Smart Card Authentication Client

Administrator's Guide

April 2013

www.lexmark.com

Contents

Overview

Smart Card Authentication Client is an authentication module application that lets you secure access to printers by requiring users to log in using a Smart Card or a user name and password. You can use the application to secure access to all applications and functions on the printer home screen or to individual applications and functions. The application also provides Kerberos authentication options and a Kerberos ticket that can be used by other secured applications.

Additional required applications

- For the application to work correctly, the **eSF Security Manager** application must be installed and running on the printer. This application lets you associate Smart Card Authentication Client with each application and function to which you want to secure access.
- If you are using Smart Cards with this application, then an **authentication token** must be installed and running on the printer. The token enables the printer to communicate with the type of Smart Card you are using. You must use the correct authentication token for your Smart Card type.
- If you want to secure access to all applications and functions on the printer home screen, then the **Background and Idle Screen** application must be installed and running on the printer. This application can be secured through Smart Card Authentication Client to provide a secure idle screen that requires users to authenticate before they can access the home screen.

For a list of application requirements, including supported printers and required firmware versions, see the *Readme* file.

For information on physically setting up the printer or using the printer features, see the *User's Guide* on the *Software and Documentation* CD that came with the printer. After completing initial setup tasks according to the printer *User's Guide*, see the *Networking Guide* that came with the printer for information on how to connect the printer to your network.

For information on licensing the application, see “Licensing applications” on page 28.

Configuring Smart Card Authentication Client

Configuring printer settings for use with the application

Even if the printer has been set up previously, make sure all settings have been configured to enable the security features of the application to work correctly.

Changing the panel login timeout

To help prevent unauthorized access if a user leaves the printer unattended with a Smart Card inserted or while logged in, you can limit the amount of time a user stays logged in without activity. If the user does not touch the screen within the specified time, then the session ends and the user is logged out, even if a Smart Card is still inserted.

1. From the Embedded Web Server, click **Settings** or **Configuration**.
2. Click **Security** > **Miscellaneous Security Settings** > **Login Restrictions**.
3. Set the Panel Login Timeout value (in seconds). The recommended value is 30 seconds.
4. Click **Submit**.

Installing certificates manually

Note: In select printer models, you can automatically download the CA. For more information, see “Installing certificates automatically” on page 5.

Before configuring Kerberos or domain controller settings, you must install the appropriate certificates on the printer. At minimum, you must install the certificate of the *Certificate Authority* (CA) that issued the domain controller certificate. The CA certificate is used for domain controller validation. Additional certificates can be installed if needed. For example, if you plan to use chain validation to validate the domain controller certificate, then you must install the entire certificate chain. Each certificate must be in a separate PEM (.cer) file.

For each certificate you want to install, do the following:

1. From the Embedded Web Server, click **Settings** or **Configuration**.
2. Click **Security** > **Certificate Management** > **Certificate Authority Management** > **New**.
3. Upload the file containing the certificate, and then click **Submit**.

   Note: The file must be in PEM (.cer) format. The contents of the file should resemble the following:

```
-----BEGIN CERTIFICATE-----
MIIE1jCCA76gAwIBAgIQY6sV0KL3tIhBtlr4gHG85zANBgkqhkiG9w0BAQUFADBs
…
l3DTbPe0mnIbTq0iWqKEaVne1vvaDt52iSpEQyevwgUcHD16rFy+sOnCaQ==
-----END CERTIFICATE-----
```

Installing certificates automatically

For eSF v4.x printers, the CA certificate can be installed automatically.

Note: Make sure to add the printer to the Active Directory Domain. For more information on how to add the printer to the Active Directory, see the *Embedded Web Server Administrator's Guide* for your printer.

1. From the Embedded Web Server, click **Settings** or **Configuration**.
2. Click **Security** > **Certificate Management** > **Certificate Authority Management** > **CA Cert Monitor Setup**.
3. Select **Enable CA monitor**.

   If you want to immediately install the CA certificate without waiting for the scheduled run time, then select **Fetch immediately**.
4. Click **Submit**.

Configuring TCP/IP settings

Make sure all necessary TCP/IP settings have been configured.

1. From the Embedded Web Server, click **Settings** or **Configuration**.
2. Click **Network/Ports** > **TCP/IP**.
3. Under the TCP/IP heading, do the following:
   - Verify the domain name. Normally, the domain will be the same one assigned to user workstations.
   - If you are using a static IP address, then verify the WINS server address and the DNS server address. If a backup DNS server is available, then type the backup DNS server address.
   - If the printer is located in a different domain than the domain controller, any e-mail servers you are using, or any file shares to which printer users may need to scan, then list the additional domains in the Domain Search Order field. Separate each domain name with a comma. If everything is in the same domain, then you can leave the Domain Search Order field blank.
4. Click **Submit**.

Setting the date and time

In order for users to log in to the printer using Kerberos authentication, the time on the printer clock must be within five minutes of the time on the domain controller system clock. Printer clock settings can be updated manually, or they can be configured to use *Network Time Protocol* (NTP) to automatically sync with a trusted clock (typically the same clock used by the domain controller).

Setting the date and time manually

1. From the Embedded Web Server, click **Settings** or **Configuration**.
2. Click **Security** > **Set Date and Time**.
3. In the “Manually Set Date & Time” field, type the correct date and time in **`YYYY-MM-DD HH:MM`** format.

   Note: Entering manual settings automatically disables the use of NTP.

4 Select the correct time zone.

Note: If you select **(UTC+user) Custom**, then you must configure additional settings under the Custom Time Zone Setup heading.

5 If *daylight saving time* (DST) is observed in your area, then select **Automatically Observe DST**.

6 If you are located in a nonstandard time zone or in an area that observes an alternate DST calendar, then adjust the Custom Time Zone Setup settings.

7 Under the Network Time Protocol heading, verify that **Enable NTP** is not selected and that the NTP Server field is cleared.

