



Lexmark™

Card Authentication

Version 5.8

Administrator's Guide

December 2020

www.lexmark.com

Contents

- Change history..... 4**
- Overview..... 5**
- Deployment readiness checklist..... 6**
- Configuring the application..... 8**
 - Accessing the Embedded Web Server..... 8
 - Setting the application as the default login method..... 8
 - Configuring printer-based card validation..... 8
 - Configuring web service card validation..... 9
 - Configuring LDAP card validation..... 10
 - Configuring Identity Service card validation..... 10
 - Configuring PIN authentication..... 11
 - Assigning a login method for card registration..... 12
 - Assigning a login method for manual login..... 12
 - Configuring administrator authentication..... 13
 - Showing realms for user accounts..... 13
 - Configuring the login screen..... 13
 - Securing access to individual applications and functions..... 14
 - Configuring the badge logout delay..... 15
 - Importing or exporting a configuration file..... 15
- Managing the application..... 16**
 - Accessing the status page for the application..... 16
 - Managing client printers and user accounts..... 16
 - Reassigning printer roles..... 17
- Using the application..... 19**
 - Registering users..... 19
 - Registering a PIN..... 19
 - Logging in to the printer manually..... 19
- Troubleshooting..... 20**
 - Application error..... 20

Authentication error.....20

User is locked out..... 21

Cannot register a client printer.....21

Cannot connect to the LDAP server.....21

Some settings do not appear in the configuration page..... 22

User has no access privileges..... 22

Cannot find realm information..... 22

Frequently asked questions..... 24

Notices..... 25

Index..... 26

Change history

December 2020

- Added information about a warning related to a missing card reader.

June 2020

- Added information on new settings for verifying certificates.
- Removed information on license requirement.

July 2019

- Added instructions on configuring PIN-only authentication.

December 2018

- Added instructions on configuring administrator authentication.

August 2017

- Added information on the following:
 - Lock screen settings
 - Custom profile
- Removed information on using the Display Customization application to manage the login screen.

August 2016

- Added information on the following:
 - PIN authentication support
 - Quick access buttons for manual login and PIN login

July 2016

- Added information on the following:
 - Manual login
 - Multiple-domain support
 - Use of service accounts to authenticate to the Identity Service Provider
 - Multiple Kerberos realms for card registration and manual login
 - Custom login text color
 - Group permissions

January 2016

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

Overview

Use the application to secure access to a printer using a card reader. When users badge in, their credentials are authenticated using either of the following:

- A master printer. If the master printer is offline, then a backup printer functions as the master printer until the master printer becomes online.

Note: When setting up the printers, make sure that they are on the same network.

- Lightweight Directory Access Protocol (LDAP), Lexmark™ Document Distributor (LDD) servers, or Identity Service Providers depending on the authentication set by the organization.

You can also configure the application to let users log in using a service account, user name, user name and password, or PIN.

This document provides instructions on how to configure, use, and troubleshoot the application.

Deployment readiness checklist

Before you begin, make sure that:

- At least one local or network account is set up on your printer. For more information, contact your system administrator.
- A card reader and its driver are installed in the printer.
- You have the web server address to configure PIN authentication.

You have the following information to configure printer-based card validation:

- Host name or IP address of the master printer

- Host name or IP address of the backup printer

You have the following information to configure web service card validation:

- Server URL

- Registration and lookup interface version

You have the following information to configure LDAP card validation:

Note: You can also use an existing LDAP network account that is configured in your printer.

- Server address

- Server port number

- Search base

- Login user name

- Login password

LDAP attributes

- User ID

- Badge ID

- User information, optional

You have the following information to configure Identity Service card validation:

Identity Service Provider address

Badge Service Provider address

Configuring the application

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 application as the default login method

- 1 From the Embedded Web Server, click **Settings > Security > Login Methods**.
- 2 Click **Change** beside Default Control Panel Login Method.
- 3 In the Control Panel menu, select **Card Authentication**.
- 4 Click **Save**.

Configuring printer-based card validation

Use printer-based validation when validating users through a master printer.

