's updated configuration. .......... 35
   The Results ......................................................................................... 36

4 After You Finish the Evaluation Scenario 37
   Try Optional Features ............................................................................... 37
   Moving to Production ............................................................................... 37
       Contact Us .......................................................................................... 37

Host Access Management and Security Server provides an administrator the means to centrally secure, manage, and monitor users’ access to host connections. Management and Security Server can manage several products including Reflection Desktop, InfoConnect, Reflection ZFE, Reflection for the Web, and Rumba.

Your Host Access Management and Security Server 12.4 Update 4 evaluation software is fully functional for 120 days. During that time you can install, configure, and test any configuration or feature.
Introduction to Host Access Management and Security Server 12.4.4

From one central location, an administrator can use Host Access Management and Security Server to secure, configure, and monitor Windows terminal client sessions, Java-based browser sessions, and HTML5 sessions (that do not require Java).

- Meeting Business Challenges
- Product Features
- Add-On Products
- Technical Resources

Meeting Business Challenges

These security challenges are top of mind for our customers. Follow the Evaluation Scenario in this guide to see how Host Access Management and Security Server can meet these challenges:

- Strengthen mainframe authentication—without making difficult changes on the mainframe.
- Reinforce security—without jeopardizing usability.
- Integrate mainframe authorization with existing Identity Access Management (IAM).
- Upgrade to TLS—without disrupting business processes.
- Ensure that only authorized personnel can connect to the host.
- Easily and efficiently harden those applications that access host resources to enforce our security mandates.

Related Topics

- Product Features
- Add-On Products
- Technical Resources

Product Features

Using Management and Security Server, the administrator can

- Centrally secure, manage, and monitor users’ access to mainframes and other hosts.
  - Use the Administrative WebStation to create and configure Windows-based terminal emulation sessions to deploy to users.
  - Use Package Manager to "push" application settings (for Windows-based sessions) to a user or user group, thereby locking down (or hardening) the application.
  - Use your current enterprise directory service, such as Active Directory or LDAP, to control access to Windows terminal client sessions, Java-based browser sessions, and HTML5 sessions.
Use **Access Mapper** to assign sessions to authorized users.

Use the **Metering Server** to centrally audit and limit user access to host sessions.

Manage Reflection Desktop (version 16.1) and InfoConnect Desktop (version 16.1) sessions without requiring Java on the desktop.

Manage other emulation products, including Extra, InfoConnect, Reflection ZFE, Reflection for the Web, and Rumba.

**Related Topics**

- Meeting Business Challenges
- Add-On Products
- Technical Resources

**Add-On Products**

You can enhance the value and benefits of Management and Security Server with add-on products. The Evaluation download includes these add-on products, which require separate production licenses:

- **Security Proxy Server** delivers end-to-end encryption and enforces access control at the perimeter with patented security technology. Specifically, the Security Proxy encrypts the data between the client and the Security Proxy Server. The Security Proxy connects to the host computer and encrypts the data before forwarding it to the user.

- **Terminal ID Manager** enables you to centrally manage access to terminal and printer sessions by dynamically allocating terminal IDs based on username, DNS name, IP address, or address pool.

- **Automated Sign-On for Mainframe** enables automated sign-on to IBM 3270 applications via your identity and access management system, including multi-factor authentication such as smartcards.

- **PKI Automated Sign-On** enables automated application sign-on to your critical enterprise systems.

- **Micro Focus Advanced Authentication** enables strong multi-factor authentication using a variety of authentication methods, including biometrics, one-time passwords, and smartphone authentication.

**Related Topics**

- “Meeting Business Challenges” on page 7
- Product Features
- Technical Resources

**Technical Resources**

Refer to these resources for more information while evaluating Host Access Management and Security Server.

- **Installation Guide**

• **Administrative WebStation Help**
  Use the Search box in the Administrative WebStation to find overviews and specific help topics. Or, click the Help button on each page.

• **Technical Resources Page**
  The [Technical Resources Page](#) provides a comprehensive list of resources, including technical notes, documentation, security information, and product news.

• **Technical Support**
  To request technical support, see [Contact Support](#).

**Related Topics**

- Product Features
- Add-On Products
- Evaluation Scenario
- Configuration Steps
Evaluation Scenario

To simplify the evaluation of this platform-independent product, follow this use-case scenario to learn about Management and Security Server’s primary features and the administrator’s workflow. In addition to this scenario, you can evaluate other options on your own.