8 Click **Submit**.

Using NTP

Note: If your network uses *Dynamic Host Configuration Protocol* (DHCP), then verify that NTP settings are not provided by the DHCP server automatically before configuring NTP settings manually.

1 From the Embedded Web Server, click **Settings** or **Configuration**.

2 Click **Security** > **Set Date and Time**.

3 Verify that the “Manually Set Date & Time” field is cleared.

4 Select the correct time zone.

Note: If you select **(UTC+user) Custom**, then you must configure additional settings under the Custom Time Zone Setup heading.

5 If daylight saving time is observed in your area, then select **Automatically Observe DST**.

6 If you are located in a nonstandard time zone or in an area that observes an alternate DST calendar, then adjust the Custom Time Zone Setup settings.

7 Under the Network Time Protocol heading, select **Enable NTP**, and then type the IP address or host name of the NTP server.

8 If the NTP server requires authentication, then do one of the following, depending on the options that are available:

- Select **MD5 key** or **Autokey IFF** from the Authentication drop-down menu, and then click **Install MD5 key** or **Install Autokey IFF params** to browse to the file containing the NTP authentication credentials. Click **Submit** to install the file.
- Select **Enable Authentication**, and then click **Install auth keys** to browse to the file containing the NTP authentication credentials. Click **Submit** to install the file.

9 Click **Submit**.

Securing access to the printer

Note: Before securing access to the printer, make sure the Application Access Manager application is installed and running. For more information about Application Access Manager, see the *Application Access Manager Administrator’s Guide*.

There are two ways to secure access to the printer:

- Enable a secure idle screen that restricts access to the entire home screen. When users insert a Smart Card or touch the screen, they will be prompted to authenticate before they can access the home screen.

  Note: The Background and Idle Screen application must be installed and running on the printer to enable this functionality.
- Restrict access to individual applications and functions. Users will be able to access the home screen, but when they touch a secured home screen icon or attempt to use a secured function, they will be prompted to authenticate before they can access that application or function. You can secure access to:
  - Installed applications, such as Scan to Network
  - Individual functions of installed applications, such as the Change Background function of the Background and Idle Screen application
  - Built-in printer functions, such as copy and fax

  Users will still be able to access unsecured applications and functions without having to authenticate.

Setting up a security template

Before you can secure access to applications and functions, you need to create a security template that uses Smart Card Authentication Client to obtain user credentials. You can then assign this security template to each application and function you want to protect.

1. Create a building block.
   a. From the Embedded Web Server, click **Security** > **Security Setup**.
   b. Under the Advanced Security Setup heading, click the building block (or blocks) appropriate for your environment, and then configure it.

      Note: For more information on configuring a specific type of building block, see the "Configuring building blocks" section of the *Embedded Web Server Administrator's Guide* for your printer.
2. Create a security template.
   a. From the Embedded Web Server, click **Settings** or **Configuration**.
   b. Click **Security** > **Security Setup**.
   c. Under the Advanced Security Setup heading, click **Security Template** > **Add a Security Template**.
   d. Type a name for the security template (for example, **`Smart Card`**).
   e. From the Authentication Setup menu, select **Smart Card Authentication Client**, and then click **Save Template**.
   f. Verify that your template appears in the Manage Security Templates list.

Setting up group authorization for the Security Template

Notes:

- This method applies only to printers running Embedded Solutions Framework (eSF) version 3.0 or later.

- Make sure you have configured the Group Authorization List from the Smart Card Authentication Client application configuration settings. For more information, see "Configuring advanced settings" on page 13.

a From the Manage Security Templates list, select the security template name.

b Click **Modify Authorization**.

c From the Authorization Setup menu, select **Smart Card Authentication Client**.

d Click **Modify Groups**.

e Select one or more groups, and then click **Save Template**.

For more information on configuring security templates and using access controls, see the *Embedded Web Server Administrator's Guide* for your printer.

Securing access to the home screen

Use this method to require users to authenticate to view and use the printer home screen.

Note: The Background and Idle Screen application must be installed and running on the printer before you can secure access to the home screen.

1 Access the Background and Idle Screen application configuration settings from the Embedded Web Server.

2 Under the Idle Screen Settings heading, make sure that **Enable** is selected.

3 In the Start Time field, enter **0**. This prompts the printer to start the secure idle screen immediately (0 seconds) after a user's login session ends.

4 Under the Home Screen Background heading, make sure that **Enable** is not selected if you do not want users to be able to change the home screen background image from the printer control panel.

5 If you want to add custom idle screen images, then click **Add** under the Idle Screen Images heading.

6 Type an image name, and then upload the file you want to use.

Note: For information about compatible image file types and recommended file sizes, see the mouse-over help next to the field.

7 Click **Apply**.

8 Repeat step 5 through step 7 to add more idle screen images. You can add up to ten images.

9 If you want to add a custom home screen background image, then under the Home Screen Background heading, select one of the default images, or upload a custom image in the Custom Image field.

Note: For information about compatible image file types and recommended file sizes, see the mouse-over help next to the field.

10 If necessary, configure the other application settings. For more information about configuring Background and Idle Screen, see the *Background and Idle Screen Administrator's Guide*.

11 Click **Apply**.

12 Secure access to the idle screen using Smart Card Authentication Client.

On printers running the Embedded Solutions Framework (eSF) version 3.0 or later:

a Make sure that you have created a security template that uses Smart Card Authentication Client to obtain user credentials. See "Setting up a security template" on page 7.

b From the Embedded Web Server, click **Settings** > **Security** > **Security Setup**.

c From Step 3 under the Advanced Security Setup heading, click **Access Controls**.

d If necessary, expand the **Device Solutions** folder.

e From the Idle Screen drop-down menu, select your security template.

f Click **Submit**.