- 1 From the Embedded Web Server, navigate to the configuration page for the application:
Apps > Card Authentication > Configure
- 2 From the User Authentication section, set Card Validation to **Printer-based**.
Note: The Verify Certificate setting is applicable only to Identity Service and Web Service validation.
- 3 From the Printer-based Settings section, do the following:
 - a Select a role for the printer.
 - **Master**—The printer maintains the list of registered users.
 - **Backup**—If the master printer is offline, then the backup printer assumes the role of the master until the master printer becomes online.
 - **Client**—The printer does not store user information. A master or backup printer is required to validate user credentials.

Notes:

- If you have one printer, then set it as a master printer.
- If you have two printers, then set one as a master printer and the other as a backup printer.
- If you have three or more printers, then set one as master printer, one as backup printer, and the rest as client printers.

- b Type the host name or IP address of the master printer and backup printer.

Notes:

- When setting up a backup printer, the host name or IP address of the master printer is required.

- When setting up client printers, the host names or IP addresses of the master and the backup printers are required.
- Before assigning a client printer to a new master printer, delete it from the old master printer.

4 Click **Save**.

Configuring web service card validation

Use web service validation when validating users through an LDD server.

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

Apps > Card Authentication > Configure

2 From the User Authentication section, set Card Validation to **Web Service**.

3 Select **Verify Certificate** to validate all connections to the server. If Verify Certificate is not selected, then CA will not be validated.

4 In the Verification Mode menu, select either **chain** or **peer**.

Note: The default value is chain.

5 Upload the server SSL certificate to connect securely to the server.

6 In the CheckHosts field, type the additional host names (other than the default server URL) to verify the entries in the certificate. Use commas to separate multiple host names.

Note: By default, that white list contains just the server URL. Type additional host names in the CheckHosts field to include them in the white list.

7 From the Web Service Settings section, type the URL of the LDD server.

8 If necessary, adjust the server connection timeout.

9 Set the registration interface. Select either of the following:

- **Version 1**—Only the badge ID and user ID are shown in the Badge Information dialog box.
- **Version 2**—The following are shown in the Badge Information dialog box:
 - Badge ID
 - User ID
 - IP address
 - Host name

10 Set the lookup interface. To record when and where the badge was last used, select **Version 2**.

11 Click **Save**.

Configuring LDAP card validation

Use LDAP validation when validating users through an LDAP server.

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

Apps > Card Authentication > Configure

- 2 From the User Authentication section, set Card Validation to **LDAP**.

Note: The Verify Certificate setting is applicable only to Identity Service and Web Service validation.

- 3 From the LDAP Server Setup section, configure the settings.

Note: If **Use Address Book** is selected, then the application uses the LDAP settings that are already configured in the printer network accounts. If there are multiple LDAP accounts configured in the printer, then the application selects the setup name based on alphabetical order. Setup names starting in uppercase letters are selected first over lowercase letters.

- **Server Address**—Type the LDAP server address.
- **Server Port**—Enter the LDAP port number.
- **Use SSL**—Select this option to enable a secure connection.
- **Search Base**—Type the node in the LDAP server where user accounts reside. You can type multiple search bases, separated by commas.
- **Login Username**—Type the LDAP account user name. In some LDAP server configurations, user credentials are required.
- **Login Password**—Type the LDAP account password. In some LDAP server configurations, user credentials are required.

- 4 From the LDAP Attributes section, configure the settings.

- **User ID**—Type the LDAP attribute that the application searches for when authenticating user credentials. For example, **samaccountname**, **uid**, **cn**, or a user-defined attribute.
- **Badge ID**—Type the LDAP attribute for authenticating users with their assigned badge numbers. For example, **employeeNumber**.
- **User Information**—Type the other user information that the application can retrieve from the LDAP server.
- **Group Membership Attribute**—Type the LDAP attribute required for group search.
- **Group List**—Type the LDAP group where the user accounts belong. The groups specified are added to the group permissions list of the application, where you can set the specific access controls for each group. You can type multiple group names, separated by commas.

- 5 Click **Save**.

Configuring Identity Service card validation

Use Identity Service card validation when validating users through an Identity Service Provider.

