Lexmark™

Smart Card Authentication

Administrator's Guide

August 2017 www.lexmark.com

Contents

Change history

August 2017

- Added instructions on changing the method for logging in.
- Added instructions on disabling the Device Quotas application.
- Added support for Brazilian Portuguese, Finnish, French, German, Italian, Simplified Chinese, and Spanish.

July 2016

- Added instructions on how to configure the Email to Self application.

January 2016

- Initial document release for multifunction products with a tablet-like touch-screen display.

Overview

Smart Card Authentication is a collection of applications used to secure access to printers and their functions. The applications let you log in to a printer manually or using a smart card, and then securely send e‑mails and release print jobs. You can also configure other security settings in an application, such as e‑mail signing and encryption.

The Smart Card Authentication bundle includes the following applications:

- **Smart Card Authentication Client**—Lets you secure access to printers by requiring users to log in using a smart card or a user name and password. You can secure access to 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 to secure other applications.
- **Smart card driver**—Lets the printer communicate with a supported smart card.
- **Display Customization**—Lets you upload images to the printer. You can use the images to create custom slide shows or to set the wallpaper and the screen saver of the printer. Secure this application using Smart Card Authentication client to require users to authenticate before they can access the printer home screen.
- **Secure E‑mail**—Lets you digitally sign and encrypt e‑mails sent from the printer. The application overrides the standard printer e‑mail function.
- **Secure Held Print Jobs**—Lets authenticated users view or release their held print jobs.

This document provides information on how to configure, use, and troubleshoot the applications.

Deployment readiness checklist

Make sure that:

□ You have installed the following in the printer:

- At least 512MB of RAM
- A smart card reader and its driver

□ You have disabled the Device Quotas application:

1. Obtain the printer IP address. Do either of the following:
   - Locate the IP address on the printer home screen.
   - From the printer home screen, touch **Settings** > **Network/Ports** > **Network Overview**.
2. Open a web browser, and then type the printer IP address.
3. Click **Apps** > **Device Quotas** > **Stop**.

You have the following to configure Smart Card Authentication Client:

□ Certificate Authority certificate (.cer file)

□ Lightweight Directory Access Protocol (LDAP) and Active Directory® accounts

____

□ Kerberos realm, domain, and domain controller

____

□ Kerberos file (for multiple domains)

Configuring the printer settings

You may need administrative rights to configure the printer settings.

Accessing the Embedded Web Server

1. Obtain the printer IP address. Do either of the following:
   - Locate the IP address on the printer home screen.
   - From the printer home screen, touch **Settings** > **Network/Ports** > **Network Overview**.
2. Open a web browser, and then type the printer IP address.

Setting the screen timeout

To prevent unauthorized access, you can limit the amount of time a user stays logged in to the printer without activity.

1. From the Embedded Web Server, click **Settings** > **Device** > **Preferences**.
2. In the Screen Timeout field, specify how long before the display becomes idle and the user is logged out. We recommend setting the value to 30 seconds.
3. Click **Save**.

Installing certificates manually

Note: To download the CA certificate automatically, see "Installing certificates automatically" on page 8.

Before configuring Kerberos or domain controller settings, install the CA certificate used for domain controller validation. If you want to use chain validation for the domain controller certificate, then install the entire certificate chain. Each certificate must be in a separate PEM (.cer) file.

1. From the Embedded Web Server, click **Settings** > **Security** > **Certificate Management**.
2. From the Manage CA Certificates section, click **Upload CA**, and then browse to the PEM (.cer) file.

   Sample certificate:

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

3. Click **Save**.

Installing certificates automatically

1. From the Embedded Web Server, click **Settings** > **Security** > **Certificate Management** > **Configure Certificate Auto Update**.
2. If you are prompted to join an Active Directory domain, then click **Join Domain**, and then type the domain information.

   Note: Make sure that the Active Directory domain matches the Kerberos realm or domain used in the smart card settings. For more information, see “Configuring the smart card settings” on page 14.
3. Select **Enable Auto Update**.

   Note: If you want to install the CA certificate without waiting for the scheduled run time, then select **Fetch Immediately**.
4. Click **Save**.

Configuring TCP/IP settings

1. From the Embedded Web Server, click **Settings** > **Network/Ports** > **TCP/IP**.
2. Do any of the following:
   - If you are using a static IP address, then type 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, then type the other domains in the Domain Search Order field. Use commas to separate multiple domains.

   Note: Use the domain name that is assigned to user workstations.
3. Click **Save**.

Setting the date and time

When using Kerberos authentication, make sure that the time difference between the printer and the domain controller does not exceed five minutes. You can manually update the date and time settings or use the Network Time Protocol (NTP) to sync the time with the domain controller automatically.

1. From the Embedded Web Server, click **Settings** > **Device** > **Preferences** > **Date and Time**.

   ## Configuring manually

   Note: Configuring the date and time manually disables NTP.

   a. From the Configure section, in the “Manually Set Date and Time” field, enter the appropriate date and time.

   b. Select the date format, time format, and time zone.