On printers running eSF version 2.0:

a Access the eSF Security Manager application configuration settings from the Embedded Web Server.

b From the Idle Screen drop-down menu, select **Smart Card Authentication Client**.

c Click **Apply**.

Note: If you are unsure about which version of eSF your printer is running, then see "Checking which version of the Embedded Solutions Framework is installed on a printer" on page 29.

Securing access to individual applications and functions

Securing access to installed applications and functions

Use this method to restrict access to installed applications, such as Scan to Network, or to restrict access to the individual functions of an installed application, such as the Change Background function of the Background and Idle Screen application.

On printers running the Embedded Solutions Framework (eSF) version 3.0 or later:

1 Make sure you have created a security template that uses Smart Card Authentication Client to obtain user credentials. See "Setting up a security template" on page 7.

2 From the Embedded Web Server, click **Settings** > **Security** > **Security Setup**.

3 From Step 3 under the Advanced Security Setup heading, click **Access Controls**.

4 If necessary, expand the **Device Solutions** folder.

5 For each application or function to which you want to secure access, select your security template from the drop-down menu.

6 Click **Submit**.

On printers running eSF version 2.0:

1 Access the eSF Security Manager application configuration settings from the Embedded Web Server.

2 For each application or function to which you want to secure access, select **Smart Card Authentication Client** from the drop-down menu.

3 Click **Apply**.

Note: If you are unsure about which version of eSF your printer is running, then see "Checking which version of the Embedded Solutions Framework is installed on a printer" on page 29.

Securing access to built-in printer functions

Use this method to restrict access to built-in printer functions, such as copy and fax.

1 Make sure you have created a security template that uses Smart Card Authentication Client to obtain user credentials. See "Setting up a security template" on page 7.

2 From the Embedded Web Server, click **Settings** or **Configuration**, and then click **Security** > **Security Setup**.

3 From Step 3 under the Advanced Security Setup heading, click **Access Controls**.

4 If necessary, expand one or more of the access control category folders.

5 For each function to which you want to secure access, select your security template from the drop-down menu.

6 Click **Submit**.

Notes:

- If you have used a built-in printer security setup to protect the Use Profiles access control, then any installed applications you secure using Smart Card Authentication Client will prompt users for credentials twice. When users touch a secured application icon, they will first be prompted for the credentials specified by the Use Profiles access control, and then they will be prompted for their Smart Card or user name and password.
- If you need to secure access to profiles you have created and installed on the printer, then you can remove the printer security template applied to the Use Profiles access control, and then apply a security template that uses Smart Card Authentication Client. All of your installed profiles will be secured and users will be prompted for their Smart Card or user name and password when they attempt to access a profile.

Configuring login screen settings

You can use the login screen settings to choose how users will be allowed to log in to the printer and whether they will be prompted for a PIN or a password after inserting a Smart Card.

1 Access the Smart Card Authentication Client application configuration settings from the Embedded Web Server.

2 Under the Login Screen heading, from the Login Type menu, select how users will be allowed to log in to the printer:
   - **Smart Card Only**—This allows users to log in using a Smart Card.
   - **Smart Card or Manual Login**—This allows users to log in using either a Smart Card or a user name and password.
   - **Manual Login Only**—This allows users to log in using a user name and password.

   Notes:

   – If you selected **Smart Card or Manual Login** or **Manual Login Only**, then configure the Manual Login Domain(s) setting under the Manual Login Setup heading. See “Configuring manual login setup settings” on page 11. If you do not configure this setting, then users will not be allowed to log in to the printer manually (using their user name and password).

   – If you selected **Smart Card Only**, then configure the setting to User Validation Mode. For more information, see “Configuring User Validation Mode settings” on page 14.

3 From the Validate Smart Card menu, select whether users will be prompted to type a PIN or a password after inserting a Smart Card.

4 Click **Apply**.

Configuring manual login setup settings

Notes:

- If users are allowed to log in to the printer manually (using a user name and password instead of a Smart Card), then specify a list of Windows domains for users to select from during login.
- For eSF v4.x printers, if a manual domain is not specified, then the printer will use the domain in the Kerberos configuration file. To view the complete list of supported printers for each version of the Embedded Web Server, see the *Readme* file.

1. Access the Smart Card Authentication Client application configuration settings from the Embedded Web Server.
2. Under the Manual Login Setup heading, in the Manual Login Domain(s) field, specify the domain or domains that will be available for users to select during login. Separate multiple domains with a comma. Domains are case-sensitive and are usually typed in lowercase.
3. Click **Apply**.

Configuring Smart Card setup settings

Note: This is required only in certain printer models. For other printer models, configuring the Kerberos Authentication system is not required.

Configuring Kerberos settings

In addition to providing the mechanism for validating login credentials, Smart Card Authentication Client can also be configured to provide Kerberos authentication.

Note: As with any form of authentication that relies on an external server, users will not be able to access secured applications and functions if a network issue prevents the printer from communicating with the authenticating server.

1. Access the Smart Card Authentication Client application configuration settings from the Embedded Web Server.
2. Under the Smart Card Setup heading, from the Kerberos Information menu, do one of the following:
   - Select **Use device Kerberos setup file** to use the Kerberos configuration file (krb5.conf) installed on the printer.
   - Select **Use simple Kerberos setup** to enter Kerberos information manually in the Simple Kerberos Setup fields.

     Notes:

     - Only one Kerberos realm can be specified using simple Kerberos setup. If you need to specify multiple realms, then use the device Kerberos setup file.
     - A Kerberos configuration file from an eSF version 2.0 or eSF version 3.0 printer will not work on an eSF version 4.0 printer.

Using the device Kerberos setup file

If you selected **Use device Kerberos setup file**, then make sure the Kerberos configuration file is installed on the printer.

a From the Embedded Web Server, click **Settings** or **Configuration**.

b Click **Security** > **Security Setup**.

c From Step 1 under the Advanced Security Setup heading, click **Kerberos 5**.

d Verify that the Kerberos configuration file is installed. If the file is not installed, then under the Import Kerberos File heading, upload the appropriate krb5.conf file, and then click **Submit**.