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

Apps > Card Authentication > Configure

- 2 From the User Authentication section, set Card Validation to **Identity Service**.

- 3** Select **Verify Certificate** to validate all connections to the server. If Verify Certificate is not selected, then CA will not be validated.
- 4** In the Verification Mode menu, select either **chain** or **peer**.
Note: The default value is chain.
- 5** Upload the server SSL certificate to connect securely to the server.
- 6** In the CheckHosts field, type the additional host names (other than the default server URL) to verify the entries in the certificate. Use commas to separate multiple host names.
Note: By default, that white list contains just the server URL. Type additional host names in the CheckHosts field to include them in the white list.
- 7** From the Identity Service Settings section, type the host name or IP address of the Identity Service Provider.
- 8** Type the host name or IP address of the Badge Service Provider.
- 9** Set the Application Access Policy.
 - **Continue**—Continue using the printer even if connecting to the Identity Service server fails.
 - **Fail**—Go back to the login screen if connecting to the Identity Service server fails.
- 10** If you have a Client ID and Client Secret from the Identity Service Provider, then type the information in their corresponding fields.
- 11** Adjust the network and socket timeouts.
- 12** Upload the server SSL certificate to connect securely to the server.
- 13** To allow users to log in to the printer using a separate service account, select **Use Service Account**, and then enter the service account credentials.
- 14** Set Card Registration to **Identity Service**.
- 15** Click **Save**.

Configuring PIN authentication

Before you begin, make sure that your credentials are set up in the local or network account settings of the printer.

- 1** From the Embedded Web Server, navigate to the configuration page for the application:
Apps > Card Authentication > Configure
- 2** From the User Authentication section, in the PIN Login section, select **Enable PIN Login**.
- 3** Select **Show on Screen Saver** to show the PIN Login button on the screen saver.
- 4** From the PIN Settings section, in the Required Credentials menu, select a login method.
 - **Userid and PIN**—Requires a user name and PIN for authentication.
 - **PIN only**—Requires a PIN for authentication.
Note: If the PIN only method is selected, then you cannot register a new PIN or update an existing one.
- 5** Type the web server address where the PINs are saved.

6 If necessary, type the PIN login text, and then set the minimum PIN length.

Note: If the PIN login text field is left blank, then the default PIN login text is shown. The default PIN login text is **Type your user credentials to log in.**

7 If necessary, type the invalid PIN error messages.

Note: If the text fields are left blank, then the default error messages are shown. The default error messages are **Invalid PIN length.** and **Invalid PIN.**

8 If necessary, adjust the network and socket timeouts.

Note: The default value for network timeout and socket timeout is 15 seconds.

9 Click **Save**.

Assigning a login method for card registration

Before you begin, make sure that your credentials are set up in the local or network account settings of the printer.

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

Apps > Card Authentication > Configure

2 From the User Authentication section, in the Card Registration menu, select a login method.

Note: If you want to use Kerberos, Active Directory, or LDAP+GSSAPI, then select a realm. If the selected login method has multiple domains, then the selected realm is the default realm shown during card registration.

3 Click **Save**.

Assigning a login method for manual login

Before you begin, make sure that your credentials are set up in the local or network account settings of the printer.

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

Apps > Card Authentication > Configure

2 From the User Authentication section, in the Manual Login Settings section, set **Manual Login** to your preferred login method.

Notes:

- If Manual Login is set to Identity Service and Use Service Account is enabled, then users are not prompted to enter credentials manually. The application uses the service account to log in.
- If you want to use Kerberos, Active Directory, or LDAP+GSSAPI, then select a realm. If the selected login method has multiple domains, then the selected realm is the default realm shown during manual login.

3 Select **Show on Screen Saver** to show the Manual Login button in the screen saver.

4 Click **Save**.

Configuring administrator authentication

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

Apps > Card Authentication > Configure

2 From the User Authentication section, in the Admin Login Settings section, set **Admin Login** to your preferred login method.

Note: Make sure that you have configured a local administrator account for the printer and that you have configured the permissions for the Device Admin Group. By default, functions and menus are not permitted for this group.