      Note: If you select **(UTC+user) Custom**, then specify the offset values for UTC (GMT) and DST.

Configuring NTP

a. From the Network Time Protocol section, select **Enable NTP**, and then type the IP address or host name of the NTP server.

b. If the NTP server requires authentication, then in the Enable Authentication menu, select **MD5 key**.

c. Depending on your printer model, either enter the key ID and password, or browse to the file containing the NTP authentication credentials.

2. Click **Save**.

Configuring LDAP network account settings

An LDAP network account is needed to send encrypted e-mails. Encryption certificates for recipients are added and configured from the LDAP server. For more information, contact your system administrator.

Note: A Kerberos network account is needed to create an LDAP + GSSAPI network account.

1. From the Embedded Web Server, click **Settings** > **Security** > **Login Methods**.
2. From the Network Accounts section, click **Add Login Method** > **LDAP**.
3. Select **LDAP** or **LDAP + GSSAPI**.
4. From the General Information section, configure the following:
   - **Setup Name**—A unique name for the LDAP network account.
   - **Server Address**

     Note: Make sure that the address is the same as the Smart Card Authentication Client domain controller address, or the KDC address in the Kerberos configuration file.
   - **Server Port**—If you are using SSL, then use port **636**. Otherwise, use port **389**.
5. From the Device Credentials section, clear **Anonymous LDAP Bind**, and then type the authentication credentials used to connect to the LDAP server.
6. If the LDAP server requires SSL, then from the Advanced Options section, set Use SSL/TLS to **SSL/TLS**.
7. From the Address Book Setup section, select **Use user credentials**.
8. Click **Save and Verify**.

Securing access to the printer

Securing access to the home screen

Users are required to authenticate before accessing the printer home screen.

Note: Before you begin, make sure that the Display Customization application is enabled in your printer. For more information, see the *Display Customization Administrator’s Guide*.

1. From the Embedded Web Server, click **Settings** > **Security** > **Login Methods**.
2. From the Public section, click **Manage Permissions**.
3. Expand **Apps**, clear **Slideshow**, **Change Wallpaper**, and **Screen Saver**, and then click **Save**.

4 From the Additional Login Methods section, click **Manage Permissions** beside Smart Card.

5 Select a group whose permissions you want to manage.

Note: The All Users group is created by default. More group names appear when you specify existing Active Directory groups in the Group Authorization List field. For more information, see "Configuring advanced settings" on page 15.

6 Expand **Apps**, and then select **Slideshow**, **Change Wallpaper**, and **Screen Saver**.

7 Click **Save**.

Securing access to individual applications and functions

Users are required to authenticate before accessing an application or a built-in printer function.

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

2 From the Public section, click **Manage Permissions**.

3 Restrict public access to the applications or functions that you want to secure. Do any of the following:

- For Secure E-mail, expand **Function Access**, clear **E-mail Function**, and then click **Save**.
- For Secure Held Print Jobs, expand **Apps**, clear **Secure Held Print Jobs**, and then click **Save**.
- For other applications or functions, expand one or more categories, clear the application or function, and then click **Save**.

4 From the Additional Login Methods section, click **Manage Permissions** beside Smart Card.

5 Select a group whose permissions you want to manage.

Note: The All Users group is created by default. More group names appear when you specify existing Active Directory groups in the Group Authorization List field. For more information, see "Configuring advanced settings" on page 15.

6 Select the applications or functions that you want authenticated users to access. Do any of the following:

- For Secure E-mail, expand **Function Access**, and then select **E-mail Function**.
- For Secure Held Print Jobs, expand **Apps**, and then select **Secure Held Print Jobs**.
- For other applications or functions, expand one or more categories, and then select the application or function.

7 Click **Save**.

Showing secured applications or functions on the home screen

By default, the secured applications or functions are hidden from the printer home screen.

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

2 In the Protected Features menu, select **Show**.

3 Click **Save**.

Configuring printer e-mail settings

The application overrides the printer e-mail function.

Configuring SMTP settings

1. From the Embedded Web Server, click **Settings** > **E-mail** > **E-mail Setup**.
2. Configure the following:
   - **Primary SMTP Gateway**—The IP address or host name of the server used for sending e-mail.

     Note: For Kerberos authentication, use the host name.
   - **Primary SMTP Gateway Port**
   - **Secondary SMTP Gateway**—The server IP address or host name of the secondary or backup SMTP server.
   - **Secondary SMTP Gateway Port**
   - **SMTP Timeout**
   - **Use SSL/TLS**
   - **Reply Address**
   - **SMTP Server Authentication**

     Notes:

     - If **Kerberos 5** is selected, then type the Kerberos realm.
     - If **NTLM** is selected, then type the NTLM domain.
     - If the SMTP server requires authentication but does not support Kerberos, then in the Reply Address field, type the printer IP address or host name.
   - **Device-Initiated E-mail**—The device credentials are required for device-initiated e-mails.