Using simple Kerberos setup

If you selected **Use simple Kerberos setup**, then enter the Kerberos information manually under the Simple Kerberos Setup heading. When you click **Apply**, the values you entered are used to create a Kerberos configuration file.

- **Realm**—Specify the Kerberos realm as configured in Active Directory. This is typically the Windows domain name. Only one realm can be specified here. To specify multiple realms, customize a Kerberos configuration file and install it on the printer. The realm must be typed in uppercase.
- **Domain Controller**—Specify the IP address or host name of the domain controller or domain controllers used for validation. Separate multiple values with a comma. The domain controllers will be tried in the order listed.
- **Domain**—Specify the domain or domains that should be mapped to the Kerberos realm specified in the Realm field. The domain is the second part of the *User Principal Name* (UserID@DomainName) on the Smart Card. Type the domain in this format: domain name, comma, period, domain name again. For example, **`DomainName,.DomainName`**. Multiple domains that map to the specified Kerberos realm can be added here, separated by a comma. For example, **`DomainName1,.DomainName1,DomainName2,.DomainName2`**. The domain is case-sensitive and is usually typed in lowercase.
- **Timeout**—Specify the number of seconds (3 to 30) to wait for a response from the domain controller before trying the next one listed.

Selecting the domain controller validation method

Under the Smart Card Setup heading, from the Domain Controller Validation menu, select the method to use for validating the domain controller certificate:

Note: Before configuring this setting, make sure the appropriate certificates are installed on the printer. See “Installing certificates manually” on page 4.

- **Use device certificate validation**—This is the most common method. This method uses the certificate of the Certificate Authority (CA) that issued the domain controller certificate to validate the domain controller certificate. The CA certificate must be installed on the printer.
- **Use device chain validation**—This method uses the entire certificate chain, from the domain controller to the root CA, to validate the domain controller certificate. The entire certificate chain must be installed on the printer.
- **Use OCSP validation**—This method uses the *Online Certificate Status Protocol* (OCSP) to validate the domain controller certificate. The entire certificate chain, from the domain controller to the root CA, must

be installed on the printer, and the settings under the Online Certificate Status Protocol (OCSP) heading must be configured:

- **Responder URL**—Specify the IP address or host name of the OCSP responder/repeater and the port being used (typically 80). Type the value in this format: **`http://ip_address:port_number`**.

  For example, **`http://255.255.255.0:80`**.

  Separate multiple values with a comma. The values will be tried in the order listed.
- **Responder Certificate**—Upload the X.509 certificate for the OCSP responder. This certificate is used to validate that the response from the OCSP responder is from a trusted source.
- **Responder Timeout**—Specify the number of seconds (5 to 30) to wait for a response from the OCSP responder before trying the next one listed.
- **Allow Unknown Status**—Select this check box to allow users to log in if the OCSP response indicates that the certificate status is unknown. If the certificate status is unknown and the check box is cleared, then users will not be allowed to log in.

When you are done configuring Smart Card setup settings, click **Apply**.

Configuring advanced settings

Not all networks require you to configure advanced settings. If necessary, adjust the settings to enable the printer to communicate on your network.

1. Access the Smart Card Authentication Client application configuration settings from the Embedded Web Server.
2. Under the Advanced Settings heading, configure the following settings:
   - **Session User ID**—Select how the user ID will be obtained when a user logs in:
     - **None**—The user ID is not set. You can select this option if the user ID is not needed by other applications.
     - **User Principal Name**—The User Principal Name (UserID@DomainName) retrieved from the Smart Card or provided during manual login is used to set the user ID.
     - **EDI-PI**—The "UserID" portion of the User Principal Name (UserID@DomainName) retrieved from the Smart Card or provided during manual login is used to set the user ID.
     - **LDAP Lookup**—The user ID is retrieved from Active Directory.
   - **E-mail From Address**—Select where the printer should retrieve the user's e-mail address when sending e-mail.
     - **Smart Card**—This retrieves the e-mail address from the user's Smart Card.
     - **LDAP Lookup**—This retrieves the user's e-mail address from Active Directory.
   - **Disable Reverse DNS Lookups**—If reverse DNS lookups are not used on your network, then select this check box (if available).

     On printers running the Embedded Solutions Framework (eSF) version 3.0 or later, this setting is not available from the application configuration settings. If your printer is running eSF version 3.0 or later, then do the following to disable reverse DNS lookups:

     a. From the Embedded Web Server, click **Settings** > **Security** > **Security Setup**.

     b. From Step 1 under the Advanced Security Setup heading, click **Kerberos 5**.

c Under the Kerberos Settings heading, select **Disable Reverse IP Lookups**.

d Click **Submit**.

Note: If you are unsure about which version of eSF your printer is running, then see "Checking which version of the Embedded Solutions Framework is installed on a printer" on page 29.

- **Wait for user information**—For some secured applications to work correctly, additional user information must be placed in the login session. Select this option to retrieve all user information before allowing the user to access the home screen or secured application.

  Note: If you have enabled manual login and you are using the Secure E-mail application along with Smart Card Authentication Client, then you must select this option. This ensures that a manual login user's e-mail address is stored in the login session and is available for use with Secure E-mail. If this option is not selected, then manual login users cannot send e-mail to themselves automatically. The Secure E-mail "Send me a copy" option will not be available.
- **Use SSL for User Info**—Select this check box to use an SSL connection to retrieve user information from the domain controller. If this check box is cleared, then a non-SSL connection is used.
- **Other User Attributes**—List any other LDAP attributes that should be added to the user's session. These attributes will be used with other applications. Separate multiple values with a comma.
- **Group Authorization List**—List all Active Directory groups that are authorized to use at least one printer function. Separate multiple groups with a comma. Leave this field blank if you are not using group authorization.
- **Hosts File**—If DNS is not enabled on your network, then upload a text file containing the necessary IP address–host name mappings.