3 Select an authorized group that can use the administrator login feature.

Note: This setting is applicable only to user name, and user name and password accounts.

4 Select **Show on Screen Saver** to show the Admin Login button in the screen saver.

5 Click **Save**.

Showing realms for user accounts

The Use Selected Realm feature is applicable only if the login methods for card registration and manual login are Kerberos, Active Directory, or LDAP+GSSAPI. This feature is also applicable only if card validation is set to Web Service or Printer-based.

For card registration, if this feature is enabled, then the badge ID that is registered is in username@realm format.

For manual login, if this feature is enabled, then the user name shown in the printer control panel is in username@realm format.

These settings do not apply to PIN login and PIN registration.

To enable this feature, do the following:

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

Apps > Card Authentication > Configure

2 From the Advanced Settings section, select **Use Selected Realm**.

3 Click **Save**.

Configuring the login screen

Note: Make sure that the screen saver setting of the Display Customization application is disabled. For more information, see the *Display Customization Administrator Guide*.

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

Apps > Card Authentication > Configure

2 From the Login Screen Settings section, do any of the following:

- To customize the login message, select **Use Custom Login Text**, and then type the message.
- Set the custom login text color to black or white.

- To change the login screen background, select **Use Custom Image for Login Screen**, and then upload the image file.
 - To customize the message for manual login, in the Manual Login Text field, type the message.
 - To customize the message for administrator login, in the Admin Login Text field, type the message.
 - Enable copying and faxing without logging in.
 - Disable the warning when no card reader is attached.
- 3** From the Lock Screen Settings section, select the location for the login text, and then type the profile name or ID of the application. The profile launches automatically after login.
 - 4** From the Custom Profile section, type the profile name or ID of the application or printer function, and then type the custom name for the icon. If necessary, select **Use Custom Icon**, and then upload the image file.
 - 5** Click **Save**.

Note: The login screen can be disabled only in environments that use Identity Service.

Enabling public access to copy and fax functions

- 1** From the Embedded Web Server, click **Settings > Security > Login Methods**.
- 2** From the Public section, click **Manage Permissions**.
- 3** Expand **Function Access**, and then select **Copy Function** and **Fax Function**.
- 4** Click **Save**.

Securing access to individual applications and functions

To require users to authenticate before accessing an application or a printer function, do the following:

Restrict public access to the applications or functions

- 1** From the Embedded Web Server, click **Settings > Security > Login Methods**.
- 2** From the Public section, click **Manage Permissions**.
- 3** Expand one or more categories, and then clear the application or function that you want to secure.
- 4** Click **Save**.

Manage group permissions

Note: If the Admin Login feature is enabled, then configure the Device Admin Group permissions.

- 1** From the Additional Login Methods section, click **Manage Permissions** beside Card Authentication.
- 2** Select a group whose permissions you want to manage.
Note: The list shows the groups that are added in the LDAP Group List in the application configuration page.
- 3** Expand one or more categories, and then select the application or function that you want to be accessible.
- 4** Click **Save**.

Notes:

- During login, the application applies the permissions of the group where the user belongs to. If the user belongs to multiple groups, then the application merges all permissions. For example, only copying is allowed for Group A, and only faxing is allowed for Group B. If the user belongs to both groups, then the application allows the user to both copy and fax.
- The group permissions of the assigned login method for card registration and manual login must have the same group permissions configured in the application.

Configuring the badge logout delay

You can set how long before the printer registers a succeeding tap as a logout. If you tap your card within the specified time, then you remain logged in. If you tap your card after the timer expires, then you are logged out.

If you are logged in, and another user logs in using a card, then you are logged out immediately and the other user is logged in. This behavior still takes effect even though the badge logout delay timer is active.

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

Apps > Card Authentication > Configure

2 From the Advanced Settings section, set the badge logout delay.

3 Click **Save**.

Importing or exporting a configuration file

Importing configuration files overwrites the existing application configurations.

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

Apps > Card Authentication > Configure

2 Click **Import/Export Configuration**.

3 Do either of the following:

- Browse to the configuration file, and then click **Import**.
- Click **Export**.

Managing the application

For printer-based card validation, you can manage the client printers and user accounts in the status page of the application.