Our customers typically install Management and Security Server and its components on server-class machines. From there, they manage Windows Desktop emulation applications, such as Reflection Desktop, across their enterprise.

**NOTE:** Even if your environment is different from the evaluation scenario presented here, you can walk through the steps to see how business objectives and company requirements can be met.

In this scenario, you will use Management and Security Server 12.4.4 to

- assign sessions to only authorized users.
- configure secure connections to host applications.
- restrict users’ access to application settings.

For evaluation purposes, install both products on your Windows workstation, provided you have both an administrator logon and a user logon.

Company Requirements

In this evaluation scenario, a desktop application administrator is in charge of setting up and using Management and Security Server 12.4.4. The company requires that

- The administrator can centrally manage the deployment of Micro Focus terminal emulation products to 1000 user workstations (in production).
  
  For this evaluation, the administrator will deploy to one user.
- Only authorized users are allowed to access the mainframe applications.
- All sessions are connected over a secure protocol.
- Applications are locked down (hardened) to ensure company security mandates are enforced.
- PCI compliance policies are enforced.
- Implementing centralized management and security does not disrupt the end-user experience.

The Assumptions

This scenario demonstrates the “before” and “after” effect of using Management and Security Server 12.4.4 to secure access to the company’s mainframe applications.

- The company uses Reflection Desktop version 16.1.
- The company uses a Windows 64-bit system environment with LDAP directory services. Users authenticate to the Windows domain.
The “domain user” in this scenario represents the end user.
The end users are accustomed to logging on before accessing their mainframe sessions.

Configuration Overview

To meet the company requirements, the administrator’s evaluation of Management and Security Server 12.4.4 would include these steps.

To test the results of the configuration, you will need both an administrator logon and a domain user logon. If you do not have all of the required systems set up, you can still follow along.

Detailed steps follow this high-level overview.

Set Up Single Sign-On and Centralized Management

1. Install the Host Access Management and Security Server 12.4.4 evaluation software.
3. Install Reflection Desktop version 16.1 evaluation software.
4. Enable Centralized Management, set the Workspace view, and create an installation point.
5. Install the customized companion package to the workstation.

Create, Deploy, and Test a TLS Session

6. Create a Windows-based 3270 session that uses TLS 1.2.
7. Deploy the session to the domain user’s workstation.
8. Test the deployment.

Lock Down the Workstation and Test the User Experience

9. Update (modify) the security settings.
10. Upload and deploy the updated companion.msi.
11. Test the domain user’s updated configuration.

Expected User Experience

After these steps are performed:

- The authorized domain user logs on to the Windows domain and can access the mainframe applications.
- The user’s sessions are connected over a secure TLS protocol.
- The user cannot alter settings because Reflection Desktop v16.1 has been locked down.
- The user experience has not been disrupted.
3 Configuration Steps

For this evaluation, you will use Management and Security Server 12.4.4 to secure Reflection Workspace sessions created by Reflection Desktop version 16.1. Some settings are configured in Management and Security Server, while others are configured in Reflection Workspace.

The steps are organized into three sections:

- Set Up Single Sign-On and Centralized Management
- Create, Deploy, and Test a TLS session
- Lock Down the Workstation and Test the User Experience

Review your progress

After you complete a set of steps, the Review your progress sections help you determine where you are in the evaluation scenario -- what you accomplished and what comes next.

Set Up Single Sign-On and Centralized Management

For the initial setup, you will install the evaluation software for two products:

Host Access Management and Security Server 12.4.4 – with an administrator logon
Reflection Desktop version 16.1 – for the administrator and domain user’s workstations

Steps in this section:

- Step 1. Install the Host Access Management and Security Server evaluation software.
- Step 3. Install Reflection Desktop version 16.1 evaluation software.
- Step 4. Enable Centralized Management and set the Workspace view.
- Step 5. Install the customized companion package to the workstation.

Step 1. Install the Host Access Management and Security Server evaluation software.

In this step, you will obtain and install the Management and Security Server evaluation software. Later in Step 3, you will obtain and install the Reflection Desktop v16.1 evaluation software.