  Type the mappings in the text file in this format: IP address, space, server host name. For example, **`0.0.0.0 HostName`**. You can assign multiple host names to an IP address. For example, **`0.0.0.0 HostName1 HostName2 HostName3`**. You cannot assign multiple IP addresses to a host name. To assign IP addresses to groups of host names, type each IP address and its associated host names on a separate line of the text file. For example:

  ```
  123.123.123.123 HostName1 HostName2
  456.456.456.456 HostName3
  ```

3 Click **Apply**.

Configuring User Validation Mode settings

You can secure your printer using the Smart Card without the need to maintain a full Kerberos authentication system. The user inserts the Smart Card into the reader and then enters the PIN in the printer home screen. If the Smart Card PIN matches the PIN entered in the home screen matches, then the user can access the application.

1 Access the Smart Card Authentication Client application configuration settings from the Embedded Web Server.

2 Under the Login Screen heading, set "Login Type" to **Smart Card Only**, and then set the Authentication mode to **PIN ONLY**.

3 From the Domain Controller Validation menu, select **Use device certificate validation**.

Note: The Online Certificate Status Protocol (OCSP) must *not* be configured.

4 Under the Advanced Setting heading, set “E-mail From Address” to **Smart Card**, and then clear the **Wait for user information** check box.

Note: Session User ID must be set to **None**, and the “Other User Attributes” and “Group Authorization List“ fields must be empty.

5 Click **Apply**.

Troubleshooting

Smart Card Authentication Client login issues

“A card reader was not detected on this device” error message

Make sure a supported Smart Card reader is attached

If you want users to access the printer using a Smart Card, then attach a supported Smart Card reader to the printer. See the *Readme* file for a list of supported card readers.

Allow users to log in manually

If you have enabled manual login, then this error message will prompt users that they can “press Login to manually authenticate.” This indicates that users can still log in to the printer using a user name and password instead of a Smart Card.

“Unsupported USB Device” error message when a Smart Card reader is attached to the printer

Try one or more of the following:

Make sure that the Smart Card reader is supported

See the *Readme* file for a list of supported card readers.

Make sure that the required firmware version is installed

The minimum required firmware version or a later version must be installed before you can attach a supported card reader to the printer. Remove the card reader, and then see the *Readme* file for a list of required firmware versions.

Make sure that all required applications are installed and running

Smart Card Authentication Client, eSF Security Manager, and the authentication token for your Smart Card must be installed and running before you can attach a supported card reader to the printer.

“An error occurred while reading the card. Remove your card and try again” error message

Check the system log for relevant details

1. Access the list of installed applications from the Embedded Web Server.
2. Click **System** tab > **Log**.
3. From the Filter menu, select an application status.
4. From the Application menu, select the application, and then click **Submit**.

If you are still unable to determine the cause of the error, then you may need to replace the card.

“Your card has been locked out from future login attempts” error message

This error occurs after a user enters an invalid Smart Card PIN or password too many times or if a user attempts to authenticate using a card that has already been locked out due to too many invalid PIN/password entries.

Reset or replace the card

When a card is locked out, it will need to be reset or replaced. Find out whether the type of card you are using can be reset. If the card cannot be reset, then it will need to be replaced.

“An error occurred while checking your PIN. Remove your card and try again” error message

Check the system log for relevant details

1. Access the list of installed applications from the Embedded Web Server.
2. Click **System** tab > **Log**.
3. From the Filter menu, select an application status.
4. From the Application menu, select the application, and then click **Submit**.

User is unable to log in manually

Make sure the Manual Login Domain(s) field are specified

Verify that the domains under Manual Login Domain(s) are specified. See “Configuring manual login setup settings” on page 11.

User is logged out almost immediately after logging in

Increase the panel login timeout interval

1. From the Embedded Web Server, click **Settings** or **Configuration**.
2. Click **Security** > **Miscellaneous Security Settings** > **Login Restrictions**.
3. Increase the number of seconds specified in the Panel Login Timeout field, and then click **Submit**.

The printer home screen fails to return to a locked state when not in use

Try one or more of the following:

Make sure all required applications are installed and running

Smart Card Authentication Client, eSF Security Manager, and the authentication token for your Smart Card must be installed and running in order to restrict access to the printer home screen or to individual home screen applications and functions. Background and Idle Screen must also be installed and running if you want to secure access to the entire home screen.

Make sure the home screen or home screen icons are secured

Either the entire home screen or individual home screen applications and functions must be secured correctly. See “Securing access to the printer” on page 6.

Smart Card Authentication Client authentication issues

“Authentication failed” error message

This error occurs when Kerberos authentication fails or domain controller validation fails while a user is attempting to log in to the printer.

Check the system log for relevant details

1. Access the list of installed applications from the Embedded Web Server.
2. Click **System** tab > **Log**.
3. From the Filter menu, select an application status.
4. From the Application menu, select the application, and then click **Submit**.

“Kerberos configuration file has not been uploaded” error message

This system log error indicates that the Kerberos configuration file is not installed on the printer.

Make sure the Kerberos configuration file is installed

If you want to use the device Kerberos setup file, then make sure the file is installed on the printer.

If you want to use simple Kerberos setup to create the Kerberos configuration file, then manually configure the simple Kerberos setup settings.

For information about installing a Kerberos configuration file or configuring simple Kerberos setup settings, see “Configuring Kerberos settings” on page 11.

“Kerberos configuration file is not properly formatted” error message

This system log error indicates that the Kerberos configuration file contains incorrect information, is missing information, or is not formatted properly.

Modify the installed Kerberos configuration file

If you used the device Kerberos setup file, then modify and reinstall the file.