Notes:

- The status page for the application is available only when using printer-based authentication.
- If a printer is not assigned with a role, then it appears as Not Configured in the status page for the application. Make sure to set the role of the printer. For more information, see [“Configuring printer-based card validation” on page 8](#).

Accessing the status page for the application

Use the status page to monitor printer activity.

- 1 From the Embedded Web Server, click **Apps > Launch Apps > Card Authentication**.
- 2 Note the following information:
 - **Status**—Shows the activity status of the printer.
 - **Not Configured**—No printer has been configured.
 - **Offline**—No printer activity or communication is performed.
 - **Online**—The printer is active.
 - **Uptime**—How long the application has been running.
 - **(this printer)**—The current printer.
 - **Last Activity**—The last activity of the master printer.
 - **Number of Users**—The total number of registered users.
 - **Registration Status**—Indicates whether the printer is offline or online.
 - **Last Sync with Master**—The last time that the backup printer updated with the master printer.
 - **Last Contact with Master**—The last time the backup printer communicated with the master printer.
 - **Last Sync as Master**—The last time that the backup printer functioned as the master printer.
 - **Last Activity as Master**—The last activity of the backup printer functioning as master printer.
 - **Duration as Master**—How long the backup printer has functioned as the master printer.
 - **Currently Serviced By**—The client printer recently in contact with the master or backup printer.
 - **Last Activity with Backup**—The last time that the client printer was in contact with the backup printer.

Managing client printers and user accounts

Note: This feature appears only when a printer functions as a master.

- 1 From the Embedded Web Server, click **Apps > Launch Apps > Card Authentication**.
- 2 From the Clients section, do either of the following:

Add client printers

- a Click **Add Clients**.
- b Type the IP address of the client printer, and then click **Add Clients**.

Notes:

- Use commas to separate multiple IP addresses.
- Use an asterisk as the last octet to search for multiple IP addresses. For example, type **10.194.1.***.

Delete client printers

- a From the Clients list, select one or more client printers.
- b Click **Delete Clients**.

Note: You cannot delete client printers if the application is offline or uninstalled.

Deleting user accounts

- 1 From the Embedded Web Server, click **Apps > Launch Apps > Card Authentication**.
- 2 From the Master section, click **Delete Users**.
- 3 Type the user ID.

Note: Use commas to separate multiple user IDs.

- 4 Click **Delete**.

Reassigning printer roles

Configuring a new master printer

- 1 From the Embedded Web Server of the new master printer, navigate to the configuration page for the application:

Apps > Card Authentication > Configure

- 2 Click **User Authentication**, and then from the Printer-based Settings section, set the role to **Master**.
- 3 Type the host name or IP address of the backup printer.
- 4 Click **Save**.

Assigning the backup printer to the new master printer

- 1 From the Embedded Web Server of the backup printer, navigate to the configuration page for the application:

Apps > Card Authentication > Configure

- 2 Click **User Authentication**, and then from the Printer-based Settings section, set the role to **Backup**.
- 3 Type the host name or IP address of the new master printer.
- 4 Click **Save**.

Reassigning a client printer

- 1 From the Embedded Web Server of the current master printer, click **Apps > Launch Apps > Card Authentication**.
- 2 From the Clients section, delete the client printer.
- 3 Do either of the following:

Add the client printer using the configuration page for the application

- a From the Embedded Web Server of the client printer, navigate to the configuration page for the application:
Apps > Card Authentication > Configure
- b Click **User Authentication**, and then from the Printer-based Settings section, set the role to **Client**.
- c Type the host names or IP addresses of the new master printer and new backup printer.
- d Click **Save**.

Add the client printer using the master printer status page

- a From the Embedded Web Server of the new master printer, click **Apps > Launch Apps > Card Authentication**.
- b From the Clients section, click **Add Clients**.
- c Type the IP address of the client printer.
- d Click **Add Clients**.

Using the application

Registering users

- 1 Tap your card on the card reader.
- 2 On the printer control panel, enter your credentials.


Note: If you are using Kerberos or Active Directory or LDAP+GSSAPI for card registration, then select a realm.

