Cloud Authentication

Administrator's Guide

December 2023

www.lexmark.com

Contents

Change history

December 2023

- Added information on supporting the coexistence of Cloud Authentication and other third-party authentication application.

September 2021

- Removed support for manual login.

April 2021

- Added information on the Admin Login feature.

December 2019

- Added information on warning the user when there is no card reader attached.
- Added information on resetting the PIN.
- Updated information on configuring authenticated proxy settings.

December 2018

Updated the following information:

- Configuring user authentication settings
- Logging in to the printer manually

Added the following information:

- Configuring the polling interval
- Configuring the printer proxy settings
- Registering a card using an e-mail registration link

June 2018

- Updated information on configuring the client ID and client secret.
- Updated information on importing and exporting configuration files.
- Added information on setting the application as the default login method.

January 2018

- Initial document release.

Overview

Use the application to secure a printer using a card reader. When users badge in, their credentials are authenticated using a cloud-based identity service provider.

The application is configured and deployed from the Lexmark™ Cloud Platform website. The settings can also be configured manually using the application configuration page.

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

Deployment readiness checklist

Before you begin, make sure that:

- ☐ Any of the supported card readers and its driver are installed in the printer:
  - omnikey5427ckdriver-1.2.9.fls or later versions
  - keyboardreader-2.4.8.fls or later versions
  - omnikeydriver-2.4.5.fls or later versions
- ☐ You have the host name or IP address of the following to configure the user authentication settings:
  - Identity service provider
  - Badge service provider
- ☐ If the application is not deployed through Lexmark Cloud Services Fleet Management, then you have the client ID and client secret. For more information, contact your Lexmark representative.
- ☐ The Card Authentication application is not installed. For more information, see the *Card Authentication Administrator's Guide*.

  Notes:

  - When creating a configuration for Cloud Print Management, Translation Assistant, or Cloud Scan Management applications, make sure that you configure the Pluggable Authentication Module setting properly. If the printer is not managed by another authentication application, then enable this setting. This setting allows Cloud Authentication to be used as the main authentication application to manage the printer security.
  - If the printer has another authentication application managing its security, then make sure to disable the Pluggable Authentication Module setting.
  - For more information on how to configure the Pluggable Authentication Module, see the *Lexmark Cloud Services Administrator's Guide*.
  - The Cloud Print Management applications may not work with some authentication applications. For more information on the limitations, see the *Cloud Authentication ReadMe*.
- ☐ Depending on your printer model, you have disabled either of the following:
  - The Screen Saver feature in the Display Customization application. For more information, see the *Display Customization Administrator's Guide*.

    Note: Installing Cloud Authentication disables the Display Customization Screen Saver feature automatically.
  - The Background and Idle Screen application. For more information, see the *Background and Idle Screen Administrator's Guide*.

Configuring the application

You may need administrative rights to configure the application. The application is preconfigured from the Lexmark Cloud Platform website. You can manually configure the settings using the application configuration page.

For information on the Embedded Solutions Framework (eSF) version installed on your printer, see the **help information documentation**.

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.
   - View the IP address in the Network Overview section or in the TCP/IP section of the Network/Ports menu.
2. Open a web browser, and then type the printer IP address.

Setting the application as the default login method

These settings are applicable only for printers with eSF version 5.0 or later. Cloud Authentication must be set as the default login method.

Note: For information on the Embedded Solutions Framework (eSF) version installed on your printer, see the **help information documentation**.

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 **Cloud Authentication**.
4. Click **Save**.

Configuring administrator login

Notes:

- Admin Login Settings allows users to log in using an authorized local account even if printers with Cloud Authentication lock screen are disconnected from the network.
- While creating a configuration in Lexmark Cloud Services Fleet Management, from the Settings section, select the **Cloud Print Management** application. From the Advanced settings section, click **Show Admin Login on Lock screen**.
- For more information on creating a configuration and deploying it to printers, see the *Lexmark Cloud Services Administrator's Guide*.
- To apply the configuration to multiple printers or a fleet, export the configuration from a printer and then apply the same configuration to the fleet.

Using the Embedded Web Server

For eSF version 5.0 or later

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

Apps > **Cloud Authentication** > **Configure**

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

Notes:

- 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. From the Embedded Web Server, click **Settings** > **Security** > **Manage Groups/Permissions**.
- 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 username accounts, and to username and password accounts.

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

5 Click **Save**.

For eSF version 4.0 or earlier

Note: When using the Admin Login feature, make sure that you have configured the security template for internal accounts, PIN, or password. For more information, see “Configuring user authentication settings” on page 9.

1 From the Embedded Web Server, access the configuration page for the application.

2 From the User Authentication section, set Admin Login Access Control to your preferred login method.

Notes:

- Make sure that the selected access control is configured with a security template. For more information, see “Configuring user authentication settings” on page 9.
- To hide the Admin Login option from the printer control panel, select **Disabled**.

3 Click **Apply**.

Accessing the configuration page for the application

1 From the Embedded Web Server, depending on your printer model, do any of the following:

- Click **Apps**.
- Click **Settings** > **Apps** > **Apps Management**.
- Click **Settings** > **Device Solutions** > **Solutions (eSF)**.
- Click **Configuration** > **Embedded Solutions**.