If you used simple Kerberos setup, then modify the simple Kerberos setup settings. For information about configuring simple Kerberos setup settings, see “Using simple Kerberos setup” on page 12.

“Unable to authenticate. Check Kerberos configuration file to verify Windows support enabled” error message

This system log error indicates that the Windows domain is not specified in the Kerberos configuration file.

Make sure the Windows domain is specified

If you used the device Kerberos setup file, then add an entry to the domain_realm section of the file, mapping the lowercase Windows domain to the uppercase realm. When you are done, reinstall the file on the printer.

If you used simple Kerberos setup, then:

1. Access the application configuration settings from the Embedded Web Server.
2. Under the Simple Kerberos Setup heading, add the Windows domain (in lowercase) to the Domain field.

   Example: If the value in the Domain field is **`DomainName,.DomainName`** and the Windows domain is **`x.y.z`**, then change the value in the Domain field to **`DomainName,.DomainName,x.y.z`**.
3. Click **Apply**.

“Unable to generate certificate from card” or “Unable to read certificate information from card” error message

These system log errors indicate that the Smart Card certificate was not found or that an error occurred while the application was attempting to retrieve data from the Smart Card certificate.

Check the certificate on the Smart Card

Verify that the certificate information on the Smart Card is correct. If the information is correct and the issue still occurs, then contact your solutions provider.

“The domain controller did not respond within the required time; the domain controller timeout may need to be increased” error message

Try one or more of the following:

Increase the domain controller timeout

If you used the device Kerberos setup file, then increase the number of seconds specified for the timeout entry in the file. When you are done, reinstall the file on the printer.

If you used simple Kerberos setup, then:

1. Access the application configuration settings from the Embedded Web Server.
2. Under the Simple Kerberos Setup heading, increase the number of seconds specified in the Timeout field.
3. Click **Apply**.

Make sure the domain controller IP address or host name is correct

If you used the device Kerberos setup file, then:

1. From the Embedded Web Server, click **Settings** or **Configuration**.
2. Click **Security** > **Security Setup** > **Kerberos 5** > **View File**.
3. Make sure the domain controller IP address or host name specified in the configuration file is correct.

If you used simple Kerberos setup, then:

1. Access the application configuration settings from the Embedded Web Server.
2. Under the Simple Kerberos Setup heading, verify that the IP address or host name specified in the Domain Controller field is correct.
3. Click **Apply**.

Make sure the domain controller is available

This error can occur if the domain controller is not available at the time a user is trying to authenticate to the printer. You can resolve this by specifying multiple domain controllers. If a domain controller is not available, then the next one listed will be tried. You can specify multiple domain controllers in the Kerberos configuration file or in the simple Kerberos setup Domain Controller field. If you are using the Domain Controller field, then separate each value with a comma.

Make sure Port 88 is not blocked by a firewall

Port 88 must be opened between the printer and the domain controller for authentication to work.

“The domain controller issuing certificate has not been installed” error message

This system log error indicates that the required Certificate Authority (CA) certificate is not installed or that an incorrect certificate is installed.

If an incorrect certificate is installed, then the error message specifies the name of the certificate that is needed: “The domain controller issuing certificate [NAME OF CERTIFICATE] has not been installed.”

Make sure the correct certificates are installed on the printer

See “Installing certificates manually” on page 4.

“The realm on the card was not found in the Kerberos configuration file” or “User’s realm was not found in the Kerberos configuration file” error message

These system log errors indicate that the user’s realm in the Kerberos configuration file is missing or incorrect.

Add the missing realm or modify the incorrect realm

If you used the device Kerberos setup file, then add the missing realm or realms to the file, or modify the incorrect realms. Make sure each realm is typed in uppercase. When you are done, reinstall the file on the printer.

If you used simple Kerberos setup, then:

1. Access the application configuration settings from the Embedded Web Server.
2. Under the Simple Kerberos Setup heading, add the missing realm to the Realm field or correct the realm. Make sure the realm is typed in uppercase.

   Note: The simple Kerberos setup settings do not support multiple Kerberos realm entries. If multiple realms are needed, then install a Kerberos configuration file containing the necessary realms.

“Unable to authenticate. Verify the realm was specified in UPPERCASE” error message

Make sure the Kerberos realm is in uppercase

If you used the device Kerberos setup file, then:

1. From the Embedded Web Server, click **Settings** or **Configuration**.
2. Click **Security** > **Security Setup** > **Kerberos 5** > **View File**.
3. Make sure the realm entries in the configuration file are in uppercase.

If you used simple Kerberos setup, then:

1. Access the application configuration settings from the Embedded Web Server.
2. Under the Simple Kerberos Setup heading, make sure the realm is correct and that it is typed in uppercase.

3 Click **Apply**.

“Unable to contact the domain controller for the user’s realm” error message

This system log error indicates that the domain, realm, or domain controller specified in the Kerberos configuration file is incorrect.

Check the domain, realm, and domain controller in the Kerberos configuration file

If you used the device Kerberos setup file, then:

1 From the Embedded Web Server, click **Settings** or **Configuration**.

2 Click **Security** > **Security Setup** > **Kerberos 5** > **View File**.

3 Make sure all domain, realm, and domain controller information is correct.

If you used simple Kerberos setup, then:

1 Access the application configuration settings from the Embedded Web Server.

2 Under the Simple Kerberos Setup heading, make sure the values typed in the Realm, Domain Controller, and Domain fields are correct. For information about configuring these settings, see “Using simple Kerberos setup” on page 12.

3 Click **Apply**.

“Domain controller and device clocks are different beyond an acceptable range. Check the device's date and time” error message

This system log error indicates that the printer clock is more than five minutes out of sync with the domain controller system clock.