- 3 Touch **Register**.

Note: After registration, you are automatically logged in. If you tap your card within the specified time in the logout delay, then you remain logged in. To log out, press the home button, or touch the user name in the upper-right corner of the printer control panel, and then confirm logout. For more information, see [“Configuring the badge logout delay” on page 15](#).

Registering a PIN

- 1 From the printer control panel, touch **PIN Login**.

- 2 Touch  > **Register PIN**.

Note: To change an existing PIN, touch **Change PIN**.

- 3 Follow the instructions on the display.

Logging in to the printer manually

- 1 From the printer control panel, touch one of the following:

- **PIN Login**
- **Manual Login**
- **Admin Login**

Note: If you select **Admin Login**, then retrieving other user information from the LDAP server is not applicable.

- 2 Enter your login credentials.

Note: If you are using Kerberos, Active Directory, or LDAP+GSSAPI for manual login, then select a realm.

- 3 Follow the instructions on the display.

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

Authentication error

Try one or more of the following:

Increase the printer timeout

If you are using Identity Service as a card validation method, then the printer may need more time to communicate to the Identity Service Provider.

- 1** From the Embedded Web Server, click **Settings > Device**.
- 2** Do the following:

Adjust the screen timeout

- a** Click **Preferences**.
- b** Increase the value of Screen Timeout.
- c** Click **Save**.

Adjust the Sleep Mode timeout

- a** Click **Power Management**.
- b** Increase the value of Sleep Mode.
- c** Click **Save**.

Make sure that the printer is connected to the network

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

Make sure that the security server is online and is not busy

For more information, contact your system administrator.

User is locked out

Update the lockout time and the allowed number of login failures

The user may have reached the allowed number of login failures.

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

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

Note: Wait for the lockout time to pass before the new settings take effect.

Cannot register a client printer

Try one or more of the following:

Make sure that the master printer or the backup printer is online

For more information, see [“Accessing the status page for the application” on page 16](#).

Make sure that the master printer and the backup printer are configured properly

For more information, see [“Configuring printer-based card validation” on page 8](#).

Contact your solution provider

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

Cannot connect to the LDAP server

Try one or more of the following:

Make sure that the LDAP settings are configured properly

For more information, see [“Configuring LDAP card validation” on page 10](#).

Contact your solution provider

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

Some settings do not appear in the configuration page

Try one or more of the following:

Make sure to use the recommended web browser

For more information, see the *Readme* file.

When using Internet Explorer, make sure not to show intranet sites in Compatibility View

For more information, see the help information for the browser.

Contact your Lexmark representative

User has no access privileges

Try one or more of the following:

Enable the permissions of the login method assigned to card registration and manual login

- 1 From the Embedded Web Server, click **Settings > Security > Login Methods**.
- 2 Click **Manage Groups/Permissions** beside the login method assigned to card registration and manual login.
- 3 Enable the permissions that are identical to the Card Authentication permissions.
- 4 Click **Save**.

Contact your Lexmark representative

Cannot find realm information

The Use Selected Realm option is enabled in the application, but the login method assigned for manual login or card registration does not require realm selection. For example, local accounts or LDAP. The login methods that require realm selection are Kerberos, Active Directory, and LDAP+GSSAPI.

Try one or more of the following:

Disable realm selection

- 1 From the Embedded Web Server, navigate to the configuration page for the application:
Apps > Card Authentication > Configure
- 2 From the Advanced Settings section, clear **Use Selected Realm**.
- 3 Click **Save**.

Change the login method

- 1** From the Embedded Web Server, navigate to the configuration page for the application:
Apps > Card Authentication > Configure
- 2** From the User Authentication section, change the login method for card registration and manual login to Kerberos or Active Directory or LDAP+GSSAPI.
- 3** Click **Save**.

Contact your Lexmark representative

Frequently asked questions

Why can't I add or delete a client printer when a backup printer functions as a master printer?

You can delete or add a client printer only when the master printer is online.

Can I remove a client printer even if the master printer is offline and reassign it to its new master printer?