     Note: If **Use Device SMTP Credentials** is selected, then type the authentication credentials.
   - **User-Initiated E-mail**—The user credentials are required for user-initiated e-mails.

     Note: If you are using Kerberos authentication, then select **Use Session User ID and Password**.
3. Click **Save**.

Configuring default e-mail and scan settings

1. From the Embedded Web Server, click **Settings** > **E-mail** > **E-mail Defaults**.
2. Configure the settings.
3. If necessary, adjust the advanced imaging and the administrative controls settings.
4. Click **Save**.

Configuring Email to Self

Email to Self allows users to send a copy of the e-mail to their e-mail address. For more information, see the *Email to Self Administrator's Guide*.

Depending on your printer model, do either of the following:

For the built-in version of the application

1. From the Embedded Web Server, click **Settings** > **E-mail** > **E-mail Defaults** > **Admin Controls**.
2. Select **Limit E-mail Recipients**.
3. Click **Save**.

For the Embedded Solutions Framework (eSF) application

1. From the Embedded Web Server, navigate to the configuration page for the application:

   Apps > **Email to Self** > **Configure**
2. Select **Enable**.
3. Click **Apply**.

Configuring the applications

Configuring Smart Card Authentication Client

You may need administrative rights to configure the application.

Configuring the login screen settings

Use the login screen settings to set how you want users to log in to the printer.

1. From the Embedded Web Server, navigate to the configuration page for the application:

   Apps > **Smart Card Authentication Client** > **Configure**

2. From the Login Screen section, select the login type.
3. In the User Validation Mode menu, select the method for validating user certificates.
   - **Active Directory**—The user certificate on the smart card is validated using Kerberos authentication. This setting may require LDAP lookups.
   - **Active Directory with guest access**—Users who have smart cards but are not in the Active Directory can access some of the printer functions. A properly configured Online Certificate Status Protocol (OCSP) server is required. If the Active Directory authentication fails, then the application queries the OCSP server.
   - **Pin-Only**—Users can access only the applications or functions that do not require Kerberos authentication.
4. In the Validate Smart Card menu, select the method for authenticating users after tapping a smart card.
5. If necessary, allow users to change the login method.
6. Click **Apply**.

Configuring the manual login settings

For manual login, the printer uses the default domain specified in the Kerberos configuration file. If you use a different domain, then specify the domain name in the manual login settings.

1. From the Embedded Web Server, navigate to the configuration page for the application:

   Apps > **Smart Card Authentication Client** > **Configure**

2. From the Manual Login Setup section, in the Manual Login Domains field, type one or more domains.
3. Click **Apply**.

Configuring the smart card settings

Note: Make sure that the network connection between the printer and the authenticating server is configured properly. For more information, contact your system administrator.

1 From the Embedded Web Server, navigate to the configuration page for the application:

   Apps > **Smart Card Authentication Client** > **Configure**

2 From the Smart Card Setup section, in the Kerberos Information menu, select either of the following:

   - **Use device Kerberos setup file**—A Kerberos configuration file must be installed on the printer manually. Do the following:
     a From the Embedded Web Server, click **Settings** > **Security** > **Login Methods**.
     b From the Network Accounts section, click **Add Login Method** > **Kerberos**.
     c From the Import Kerberos File section, browse to the appropriate krb5.conf file.
     d If your network does not use reverse DNS lookup, then from the Miscellaneous Settings section, select **Disable Reverse IP Lookups**.
     e Click **Save and Verify**.
   - **Use simple Kerberos setup**—A Kerberos file is created on the printer automatically. Specify the following:
     - **Realm**—The realm must be typed in uppercase.
     - **Domain Controller**—Use commas to separate multiple values. The domain controllers are validated in the order listed.
     - **Domain**—The domain that must be mapped to the Kerberos realm specified in the Realm field. Use commas to separate multiple domains.

       Note: The domain is case sensitive.
     - **Timeout**—Enter a value from 3 to 30 seconds.

3 In the Domain Controller Validation menu, select the method for validating the domain controller certificate.

   Note: Before configuring this setting, make sure that the appropriate certificates are installed on the printer. For more information, see "Installing certificates manually" on page 7.

   - **Use device certificate validation**—The CA certificate that is installed on the printer is used.
   - **Use device chain validation**—The entire certificate chain that is installed on the printer is used.
   - **Use OCSP validation**—The OCSP server is used. The entire certificate chain must be installed on the printer. From the Online Certificate Status Protocol (OCSP) section, configure the following:
     - **Responder URL**—The IP address or host name of the OCSP responder or repeater, and the port number used. Use commas to separate multiple values.
       For example, `http://x:y`, where ***x*** is the IP address or host name, and ***y*** is the port number.
     - **Responder Certificate**—The X.509 certificate is used.
     - **Responder Timeout**—Enter a value from 5 to 30 seconds.
     - **Allow Unknown Status**—Users can log in even if the status of one or more certificates is unknown.