Check the date and time on the printer

1 From the Embedded Web Server, click **Settings** or **Configuration**.

2 Click **Security** > **Set Date and Time**.

- If you configured date and time settings manually, then verify or correct the settings. Make sure the time zone and daylight saving time (DST) settings are correct.
- If you configured the printer to use a Network Time Protocol (NTP) server, then verify that the NTP settings are correct and that the NTP server is functioning correctly.

  Note: If your network uses Dynamic Host Configuration Protocol (DHCP), then verify that NTP settings are not provided by the DHCP server automatically before configuring NTP settings manually.

3 Click **Submit**.

“Unable to validate certificate from domain controller” error message

This system log error indicates that the required Certificate Authority (CA) certificate or certificates are not installed on the printer or that you selected the wrong domain controller validation method. Try one or more of the following:

Make sure the correct certificates are installed on the printer

See “Installing certificates manually” on page 4.

Check the domain controller validation method

1. Access the application configuration settings from the Embedded Web Server.
2. Under the Smart Card Setup heading, make sure you selected the correct method from the Domain Controller Validation menu. For information about configuring this setting, see “Selecting the domain controller validation method” on page 12.
3. Click **Apply**.

“An error occurred during domain controller chain validation” or “At least one of the certificates in the domain controller certificate chain has been revoked” error message

These system log errors indicate that there is a problem with one or more of the certificates needed for chain validation. Certificates may be missing, expired, or revoked, or they may contain incorrect information.

Check the certificates installed on the printer

1. From the Embedded Web Server, click **Settings** or **Configuration**.
2. Click **Security** > **Certificate Management** > **Certificate Authority Management**.
3. Make sure all certificates required for chain validation are installed and contain correct information. Make sure none of the certificates have been revoked or are expired.

   If you need to install certificates, then see “Installing certificates manually” on page 4.

   If all certificates are installed correctly and these issues still occur, then contact your solutions provider.

“The OCSP responder URL or certificate has not been configured” error message

This system log error indicates that OCSP settings are not configured correctly.

Check the OCSP responder URL and responder certificate

1. Access the application configuration settings from the Embedded Web Server.
2. Under the Online Certificate Status Protocol (OCSP) heading, make sure the values in the Responder URL and Responder Certificate fields are correct. For information about configuring these settings, see “Selecting the domain controller validation method” on page 12.
3. Click **Apply**.

“An error occurred while trying to connect to the OCSP responder” error message

This system log error indicates that the OCSP responder URL is configured incorrectly or that the responder timed out before the application could connect to it. Try one or more of the following:

Check the OCSP responder URL

1. Access the application configuration settings from the Embedded Web Server.
2. Under the Online Certificate Status Protocol (OCSP) heading, make sure the value in the Responder URL field is correct. For information about configuring this setting, see “Selecting the domain controller validation method” on page 12.
3. Click **Apply**.

Increase the responder timeout

1. Access the application configuration settings from the Embedded Web Server.
2. Under the Online Certificate Status Protocol (OCSP) heading, increase the number of seconds specified in the Responder Timeout field.
3. Click **Apply**.

“The status of at least one of the certificates in the domain controller certificate chain is unknown” error message

Try one or more of the following:

Check the certificates installed on the printer

1. From the Embedded Web Server, click **Settings** or **Configuration**.
2. Click **Security** > **Certificate Management** > **Certificate Authority Management**.
3. Make sure all certificates required for chain validation are configured correctly. See “Installing certificates manually” on page 4.

Allow users to log in if the certificate status is unknown

1. Access the application configuration settings from the Embedded Web Server.
2. Under the Online Certificate Status Protocol (OCSP) heading, select **Allow Unknown Status**. This allows users to log in to the printer even if the status of one or more of the required certificates is unknown.
3. Click **Apply**.

“The OCSP responder certificate, stored on the printer, does not match the one returned by the responder” error message

Try one or more of the following:

Check the OCSP responder certificate

1. Access the application configuration settings from the Embedded Web Server.
2. Under the Online Certificate Status Protocol (OCSP) heading, make sure the correct certificate has been uploaded in the Responder Certificate field.
3. Click **Apply**.

Check the certificate returned from the OCSP responder

Make sure the OCSP responder is returning the correct certificate.

“An error occurred while trying to validate the domain controller certificate against the OCSP responder” error message

This system log error indicates that the domain controller is returning an incorrect certificate or that the OCSP responder is not checking the correct certificate. Try one or more of the following:

Check the domain controller certificate

Make sure the domain controller is returning the correct certificate.

Check the OCSP responder

Make sure the OCSP responder is checking the correct domain controller certificate.

“The user is not authorized to use this device. Make sure the user belongs to an Active Directory group that is authorized to use the device” error message

This system log error usually indicates that the user is not in an Active Directory group that is authorized to use the printer. Try one or more of the following:

Add the user to an authorized Active Directory group

If user authorization is enabled for the printer, then add the user to an Active Directory group that is included in the authorization list for the printer.

Add the user’s group to the authorization list for the printer

Make sure the user’s Active Directory group is listed in the Group Authorization List field in the application configuration settings.

1. Access the application configuration settings from the Embedded Web Server.
2. Under the Advanced Settings heading, add the user’s Active Directory group to the Group Authorization List field. Separate multiple groups with a comma.

3 Click **Apply**.

Smart Card Authentication Client LDAP issues

LDAP lookups fail

Try one or more of the following:

Make sure Port 389 (non-SSL) and Port 636 (SSL) are not blocked by a firewall

The printer uses these ports to communicate with the LDAP server. The ports must be open for LDAP lookups to work.

Disable reverse DNS lookups

The printer uses reverse DNS lookups to verify IP addresses. If reverse DNS lookups are not used on your network, then do the following:

On printers running the Embedded Solutions Framework (eSF) version 3.0 or later:

1 From the Embedded Web Server, click **Settings** > **Security** > **Security Setup**.

2 From Step 1 under the Advanced Security Setup heading, click **Kerberos 5**.

3 Under the Kerberos Settings heading, select **Disable Reverse IP Lookups**.

4 Click **Submit**.

On printers running eSF version 2.0:

1 Access the application configuration settings from the Embedded Web Server.

2 Under the Advanced Settings heading, select **Disable Reverse DNS Lookups**.

3 Click **Apply**.

Note: If you are unsure about which version of eSF your printer is running, then see "Checking which version of the Embedded Solutions Framework is installed on a printer" on page 29.

