Smart Card Authentication Client

Administrator's Guide
## Contents

### Overview .................................................................................................................. 3

### Configuring Smart Card Authentication Client .................................................. 4

- Configuring printer settings for use with the application ........................................ 4
  - Changing the panel login timeout .................................................................. 4
  - Installing certificates .................................................................................... 4
  - Setting the date and time .............................................................................. 5
  - Configuring TCP/IP settings ......................................................................... 6
- Securing access to the printer .............................................................................. 6
  - Setting up a security template ..................................................................... 7
  - Securing access to the home screen .............................................................. 7
  - Securing access to individual applications and functions ......................... 8
- Configuring login screen settings ...................................................................... 9
- Configuring manual login setup settings ........................................................... 10
- Configuring Smart Card setup settings .............................................................. 10
- Configuring advanced settings ....................................................................... 12

### Troubleshooting ..................................................................................................... 14

- Smart Card Authentication Client login issues ............................................... 14
- Smart Card Authentication Client authentication issues .................................. 16
- Smart Card Authentication Client LDAP issues ............................................... 23
- Smart Card Authentication Client licensing issues .......................................... 24

### Appendix ................................................................................................................. 26

- Configuring applications using the Embedded Web Server ............................... 26
- Licensing the application .................................................................................. 26
- Exporting and importing configuration files ..................................................... 26
- Checking the Embedded Solutions Framework version .................................. 27

### Notices ................................................................................................................... 28

- Edition notice ................................................................................................... 28

### Index ....................................................................................................................... 32
**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 about 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 about how to connect the printer to your network.
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 tell 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 THE SMART CARD READER IS SUPPORTED**

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

**MAKE SURE 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 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 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 10.

“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 10.
“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.
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” 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.


   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.


   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 10.

   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” 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 11.
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.
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” 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 11.
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 11.
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.
3. Make sure all certificates required for chain validation are configured correctly. See “Installing certificates” 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 27.

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.