4 Click **Apply**.

Configuring advanced settings

1 From the Embedded Web Server, navigate to the configuration page for the application:

Apps > **Smart Card Authentication Client** > **Configure**

2 From the Advanced Settings section, select a session user ID.

Note: Some applications, such as Secure Held Print Jobs and Secure E-mail, require a value for the session user ID.

3 In the E-mail From Address menu, select where the printer retrieves the user e-mail address.

4 If necessary, select **Wait for user information** to retrieve all user information before the user is allowed to access the home screen or secure application.

If the following settings are set to LDAP Lookup, then select this option.

- Session User ID
- E-mail From Address

If the following settings are not empty, then select this option.

- Other User Attributes
- Group Authorization List

Note: If you are using manual login for Secure E-mail, then select this option to store the user e-mail address in the login session. To allow manual login users to send e-mail to themselves, enable “Send me a copy” in the printer e-mail settings.

5 If necessary, select **Use SSL for User Info** to retrieve user information from the domain controller using an SSL connection.

6 If necessary, in the Other User Attributes field, type other LDAP attributes that must be added to the session. Use commas to separate multiple values.

7 In the Group Authorization List, type the Active Directory groups that can access applications or functions. Use commas to separate multiple values.

Note: The groups must be in the LDAP server.

8 If DNS is not enabled in your network, then upload a hosts file.

Type the mappings in the text file in the format of ***xy***, where ***x*** is the IP address and ***y*** is the host name. You can assign multiple host names to an IP address. For example, **`255.255.255.255 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
```

9 Click **Apply**.

Configuring Secure E-mail

You may need administrative rights to configure the application.

Configuring the Secure E-mail settings

1. From the Embedded Web Server, navigate to the configuration page for the application:

   Apps > **Secure E-mail** > **Configure**

2. Configure the settings.

   Notes:

   - To sign an e-mail digitally, you must have a valid digital signing certificate, and be logged in using a smart card. Signing certificates are available only from the smart card. For more information, contact your system administrator.
   - To receive an encrypted e-mail, the recipient must be in the LDAP server address book and must have a valid encryption certificate. For more information, see "Configuring LDAP network account settings" on page 9.
   - To apply a security marking to an e-mail, enable the setting, and then type the text that you want to use.
   - For more information on each setting, see the mouse-over help.

3. Click **Apply**.

Configuring Secure Held Print Jobs

Restricting unauthenticated users from viewing held jobs

The built-in Held Jobs application can be used to view all held jobs in the printer. After setting up Secure Held Print Jobs, remove the Held Jobs icon from the printer home screen.

1. From the Embedded Web Server, click **Settings** > **Device** > **Visible Home Screen Icons**.
2. Clear **Held Jobs**.
3. Click **Save**.

Configuring the Secure Held Print Jobs settings

1. From the Embedded Web Server, navigate to the configuration page for the application:

   Apps > **Secure Held Print Jobs** > **Configure**

2. From the Release Options section, configure the settings.

   - **Release Method**—Specify how users print their held jobs.
   - **Display Print Jobs Sorted By**—Specify how the print jobs are listed on the display.

3. Click **Apply**.

Converting print jobs to secure held print jobs

1. From the Embedded Web Server, click **Settings** > **Security** > **Confidential Print Setup**.
2. Select **Require All Jobs to be Held**.
3. Click **Save**.

Importing or exporting a configuration file

Note: Importing configuration files overwrites the existing application configurations.

1. From the Embedded Web Server, navigate to the configuration page for the application. Do one of the following:
   - Click **Apps** > **Smart Card Authentication Client** > **Configure**
   - Click **Apps** > **Secure E-mail** > **Configure**
   - Click **Apps** > **Secure Held Print Jobs** > **Configure**
2. Click **Import** or **Export**.

Using the applications

Secure E-mail

Sending digitally signed and encrypted e-mail

Notes:

- When using manual login, configure the Smart Card Authentication Client authentication settings to retrieve all user information. For more information, see the *Smart Card Authentication Client Administrator's Guide*.
- To send an e-mail, make sure that you have a valid e-mail address assigned to your account.

1. Log in to the printer.
2. From the printer home screen, touch the application icon.
3. Load a document into the ADF tray or on the scanner glass.
4. Type the e-mail address of the recipient. Use commas to separate multiple e-mail addresses.
5. If necessary, configure other e-mail and scan settings.
6. Touch **Send**.
7. Digitally sign or encrypt the e-mail.

   Note: To sign an e-mail digitally, you must have a valid digital signing certificate, and be logged in using a smart card. Signing certificates are available only from the smart card. For more information, contact your system administrator.

8. If necessary, select a security option.
9. Touch **Send**.
10. If an encryption error occurs, then do either of the following:
    - To send an encrypted e-mail to only recipients with encryption certificates, select **Send Encrypted**.
    - To send an unencrypted e-mail to all recipients, select **Send Unencrypted**.
11. Touch **Send**.

Secure Held Print Jobs

Printing held jobs

Notes:

- Make sure to convert standard print jobs to secure held print jobs. For more information, see "Converting print jobs to secure held print jobs" on page 17.

- When using the print-and-hold feature, make sure that the print driver supports it. For more information, see the *Print Driver Help*. You can download the Lexmark Universal Print Driver for Windows and the print driver for Macintosh at **www.lexmark.com**.

1. With a document open, click **File** > **Print**.
2. Select a printer.

   Note: If necessary, configure the print settings.

3. If necessary, use the print-and-hold feature.
   - a Select the print-and-hold feature.
     - For Windows users, click **Properties**, **Preferences**, **Options**, or **Setup**, and then click **Print and Hold**.
     - For Macintosh users, select **Print and Hold** from the options menu.
   - b Select the print job type.
     - **Reserve**—Send print jobs and store them in the printer memory for printing later.
     - **Verify**—Print the first copy of a multiple-copy print job for verification. The remaining copies are held until they are printed or canceled.
     - **Repeat**—Print the job immediately and store a copy in the printer memory so that more copies can be printer later.

     Note: The Secure Held Print Jobs application does not support confidential print jobs.
   - c Type the user name from the LDAP directory associated with the print job.
4. Click **OK** or **Print**.
5. From the printer home screen, log in to your account, and then touch the application icon.

   Notes:

   - Make sure that the same account is used when logging in to the printer and when sending the print jobs.
   - Depending on how the application is configured, all jobs in your print release queue may print automatically when you touch the application icon. For more information, see “Configuring the Secure Held Print Jobs settings” on page 16.
6. If prompted, enter your authentication credentials.
7. Select the job or jobs that you want to print, and then specify the number of copies to print.
8. Touch **Print**.

Troubleshooting

Application error

Try one or more of the following:

Check the diagnostic log

1. Open a web browser, and then type ***`IP/se`***, where ***`IP`*** is the printer IP address.
2. Click **Embedded Solutions**, and then do the following:
   - a. Clear the log file.
   - b. Set the logging level to **Yes**.
   - c. Generate the log file.
3. Analyze the log, and then resolve the problem.

   Note: After resolving the problem, set the logging level to **No**.

Contact your Lexmark representative

Login issues

Cannot detect the card reader or the smart card

Try one or more of the following:

Make sure that the card reader is connected properly to the printer

Make sure that the card reader and the smart card are compatible

Make sure that the card reader is supported

For a list of supported card readers, see the *Readme* file.

Make sure that the card reader driver is installed on the printer

Contact your Lexmark representative

User is locked out

Try one or more of the following:

Increase the allowed number of login failures and lockout time

Note: This solution is applicable only in some printer models.

1. From the Embedded Web Server, click **Settings** > **Security** > **Login Restrictions**.
2. Increase the allowed number of login failures and the lockout time.
3. Click **Save**.

   Note: The new settings take effect after the lockout time has passed.

Reset or replace the smart card

Cannot validate PIN

Try one or more of the following:

Make sure that the PIN that you entered is correct

Contact your system administrator

Cannot log in manually

Try one or more of the following:

Make sure that the domain specified in the Kerberos configuration is correct

Specify the domains in the manual login settings

For more information, see “Configuring the manual login settings” on page 13.

Contact your system administrator

Printer home screen does not lock

Try one or more of the following:

Make sure that Display Customization is enabled

For more information, see the *Display Customization Administrator’s Guide*.

Secure access to the home screen

For more information, see “Securing access to the home screen” on page 9.

Authentication issues

Kerberos authentication failed

Try one or more of the following:

Check the diagnostic log

1. Open a web browser, and then type ***IP*/se**, where ***IP*** is the printer IP address.
2. Click **Embedded Solutions**, and then do the following:
   - a. Clear the log file.
   - b. Set the logging level to **Yes**.
   - c. Generate the log file.
3. Analyze the log, and then resolve the problem.

   Note: After analyzing the log, set the logging level to **No**.

Make sure that the configuration file is installed on the printer

- If you are using simple Kerberos setup to create the Kerberos configuration file, then do the following:
  1. From the Embedded Web Server, navigate to the configuration page for the application:

     Apps > **Smart Card Authentication Client** > **Configure**
  2. From the Simple Kerberos Setup section, make sure that the realm, domain controller, domain, and timeout values are correct.
- If you are using the device Kerberos setup file, then do the following:
  1. From the Embedded Web Server, click **Settings** > **Security** > **Login Methods**.
  2. From the Network Accounts section, click **Kerberos** > **View File**.
  3. If the Kerberos configuration file is not installed, then in the Import Kerberos File section, browse to the appropriate krb5.conf file.
  4. Click **Save and Verify**.

Make sure that the configuration file content and format are correct

- If you are using simple Kerberos setup, then modify the simple Kerberos setup settings.
- If you are using the device Kerberos setup file, then modify and reinstall the file.

Make sure that the Kerberos realm is in uppercase

- If you are using simple Kerberos setup, then do the following:
  1. From the Embedded Web Server, navigate to the configuration page for the application:

     Apps > **Smart Card Authentication Client** > **Configure**
  2. From the Simple Kerberos Setup section, make sure that the realm is correct and that it is typed in uppercase.
  3. Click **Apply**.

- If you are using the device Kerberos setup file, then do the following:
  1. From the Embedded Web Server, click **Settings** > **Security** > **Login Methods**.
  2. From the Network Accounts section, click **Kerberos** > **View File**.
  3. Make sure that the realms in the configuration file are typed in uppercase.

Specify the Microsoft® Windows® operating system domain

- If you are using simple Kerberos setup, then do the following:
  1. From the Embedded Web Server, navigate to the configuration page for the application:

     Apps > **Smart Card Authentication Client** > **Configure**
  2. From the Simple Kerberos Setup section, in the Domain field, add the Windows domain in the Domain field.

     For example, if the Domain field value is **`DomainName,.DomainName`**, and the Windows domain is **`x.y.z`**, then change the Domain field value to **`DomainName,.DomainName,x.y.z`**.

     Note: The domain is case sensitive.
  3. Click **Apply**.
- If you are using the device Kerberos setup file, then add an entry to the **`domain_realm`** section of the file. Type the Windows domain realm in uppercase, and then reinstall the file on the printer.

Contact your Lexmark representative

Cannot generate or read certificate information from the smart card

Try one or more of the following:

Make sure that the certificate information on the smart card is correct

Contact your Lexmark representative

Cannot validate the domain controller

Try one or more of the following:

Make sure that the realm, domain controller, and domain in the Kerberos configuration file are correct

- If you are using simple Kerberos setup, then do the following:
  1. From the Embedded Web Server, navigate to the configuration page for the application:

     Apps > **Smart Card Authentication Client** > **Configure**
  2. From the Simple Kerberos Setup section, make sure that the realm, domain controller, and domain are correct.
- If you are using the device Kerberos setup file, then do the following:
  1. From the Embedded Web Server, click **Settings** > **Security** > **Login Methods**.
  2. From the Network Accounts section, click **Kerberos** > **View file**.
  3. Make sure that the realm, domain controller, and domain are correct.

Increase the domain controller timeout value

- If you are using simple Kerberos setup, then do the following:
  1. From the Embedded Web Server, navigate to the configuration page for the application:

     Apps > **Smart Card Authentication Client** > **Configure**
  2. From the Simple Kerberos Setup section, in the Timeout field, enter a value from 3 to 30 seconds.
  3. Click **Apply**.
- If you are using the device Kerberos setup file, then enter a value from 3 to 30 seconds. When you are finished, reinstall the file on the printer. For more information on configuring the smart card settings, see "Configuring the smart card settings" on page 14.

Make sure that the domain controller is available

Use commas to separate multiple values. The domain controllers are validated in the order listed.

Make sure that port 88 is not blocked between the printer and the domain controller

Cannot validate the domain controller certificate

Try one or more of the following:

Make sure that the certificates that are installed on the printer are correct

For more information, see "Installing certificates manually" on page 7.

Make sure that the domain controller validation method is configured properly

1. From the Embedded Web Server, navigate to the configuration page for the application:

   Apps > **Smart Card Authentication Client** > **Configure**
2. From the Smart Card Setup section, in the Domain Controller Validation menu, select the appropriate validation method.
3. Click **Apply**.

Cannot find realm in the Kerberos configuration file

Add or change the realm

- If you are using simple Kerberos setup, then do the following:
  1. From the Embedded Web Server, navigate to the configuration page for the application:

     Apps > **Smart Card Authentication Client** > **Configure**
  2. From the Simple Kerberos Setup section, in the Realm field, add or change the realm. The realm must be typed in uppercase.

     Note: The simple Kerberos setup does not support multiple Kerberos realm entries. If multiple realms are needed, then install a Kerberos configuration file containing the necessary realms.
  3. Click **Apply**.
- If you are using the device Kerberos setup file, then add or change the realm in the file. The realm must be typed in uppercase. When you are finished, reinstall the file on the printer.

Domain controller and device clocks are out of sync

Make sure that the time difference between the printer and the domain controller does not exceed five minutes

For more information, see "Setting the date and time" on page 8.

Cannot validate the domain controller certificate chain

Try one or more of the following:

Make sure that all certificates required for chain validation are installed on the printer and that the information is correct

For more information, see "Installing certificates manually" on page 7.

Make sure that the certificate chain is from the domain controller to the root CA

Make sure that all certificates are not expired

1. From the Embedded Web Server, click **Settings** > **Security** > **Certificate Management**.
2. Make sure that the Valid From and Valid To dates have not expired.

Allow users to log in even if the status of one or more certificates is unknown

1. From the Embedded Web Server, navigate to the configuration page for the application:
   Apps > **Smart Card Authentication Client** > **Configure**