Yes. Do the following:

- 1 Reinstall the application from the client printer.
- 2 Set the role as a client printer and configure it to its new master and backup printers. For more information, see [“Configuring printer-based card validation” on page 8](#).

Why can't I see a Copy or Fax button on the lock screen even if I enabled copy or fax without logging in?

The copy or fax button does not appear if access control to the Copy or Fax function is not set. For more information, see [“Configuring the login screen” on page 13](#).

How do I restrict public access to the configuration page for all applications?

- 1 From the Embedded Web Server, click **Settings** > **Security** > **Login Methods**.
- 2 From the Public section, click **Manage Permissions**.
- 3 Expand **Device Management**, and then clear **Apps Configuration**.
- 4 Click **Save**.
- 5 From the Embedded Web Server, click **Settings** > **Security** > **Login Methods**.
- 6 Click **Manage Permissions** or **Manage Groups/Permissions** beside the login method that you want to configure.
- 7 Click the group that you want to have access to the configuration page for all applications.
- 8 Expand **Device Management**, and then make sure that **Apps Configuration** is selected.
- 9 Click **Save**.

Notices

Edition notice

December 2020

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, go to <http://support.lexmark.com>.

For information on Lexmark's privacy policy governing the use of this product, go to www.lexmark.com/privacy.

For information on supplies and downloads, go to www.lexmark.com.

© 2016 Lexmark International, Inc.

All rights reserved.

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.

All other trademarks are the property of their respective owners.

Index

A

- access controls 14
- accessing
 - status page 16
- accessing the Embedded Web Server 8
- adding
 - client printers 16
 - users 19
- adding local accounts 12
- administrator authentication
 - configuring 13
- application error 20
- applications
 - securing 14
- assigning a login method 12
- assigning a login method for manual login 12
- authentication
 - configuring 8
- authentication error 20

B

- badge logout delay
 - configuring 15

C

- cannot connect to the LDAP server 21
- cannot find realm information 22
- cannot register a client printer 21
- card authentication
 - default login method 8
- change history 4
- changing a PIN 19
- checklist
 - deployment readiness 6
- client printers
 - adding 16
 - deleting 16
 - migrating 17
- configuration file
 - importing or exporting 15
- configuring
 - badge logout delay 15
 - Identity Service card validation 10

- LDAP card validation 10
- login screen 13
- new backup printer 17
- new master printer 17
- PIN authentication 11
- printer-based card validation 8
- web service card validation 9
- configuring administrator authentication 13
- configuring realms
 - login methods 13
- copy function
 - using without logging in 13

D

- default login method 8
- deleting
 - client printers 16
 - user accounts 16
- deployment readiness checklist 6

E

- Embedded Web Server
 - accessing 8
- exporting a configuration file 15

F

- FAQs 24
- fax function
 - using without logging in 13
- frequently asked questions 24
- functions
 - securing 14

I

- Identity Service card validation
 - configuring 10
- importing a configuration file 15

L

- LDAP card validation
 - configuring 10
- local accounts
 - adding 12
- logging in to the printer manually 19

- login
 - manual 19
 - PIN 19
- login screen
 - configuring 13

M

- manual login 19
 - assigning a login method 12
- migrating
 - client printers 17
 - user accounts 17

O

- overview 5

P

- PIN
 - registering 19
- PIN authentication
 - configuring 11
- PIN login 19
- printer roles
 - reassigning 17
- printer-based card validation
 - configuring 8

R

- reassigning printer roles 17
- registering a PIN 19
- registering users 19

S

- securing
 - applications 14
 - printer functions 14
- showing realms for user accounts 13
- some settings do not appear in the configuration page 22
- status page
 - accessing 16

T

- troubleshooting
 - application error 20

- authentication error 20
- cannot connect to the LDAP server 21
- cannot find realm information 22
- cannot register a client printer 21
- some settings do not appear in the configuration page 22
- user has no access privileges 22
- user is locked out 21

U

- user accounts
 - deleting 16
 - migrating 17
- user has no access privileges 22
- user is locked out 21
- users
 - adding 19
 - registering 19
- using copy function without logging in 13
- using fax function without logging in 13

W

- web service card validation
 - configuring 9