The test server, for this scenario (which could be the administrator workstation) requires:

- Windows 64-bit OS
- Java Virtual Machine 8 or higher, capable of running Java applications
- a web browser using JRE 8 or later
- no previous installation of Management and Security Server, Reflection for the Web, or Reflection Security Gateway
The **domain user’s workstation** requires:

- Windows workstation

**Note:** System requirements for Management and Security Server 12.4.4 are detailed in the Installation Guide.

## Obtain and install an evaluation copy of Management and Security Server

In this section, you will obtain an evaluation copy of Management and Security Server 12.4.4, and then install it on a test server, which could be the administrator’s workstation.

1. Log on as administrator to the Windows machine that you are using for your evaluation.
2. Request the **Host Access Management and Security Server** evaluation software:
   

   Enter the requested information and click **Submit**. You will receive an email message with download instructions.

3. Open the Product Evaluation email message and click the link to download the software.
4. Find the line for Windows 64-bit and click the filename: `mss-12.4.4.<nnn>-eval-wx64.exe`
5. Accept the **Terms of Use** and download the file. Run the self-extracting executable. Refer to the Installation Guide, as needed.
6. Open the **install_automated** folder and click the `.exe` file to start the installation. Proceed through the installation dialogs, accepting the defaults.
   
   **Note:** The password you enter here will be used to access the Administrative WebStation.

7. On the **Install and Start Services** page, click **Next** to Start server components now.
8. On the **Installation Complete** page, click the link under Administrative Server to start Host Access Management and Security Server.

   Acknowledge the Security messages:

   - When you first open the Administrative Server, you may see a security message about verifying the site’s certificate. Click **Yes** to proceed.
   - When asked, "Do you want to run this application?", select "Run" or "Grant this session" (depending on your browser).

**NOTE:** After installation, open the **Administrative Server** from the Start menu (under Micro Focus Host Access Management and Security Server).

9. Notice that you are logging in as server administrator.

   Enter the password you entered during installation, and click **Submit**.

10. This dialog will later be populated with the sessions you configure.

    Click **Administrative WebStation** (bottom right).
About the Administrative WebStation

The Administrative WebStation provides the tools to create, secure, and manage terminal emulation
sessions. The Administrative WebStation is the interface for the Administrative Server.

On the Administrative WebStation Home page, the primary tools (Activities) are listed, along with a
variety of resources. Product Help is available from Search, the home page, and the configuration
pages. Take a look to see what is available.

NOTE: To avoid a session timeout while you are evaluating, go to the Administrative WebStation >
Security Setup. On the Security tab, find the "Require new login after" field. Enter a value greater
than the 60-minute default.

Step 2. Configure Management and Security Server for
Windows Single Sign-On.

Of the many authentication types that Management and Security Server supports, in this evaluation
you will use Windows Active Directory for authentication (to the Administrative Server) and LDAP
for authorization. By using Single Sign-On and your existing identity management system, the user
experience will not be disrupted.

When users authenticate to Management and Security Server’s Administrative Server with their
Windows domain logon, they will have access to the sessions that the administrator makes available
to them.

NOTE: If you do not have access to LDAP or Active Directory, you can leave Authentication set to
“None”; however the business objective for this evaluation will not be met.

As the administrator:

1. In the Administrative WebStation, open Access Control Setup. Note the current setting of “None”
   for Authentication and Authorization. Click Configure

2. Select Single sign-on through Windows authentication, and click Next.

   ![Administrative WebStation](image)

   NOTE: By using single sign-on, the user experience is not disrupted because the user is already
   familiar with their Windows domain logon.

3. Select, or verify the selection of, Active Directory (NTLM v2). Enter your system information, See
   Help for assistance.
4. Use the default, Only on HTTPS connection. Click Next.

5. On the Choose Authorization Method page, select Use LDAP to restrict access to sessions. Click Next.

6. Enter your LDAP Server information, with Windows Active Directory as the Server type. Click Next.

7. On the confirmation page, click Save Settings.
Step 3. Install Reflection Desktop version 16.1 evaluation software.

Now that Management and Security Server is installed and configured for Single Sign-On, you are ready to install the evaluation copy of Reflection Desktop v16.1.

**A. Obtain the Reflection Desktop version 16.1 evaluation software:**

2. Enter the requested information and click *Submit*. You will receive an email message with download instructions.
3. Open the Product Evaluation email message and click the link to download the software.
4. Agree to the Terms of Use, and click the file to download now: `rdesktop-16.1-eval-w32.exe`
5. Note the download location. Rather than installing the product directly, you will create an administrative installation point.