2. From the Online Certificate Status Protocol (OCSP) section, select **Allow Unknown Status**.
3. Click **Apply**.

Contact your Lexmark representative

Cannot connect to the OCSP responder

Try one or more of the following:

Make sure that the OCSP responder URL is correct

1. From the Embedded Web Server, navigate to the configuration page for the application:
   Apps > **Smart Card Authentication Client** > **Configure**
2. From the Online Certificate Status Protocol (OCSP) section, make sure that the responder URL is correct.
3. Click **Apply**.

Increase the responder timeout value

1. From the Embedded Web Server, navigate to the configuration page for the application:

   Apps > **Smart Card Authentication Client** > **Configure**
2. From the Online Certificate Status Protocol (OCSP) section, in the Responder Timeout field, enter a value from 5 to 30.
3. Click **Apply**.

Cannot validate the domain controller certificate against the OCSP responder

Try one or more of the following:

Make sure that the OCSP responder URL and the responder certificate are configured correctly

1. From the Embedded Web Server, navigate to the configuration page for the application:

   Apps > **Smart Card Authentication Client** > **Configure**
2. From the Online Certificate Status Protocol (OCSP) section, in the Responder URL field, specify the following:
   - IP address or host name of the OCSP responder or repeater
   - Port number used

   For example, **`http://`*`x`*`:`*`y`***, where ***x*** is the IP address and ***y*** is the port number.
3. In the Responder Certificate field, browse to the appropriate certificate.
4. Click **Apply**.

Make sure that the domain controller returns the correct certificate

Make sure that the OCSP responder validates the correct domain controller certificate

Cannot access individual applications and functions on the printer

Try one or more of the following:

Allow secure access to applications or functions

For more information, see “Securing access to individual applications and functions” on page 10.

If the user belongs to an Active Directory group, then make sure that the group is authorized to access the applications and functions

Secure E-mail issues

Cannot send e-mail using the application

Make sure that the Device Quotas application is disabled

From the Embedded Web Server, click **Apps** > **Device Quotas** > **Stop**.

Cannot retrieve the user e-mail address

Try one or more of the following:

Make sure that the printer e-mail function is secured

For more information, see “Securing access to the printer” on page 9.

Make sure that the user e-mail address is retrieved correctly

1. From the Embedded Web Server, navigate to the configuration page for Smart Card Authentication Client:

   Apps > **Smart Card Authentication Client** > **Configure**

2. From the Advanced Settings section, in the E-mail From Address menu, select where the printer retrieves the user e-mail address.
3. Select **Wait for user information**.
4. Click **Apply**.

Contact your Lexmark representative

Cannot retrieve the user signing certificate

Try one or more of the following:

Make sure that a signing certificate is available for the user

Install the appropriate signing certificate on the user’s smart card.

Make sure that the certificates are retrieved correctly

1. From the Embedded Web Server, navigate to the configuration page for Smart Card Authentication Client:

   Apps > **Smart Card Authentication Client** > **Configure**

2. From the Advanced Settings section, select **Wait for user information**.
3. Click **Apply**.

Contact your Lexmark representative

Signing certificate unavailable for the user

Try one of the following:

Send the e-mail without a digital signature

Make sure that a signing certificate is available for the user

Install the appropriate signing certificate on the user’s smart card.

Contact your system administrator

Cannot retrieve certificates from the LDAP server

Try one or more of the following:

Make sure that the network cables are connected securely and that the network settings of the printer are configured correctly

For more information, see the printer *User’s Guide*.

Make sure that the server and firewall settings are configured to allow communication between the printer and the LDAP server on port 389 or port 636

If you are using SSL, then use port **636**. Otherwise, use port **389**.

Make sure that the LDAP server address contains the host name, not the IP address

For more information, see “Configuring LDAP network account settings” on page 9.

If the LDAP server requires SSL, then make sure that the SSL settings are correct

For more information, see “Configuring LDAP network account settings” on page 9.

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

Make sure that all LDAP attributes are correct

Contact your system administrator

Cannot encrypt e-mail for one or more recipients

Try one or more of the following:

Send an unencrypted e-mail to recipients without an encryption certificate and an encrypted e-mail to recipients with an encryption certificate

Select **Send to All**. For more information, see “Sending digitally signed and encrypted e-mail” on page 18.

Send an encrypted e-mail to only recipients with encryption certificates

Select **Send Encrypted**. For more information, see “Sending digitally signed and encrypted e-mail” on page 18.

Send unencrypted e-mail to all recipients

Select **Send Unencrypted**. For more information, see “Sending digitally signed and encrypted e-mail” on page 18.

Contact your Lexmark representative

Cannot connect to the e-mail server

Try one or more of the following:

Make sure that the printer is connected to a domain

For more information, see “Configuring TCP/IP settings” on page 8.

Make sure that the SMTP Server Authentication setting is correct