If the LDAP server requires SSL, then enable SSL for LDAP lookups

1 Access the application configuration settings from the Embedded Web Server.

2 Under the Advanced Settings heading, select **Use SSL for User Info**.

3 Click **Apply**.

Narrow the LDAP search base

Narrow the LDAP search base to the lowest possible scope that includes all necessary users.

Verify that the LDAP attributes being searched for are correct

Make sure all LDAP attributes for the user are correct.

Smart Card Authentication Client licensing issues

License error

Try one or more of the following:

Make sure the application is licensed

Applications require a license to run.

For more information on purchasing a license, contact your Lexmark representative.

Make sure the license is up-to-date

Make sure the license for the application has not yet expired. Check the license expiry date using the Embedded Web Server.

Appendix

Configuring applications using the Embedded Web Server

Accessing application configuration settings using the Embedded Web Server

1. Obtain the printer IP address:
   - From the printer home screen
   - From the TCP/IP section in the Network/Ports menu
   - By printing a network setup page or menu settings page, and then finding the TCP/IP section

Note: An IP address appears as four sets of numbers separated by periods, such as 123.123.123.123.

2. Open a Web browser, and then type the printer IP address in the address field.

   The Embedded Web Server appears.

3. From the navigation menu on the left, click **Settings** or **Configuration**, and then do one of the following:
   - Click **Apps** > **Apps Management**.
   - Click **Device Solutions** > **Solutions (eSF)**.
   - Click **Embedded Solutions**.

4. From the list of installed applications, click the application you want to configure, and then click **Configure**.

Licensing the application

Licensing applications

Applications require a valid electronic license to run on select printers.

For more information on purchasing a license for an application, or for any other licensing information, contact your Lexmark representative.

Exporting and importing configuration files

After configuring an application, you can export your current settings into a file that can then be imported and used to configure that application on one or more additional printers.

Exporting and importing a configuration using the Embedded Web Server

You can export configuration settings into a text file, and then import it to apply the settings to other printers.

1. From the Embedded Web Server, click **Settings** or **Configuration**, and then do one of the following:
   - Click **Apps** > **Apps Management**.
   - Click **Device Solutions** > **Solutions (eSF)**.
   - Click **Embedded Solutions**.
2. From the list of installed applications, click the name of the application you want to configure.
3. Click **Configure**, and then do one of the following:
   - To export a configuration to a file, click **Export**, and then follow the instructions on the computer screen to save the configuration file.

     Note: If a **`JVM Out of Memory`** error occurs, then repeat the export process until the configuration file is saved.
   - To import a configuration from a file, click **Import**, and then browse to the saved configuration file that was exported from a previously configured printer.

     Notes:

     - Before importing the configuration file, you can choose to preview it first.
     - If a timeout occurs and a blank screen appears, then refresh the Web browser, and then click **Apply**.

Checking the Embedded Solutions Framework version

Checking which version of the Embedded Solutions Framework is installed on a printer

1. Obtain the printer IP address:
   - From the printer home screen
   - From the TCP/IP section in the Network/Ports menu
   - By printing a network setup page or menu settings page, and then finding the TCP/IP section

   Note: An IP address appears as four sets of numbers separated by periods, such as 123.123.123.123.
2. Open a Web browser, and then type the printer IP address in the address field.
3. From the Embedded Web Server, click **Reports** > **Device Settings**.
4. Scroll down until you see “Embedded Solutions” (usually found near the bottom).
5. In the Embedded Solutions section, note the value next to “Framework =”. This signifies the installed version.

Note: To view the complete list of supported printers for each version of the Embedded Web Server, see the *Readme* file.

Notices

Edition notice

April 2013

The following paragraph does not apply to any country where such provisions are inconsistent with local law: LEXMARK INTERNATIONAL, INC., PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions; therefore, this statement may not apply to you.

This publication could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in later editions. Improvements or changes in the products or the programs described may be made at any time.

References in this publication to products, programs, or services do not imply that the manufacturer intends to make these available in all countries in which it operates. Any reference to a product, program, or service is not intended to state or imply that only that product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any existing intellectual property right may be used instead. Evaluation and verification of operation in conjunction with other products, programs, or services, except those expressly designated by the manufacturer, are the user’s responsibility.

For Lexmark technical support, visit **http://support.lexmark.com**.

For information on supplies and downloads, visit **www.lexmark.com**.

Trademarks

Lexmark and the Lexmark logo are trademarks or registered trademarks of Lexmark International, Inc. in the United States and/or other countries.

All other trademarks are the property of their respective owners.

GOVERNMENT END USERS

The Software Program and any related documentation are "Commercial Items," as that term is defined in 48 C.F.R. 2.101, "Computer Software" and "Commercial Computer Software Documentation," as such terms are used in 48 C.F.R. 12.212 or 48 C.F.R. 227.7202, as applicable. Consistent with 48 C.F.R. 12.212 or 48 C.F.R. 227.7202-1 through 227.7207-4, as applicable, the Commercial Computer Software and Commercial Software Documentation are licensed to the U.S. Government end users (a) only as Commercial Items and (b) with only those rights as are granted to all other end users pursuant to the terms and conditions herein.

GNU Lesser General Public License

View the GNU Lesser General Public License online at **http://www.gnu.org/licenses/lgpl.html**.

Additional copyrights

This product includes software developed by:

Redistribution and use in source an binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions, and the following disclaimer.

2. Redistribution in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution:

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Index