**B. Create an Administrative installation image of Reflection Desktop v16.1.**

Use this procedure to create an *administrative installation point* on a networked file server.

The administrative installation point provides a single location for all of the administrative tools and installation files, including a source image of the application, needed to customize and install Reflection. From there you can customize the deployment for your users.

To create an administrative installation point:

1. Be sure you are logged on to your workstation with *administrator* privileges to install Reflection Desktop v16.1.
3. From the root directory of the installation files, click `setup.exe` to start the Micro Focus Reflection Desktop Setup Program. Click *Continue* to install Micro Focus Reflection Desktop.
4. Click *Continue* and accept the license.
5. Open the Advanced tab and click *Create an Administrative install image on a server.*
6. Click **Continue**. The File Location tab is selected automatically.

7. For this evaluation, use the default location, C:\Reflection, for the administrative install image.

**NOTE:** For testing, you can create the image in any folder on a local hard disk. For production, the installation image would be created on a network drive accessible to user’s workstations, and you need to specify a UNC path for the network share. For example: \share_name\administrative_install_point

8. Click **Install Now**. Click **Close** when the installation is complete.

From this administrative installation point (C:/Reflection), you can enable centralized management and customize the installation’s security settings.

**Review your progress**

Now that Management and Security Server is installed (Steps 1-2) and the Reflection Desktop v16.1 administrative installation point is created (Step 3), you are ready to enable Centralized Management so that access to the mainframe can be secured by Management and Security Server.

**Step 4. Enable Centralized Management and set the Workspace view.**

To enable centralized management, the administrator must modify the settings for all users.

These steps configure a companion package that will be installed on user workstations. The package enables centralized management and customizes the Workspace opening view to make it easy for users to find their customized sessions.

First, you need to install Reflection Desktop v16.1 on your administrator workstation so that you can use the Installation Customization Tool to configure the settings.

1. **Install Reflection Desktop to your administrator workstation:**
   a. From the administrative install point (C:\Reflection, created in Step 3), run setup.exe.
   b. Proceed through the installation, accepting all defaults. (Install to this PC is selected on the Advanced tab.) Click **Close** when the installation is complete.

2. **Use the Installation Customization Tool:**
   a. In the Windows **Run** line, enter `<path_to_setup>\setup.exe /admin`
      The default is C:\Reflection\setup.exe /admin
   b. In the Select Customization dialog, select **Create a new Companion installer**. Click **OK**.
c. From the left nav, click Modify user settings.

d. From the list of Application - Settings, select Reflection Desktop - Workspace Settings and then click Define.

The Reflection Workspace Settings open in a separate window. (There may be a pause.)

3. **Enable Centralized Management:**
   
b. Click **Enable Centralized Management**.
   For the **Server URL**, enter the URL that displays in the Management and Security Server browser when the administrator logs on. This URL is for the Administrative Server.
   For example, `http://<servername>/mss/`
   c. Click **Test Connection** to verify the entry.

   Changes take effect after you reopen the workspace.

d. Resist clicking OK to keep Reflection Workspace Settings open. Changes will be saved when you close the Customization Tool (step 4d).
   If Reflection Workspace closes, re-open it by clicking Define in the Installation Customization Tool. If prompted for credentials, click Cancel.

4. **Set the Workspace opening view:**
   By default Reflection Desktop displays the “Create new Document” dialog box when it first opens. Because you will be managing sessions from Management and Security Server Workspace, users will not need to create their own sessions.
   These steps configure the Workspace to show the File > Open dialog box.
   a. Click File > Settings > **Reflection Workspace Settings**.
   b. Under Workplace Settings, click **Configure Workspace Defaults**.
   c. On the “When starting workspace” drop-down menu, change the setting to **Show Open** dialog.
d. Click OK. Reflection Workspace closes.

e. In the Installation Customization Tool, click File > Save. Save the file with the default name, companion.msi, in the default location, C:\Reflection.

f. Click File > Save to close the customization tool.

**Step 5. Install the customized companion package to the workstation.**

Now, switch to the domain user’s perspective. For this evaluation, you will install the companion package manually.