1. From the Embedded Web Server, click **Settings** > **E-mail** > **E-mail Setup**.
2. In the SMTP Server Authentication menu, do one of the following:
   - If the SMTP server requires user credentials, then select **Kerberos 5**.
   - If Kerberos is not supported, then select **No authentication required**.
   - If the SMTP server requires authentication but does not support Kerberos, then in the Reply Address field, type the printer IP address or host name.
3. Click **Save**.

Note: For more information, see “Configuring SMTP settings” on page 11.

If the SMTP server uses Kerberos, then make sure that the host names of the primary and secondary SMTP gateways are correct

1. From the Embedded Web Server, click **Settings** > **E-mail** > **E-mail Setup**.
2. In the Primary SMTP Gateway and Secondary SMTP Gateway fields, type the host name of the gateway instead of the IP address.
3. Click **Save**.

Make sure that the server and firewall settings are configured to allow communication between the printer and the SMTP server on port 25

Make sure that the network cables are connected securely and that the network settings of the printer are configured correctly

For more information, see the printer *User’s Guide*.

Contact your system administrator

Cannot send a copy to self

Try one or more of the following:

Make sure that all user information is entered in the login session

Make sure that the printer is configured to retrieve all user information

1. From the Embedded Web Server, navigate to the configuration page for Smart Card Authentication Client:

   Apps > **Smart Card Authentication Client** > **Configure**

2. From the Advanced Settings section, select **Wait for user information**.
3. Click **Apply**.

Make sure that Email to Self is configured correctly

For more information, see “Configuring Email to Self” on page 12.

Contact your Lexmark representative

Secure Held Print Jobs issues

Cannot determine the user ID

This error indicates that the local account, network account, or authentication module login method is not setting the user ID for the session. Try one or more of the following:

Make sure that the application is secured

For more information, see “Configuring the Secure Held Print Jobs settings” on page 16.

Make sure that the session user ID is set correctly

From the Embedded Web Server, do one of the following:

Using a local account login method

1. Click **Settings** > **Security** > **Login Methods**.
2. From the Local Accounts section, click the local account type, and then make sure that the account has a user name.
3. Click **Save**.

Using a network account login method

1. Click **Settings** > **Security** > **Login Methods**.
2. From the Network Accounts section, click the network account, and then make sure that the account has the correct user ID. For more information, contact your system administrator.
3. Click **Save**.

Using an authentication module

1. Click **Apps**.
2. Select the authentication module, and then click **Configure**.
3. Specify the appropriate setting for the session user ID.
4. Click **Save** or **Apply**.

Contact your solution provider

If you still cannot resolve the problem, then contact your solution provider.

No print jobs are available for the user

Try one or more of the following:

Make sure that jobs are sent to the correct printer and have not expired

The user may have sent the jobs to a different printer, or the jobs may have been automatically deleted because they were not printed in time.

Make sure that the session user ID is set correctly

From the Embedded Web Server, do one of the following:

Using a local account login method

1. Click **Settings** > **Security** > **Login Methods**.
2. From the Local Accounts section, click the local account type, and then make sure that the account has a user name.
3. Click **Save**.

Using a network account login method

1. Click **Settings** > **Security** > **Login Methods**.
2. From the Network Accounts section, click the network account, and then make sure that the account gets the correct user ID. For more information, contact your system administrator.
3. Click **Save**.

Using an authentication module

1. Click **Apps**.
2. Select the authentication module, and then click **Configure**.
3. Specify the appropriate setting for the session user ID.
4. Click **Save** or **Apply**.

Contact your solution provider

If you still cannot resolve the problem, then contact your solution provider.

LDAP issues

LDAP lookups fail

Try one or more of the following:

Make sure that the server and firewall settings are configured to allow communication between the printer and the LDAP server on port 389 and port 636

If reverse DNS lookup is not used in your network, then disable it in the Kerberos settings

1. From the Embedded Web Server, click **Settings** > **Security**.
2. From the Network Accounts section, click **Kerberos**.
3. From the Miscellaneous Settings section, select **Disable Reverse IP Lookups**.
4. Click **Save and Verify**.

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

1. From the Embedded Web Server, navigate to the configuration page for the application:
   Apps > **Smart Card Authentication Client** > **Configure**
2. From the Advanced Settings section, select **Use SSL for User Info**.
3. Click **Apply**.

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

Make sure that all LDAP attributes are correct

License error

Contact your Lexmark representative

Notices

Edition notice

August 2017

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**.

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.

Trademarks

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

Microsoft, Windows, and Active Directory are either registered trademarks or trademarks of the Microsoft group of companies in the United States and other countries.

All other trademarks are the property of their respective owners.

Index