In a production scenario, the administrator would likely deploy both the product msi file and the companion.msi in a chained sequence using the Installation Customization tool or through other standard deployment tools.

1. Log off Windows as the administrator, and log on as the domain user.
2. Browse to the administrative install point, and double-click companion.msi to install it. You may be prompted for administrative credentials to install the package.

A progress bar displays as the msi runs and the companion package is installed.

**NOTE:** In a production scenario, the administrator would likely deploy both the product msi file and the companion.msi in a chained sequence through the standard deployment tools.


**Review your progress**

The initial setup is completed. Now you are ready to create and deploy a TLS session.

**Related Topics**

- Create, Deploy, and Test a TLS 1.2 Session
- Configuration Steps
Create, Deploy, and Test a TLS 1.2 Session

In this section, you will create a TLS 1.2 session and then test the “before” security settings -- before the workstation is locked down.

Steps in this section:

- Step 6. Create a Windows-based 3270 session that uses TLS 1.2.
- Step 7. Deploy the session to the domain user’s workstation.
- Step 8. Test the deployment.

Step 6. Create a Windows-based 3270 session that uses TLS 1.2.

The administrator’s company requires secure access to the mainframe. To meet this requirement, create a session to an IBM 3270 host, using both Management and Security Server and Reflection Desktop.

1. Log off Windows as the domain user, and log on as the administrator.
3. Click Administrative WebStation, and click Session Manager.
4. Click Add and notice the available Windows-Based sessions.
5. Select Reflection/InfoConnect Workspace and enter a Session name, such as 3270-TLS. Click Continue.
6. Accept the default settings on the Configure a Windows-Based Reflection Session page, and click Launch. Reflection Workspace launches in a separate window.
7. In Reflection Workspace, create a new document using the 3270 terminal template. Click Create.

8. In the Create New 3270 Terminal Document dialog, enter the Host name of a TLS-enabled host name and the appropriate port.

   If you cannot connect with TLS, enter the name of another mainframe host. You will not be able to evaluate the exact behavior on your system, but you can follow along.

9. Check Configure additional settings (at the bottom), and click OK.
10. In the Settings for 3270 dialog under Host Connection, click **Configure Advanced Connection Settings**. Scroll to and click **Security Settings**. (If prompted, disconnect the session.)

11. On the SSL/TLS tab:
   a. Click **Use SSL/TLS security**, and keep the Default Encryption strength.
   b. In the SSL/TLS version drop-down menu, select **TLS Version 1.2**.
c. Click OK twice. The session is now configured.

As mentioned earlier, if you cannot connect with TLS, you will not be able to evaluate the exact behavior on your system, but you can follow along.

12. In Reflection Workspace, click File > Save. Click OK to send the settings to the Administrative Server.

For this evaluation, you do not need to send it as a compound session.

(When the session is sent as a compound file, all of the custom keyboard maps and other settings that apply to that session are saved in the session file. Compound files simplify the deployment process because you do not have to deploy these settings in separate files.)


*Review your progress*

The security settings are configured (Steps 4, 5), and the session to the mainframe is created (Step 6). Now you can “push” the settings to the domain user.

**Step 7. Deploy the session to the domain user’s workstation.**

In Management and Security Server, use the Access Mapper to authorize the domain user to access the mainframe session.

1. In the Administrative WebStation, open Access Mapper. Or, if the Session Saved page is still open, click Map session access to open the Access Mapper.

2. For this evaluation, deploy the 3270-TLS session to the domain user. Search the LDAP directory for that user.

   To find the user, enter a user name, a group or folder name, along with an asterisk (*) wildcard, or a combination of * and letters. Click Search.
Note: If you are not using LDAP, the only option is to deploy the session to all (or no) users.

3. On the Terminal Sessions tab, verify that the correct user name is displayed. Click your session, 3270-TLS, to grant access to the domain user. In this example, the domain user is “User User1 One.”

4. Click Save Settings (you may need to scroll).

Now, when the domain user opens Reflection Workspace, they will see the 3270-TLS session.

5. Log off as administrator.

Review your progress

The companion package is installed on the user workstation, with settings to enable Centralized Management in the Reflection Workstation and to display the Open dialog box when the Workstation first opens.

The completion of Steps 1–7 meet the company requirements to ensure that:

- Only authorized users are allowed access to the mainframe applications.
- All sessions are connected over a secure protocol.
Step 8. Test the deployment.

Test the initial deployment and make note of what the user can and cannot change.

1. Log on as the Windows domain user.
2. Click Start > All Programs > Micro Focus Reflection > Reflection Workspace.
   When the domain user launches Reflection Workspace, any sessions made available to that user using Management and Security Server are downloaded to the users documents folder. Notice that Reflection Workspace opens and presents the Open dialog (that you configured earlier).
3. Find and double-click the 3270-TLS session you created (in Step 6).
4. Note the default security settings for Primary Account Number (PAN) Redaction Rules:
   a. Open Reflection Workspace Settings (File > Settings > Reflection Workspace Settings).
   b. Under Trust Center, click Set Up Information Privacy, and scroll to Primary Account Number (PAN) Redaction Rules.
   
   **NOTE:** The first three checkboxes under Primary Account Number (PAN) Redaction Rules are not checked for this user. (These settings will be modified in a future step.)
   
   Click OK.

5. View the TLS Connection settings (from Step 6):
   a. Click File > Settings > Document Settings, and under Host Connection, click Configure Advanced Connection Settings.
   b. Scroll to and click Security Settings.

   **NOTE:** Although the Use SSL/TLS security setting is checked, the user could change the setting.

Review your progress

When you tested the initial deployment (Step 8), you observed the “before” settings – before access to the company’s mainframe applications is locked down.

Now the administrator needs to restrict the end user’s ability to change the security settings and thereby lock down the workstation.
Lock Down the Workstation and Test the User Experience

In this section, you will lock down the user’s workstation by restricting the ability to change settings, and then deploying the updated package of security settings.

Steps in this section:

Step 9. Update (modify) the security settings
Step 10. Upload and deploy the updated companion.msi.
Step 11. Test the domain user’s updated configuration.

Step 9. Update (modify) the security settings.

The administrator can modify the existing companion.msi and “push” those restrictions to lock down the user’s workstation.

NOTE: You will use the Installation Customization Tool for all of Step 9.

A. Open the Installation Customization Tool, as before.

1. Log off Windows as the user; log on as the administrator.
2. Open the Installation Customization Tool, as before:
   In the Windows Run line, enter C:\Reflection\setup.exe /admin
3. In the Select Customization dialog, select Open an existing Setup customization file or Companion installer. Click OK.
4. Select the companion msi that you previously customized.

B. Restrict the user from modifying the PAN Redaction Rules.

1. From the left nav, click Modify user settings.
2. From the list of Application – Settings, select Workspace Settings, and click Define.
3. In Reflection Workspace Settings under Trust Center, select Set Up Information Privacy.
4. Scroll to Primary Account Number (PAN) Redaction Rules, and check the first three boxes.

   Primary Account Number (PAN) Redaction Rules

   ![Select Customization dialog box](image1)

   - Enable redaction (exported data only)
   - Portion of PAN to redact: Show last 4 digits only
   - Redact display data (Terminals Supported: IBM)
   - Redact data while typing (Terminals Supported: IBM)
   - Do not store typed PANs

   Click OK.

5. From the list of Application - Settings, select Reflection Desktop – application.access, and then click Define.
Make changes to user settings on the computer where the customization file is installed

The Reflection Desktop Permissions Manager opens in a separate window. (There may be a pause.)

6. In the Groups drop-down menu, select PCIDSS.

7. Select these five items one at a time, and change the setting to Restricted for each. The “Restricted” setting requires an administrator logon to change the setting.

   RecognitionStyle
   RedactionRules
   RedactStyle
   RegularExpressions
   StoreTypedPANs

8. Click Next; then click Finish. Continue in the Installation Customization Tool
C. Restrict the user from modifying Centralized Management capabilities.

If Centralized Management is not enabled, the user’s workstation will no longer be managed by Management and Security Server, which defeats the administrator’s goal.

1. Select **Reflection Desktop – application.access** again, and click **Define**.
2. In the **Permissions Manager Groups** drop-down menu, select **ApplicationOptions**.
3. Select **CentralizedManagementEnabled** and change the setting to **Restricted**.
4. Select **CentralizedManagementServerUrl**, and change the setting to **Restricted**.

5. Click **Next**; then click **Finish**. Continue in the Installation Customization Tool.

D. Restrict the user’s ability to change the TLS settings.

1. Select **Reflection Desktop-rd3x.access**, and click **Define**.

2. In the **Groups** drop-down menu, select **Document\Connection\TN3270Advanced**.
3. On the right, click **Restrict All**. Click **Next**; then click **Finish**.

**E. Save the companion file.**

1. Click **File > Save**. Click **Yes** to increase the version number.

The new version number for the same file name will be recognized as a revision, and the resulting package will upgrade the previously deployed file.

2. **Save** the companion file using the same name. Click **Yes** to replace it and increase the version number.

3. **Exit** the Installation Customization Tool.

**Step 10. Upload and deploy the updated companion.msi.**

You can use the Package Manager feature in Management and Security Server to upload and then deploy the updated companion.msi with restricted settings to the end user workstation.
A. Upload the updated companion.msi file.

1. Open the Administrative WebStation, open Package Manager.
2. Click Add and then Browse to the companion.msi file that you created and updated on the administrative installation point. Select the file and click Open.

   The default location is C:\Reflection\.

   ![Package Manager](image)

   3. In Package Manager, note the file name on the “Package to upload:” line. Enter a description and click Save to upload the package to the Administrative Server. Verify the package is included in the list.

   Next, you will use Access Mapper to assign the package (with your updated companion.msi) to your domain user.

B. Deploy the updated companion.msi to the domain user.

Earlier, you used the Access Mapper to make a session available to the domain user. This time, you will use Access Mapper to “push” the modified companion package to the domain user.

1. In the Administrative WebStation, open Access Mapper.
2. As before, Search the LDAP directory for the domain user.
3. On the Terminal Sessions tab, verify that the correct user name is displayed.
4. In the Packages section, check companion.msi.
5. Click Save Settings (you may need to scroll) to deploy the package.

Now, when the domain user launches Reflection Workspace or a session, the package is downloaded, and the changes in the companion.msi are applied. The contents of the package are installed to the location specified in the .msi package.

Later, if you update the package (with the same file name), the newer one will be downloaded.

Review your progress

After updating the companion.msi with restricted security settings (Step 9) and deploying the msi package to the domain user (Step 10), you can now observe the “after” effect on the user’s restrictions.

Step 11. Test the domain user’s updated configuration.

1. Log off as the Windows administrator; log on as the domain user.
2. Launch the 3270-TLS session either in Recent Documents or by launching the product and the session.
3. NOTE: The settings for PAN Redaction Rules (Step 8: 4) are checked and cannot be changed without entering the administrator credentials.
4. NOTE: The TLS Connection settings (Step 8: 5) are restricted and cannot be changed by the domain user without entering administrator credentials.

Review your progress

Your test in Step 11 confirms that the company requirements to lock down the desktop are met:

- Applications are hardened (locked down) to ensure company security mandates are enforced.
- PCI compliance policies are enforced (with the PAN Redaction Rules).
- Implementing centralized management and security does not disrupt the end-user experience.

Related Topics

- The Results
The Results

This evaluation scenario demonstrates how Management and Security Server can be used to meet a company's security requirements when managing a domain user's access to the mainframe.

Specifically, the administrator is able to

- integrate mainframe authorization with Windows Single Sign-On -- the existing Identity Access Management (IAM).
- upgrade to TLS 1.2 -- without disrupting the business processes.
- reinforce security -- without jeopardizing usability.

The user

- is able to log on as usual, access a secure mainframe session, and begin working.
- is not able to alter settings that were locked down.

In production, a similar approach can be used to secure and manage thousands of workstations.

Related Topics

- After You Finish the Evaluation Scenario
4 After You Finish the Evaluation Scenario

- Try Optional Features
- Moving to Production

As you continue to evaluate Management and Security Server, you can explore more features -- including the add-on products. When you purchase, be sure to download version 12.4 Update 4.

Try Optional Features

Consider evaluating these optional features, which are available in the evaluation download.

Note: In production, each add-on product requires a separate license along with Host Access Management and Security Server.

- Metering
- Security Proxy Add-On
- Terminal ID Management Add-On

Refer to the Technical Resources for assistance and overviews.

Moving to Production

When you transition from the evaluation software to a licensed copy, be sure to download Host Access Management and Security Server version 12.4 Update 4.

See the Release Notes for more information.

Contact Us

If you have any questions about Management and Security Server, please contact us.