2 Click **Cloud Authentication** > **Configure**.

Configuring user authentication settings

Notes:

- Starting with eSF versions 5.2.x and 2.2.x, the user authentication settings inherit the printer login configuration settings defined for the organization where the printer is enrolled.
- For more information on the Embedded Solutions Framework (eSF) version installed on your printer, see the **help information documentation**.
- For more information on configuring the printer login, see the *Lexmark Cloud Services Administrator's Guide*.
- The printer settings are updated through the identity service provider, client ID, and client secret of the organization. To show the updated settings, after specifying the identity service provider values, save the settings, and then refresh the page.

1. From the Embedded Web Server, access the configuration page for the application.
2. From the Identity Service Settings section, select **Enable Lock Screen** or **Enable Idle Screen**.
3. Type the IP address, host name, or URL of the identity service provider and the badge service provider.
4. Set the application access policy.
   - **Continue**—If the connection to the identity service provider fails, then the user can continue using the printer.
   - **Fail**—If the connection to the identity service provider fails, then the printer display returns to the login screen.
5. To use a secure connection, upload the identity service provider SSL certificate.

   Note: For more information on creating the SSL certificate, see the documentation that came with your web browser.
6. To let users log in to the printer using a separate service account, select **Use Service Account**, and then enter the service account credentials.

   Note: This setting is not applicable when the application is configured for federated access. For more information, see "Configuring the client ID and the client secret" on page 10.
7. Do any of the following:

For eSF version 5.0 or later

a. From the Card Registration Settings section, set Card Registration to **Identity Service**.

   Note: If Card Registration is set to **Disabled**, then the users cannot register their card.

b. Click **Save**.

For eSF versions 3.x and 4.x

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

b. Set Card Registration Access Control to **Identity Service**.

c. Click **Apply**.

d. From the Embedded Web Server, click **Settings** > **Security** > **Security Setup** > **Access Control** > **Device Solutions**.

e Set Session Access Control to the security template configured with Cloud Authentication.

Note: The default security template is Solution 2.

f Click **Apply**.

Configuring the client ID and the client secret

The client ID and client secret are used to validate whether the user and printer are part of the same organization.

The client ID and client secret can be generated from Lexmark Cloud. For more information, see the *Lexmark Cloud Administrator's Guide*.

1 From the Embedded Web Server, access the configuration page for the application.

2 From the Advanced Settings section, type the client ID and client secret.

3 Click **Save**.

Configuring login screen settings

1 From the Embedded Web Server, access the configuration page for the application.

2 Configure the settings.

For eSF version 5.0 or later

a Click **Login Screen Settings**, and then do any of the following:

- Customize the login message.
- Set the custom login text color to black or white.
- Upload a login screen background image.
- Enable copying and faxing without logging in.

  Note: For more information, see "Enabling public access to applications, copy, and fax functions" on page 11.
- Disable the warning when no card reader is attached.
- From the Lock Screen Settings section, do either of the following:
  - Select the login text location.
  - Type the name of the profile to be launched automatically after a successful login.
- From the Custom Profile section, do any of the following:
  - Type the profile name or printer function that users can access from the lock screen.

    Note: Make sure that public access to the application specified is enabled. For more information, see "Enabling public access to applications, copy, and fax functions" on page 11.
  - Customize the name of the icon that is shown on the lock screen.
  - Upload a custom icon image.

b Click **Save**.

For eSF version 4.0 or earlier

a From the Login Screen section, do any of the following:

- Enable background transparency.
- Customize the login message.
- Upload a login screen background image.
- Enable copying and faxing without logging in.

  Note: For more information, see "Enabling public access to applications, copy, and fax functions" on page 11.
- Disable the warning when no card reader is attached.
- In the Custom Profile field, type the application name or printer function that users can access from the lock screen.

  Note: Make sure that public access to the application specified is enabled. For more information, see "Enabling public access to applications, copy, and fax functions" on page 11.
- Customize the name of the icon that is shown on the lock screen.
- Select the login text location.
- Select the icon and icon text location.

Note: For more information on each setting, see the mouse-over help.

b Click **Apply**.

Enabling public access to applications, copy, and fax functions

Note: For more information on the access controls, see the *Embedded Web Server — Security Administrator's Guide* for your printer.

For eSF version 5.0 or later

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. Expand **Apps**, and then select the applications.
5. Click **Save**.

For eSF version 4.0 or earlier

1. From the Embedded Web Server, click **Settings** or **Configuration**.
2. Depending on your printer model, do either of the following:
   - Click **Security** > **Security Setup** > **Access Controls** > **Function Access**.
   - Click **Security** > **Edit Security Setups** > **Access Controls**.
3. Set the application, copy, and fax function to **No Security**.
4. Click **Submit**.

Configuring the badge logout delay

Set how long before the printer registers a succeeding tap as a logout.

1. From the Embedded Web Server, access the configuration page for the application.
2. Do either of the following:

For eSF version 5.0 or later

a. Click **Advanced Settings**, and then adjust the badge logout delay.
b. Click **Save**.

For eSF version 4.0 or earlier

a. From the Home Screen section, enter the badge logout delay value.
b. Click **Apply**.

Configuring the connection timeouts

1. From the Embedded Web Server, access the configuration page for the application.
2. Do either of the following:

For eSF version 5.0 or later

a. From the Identity Service Settings section, adjust the network and socket timeouts.
b. Click **Save**.

For eSF version 4.0 or earlier

a. From the Advanced Settings section, enter the network and socket timeout values.
b. Click **Apply**.

Importing or exporting a configuration file

Importing configuration files overwrites the existing application configurations.

1. From the Embedded Web Server, access the configuration page for the application.
2. Do either of the following:

For eSF version 5.0 or later

a. Click **Import/Export Configuration**.
b. Do either of the following:

Export a configuration file

Click **Export**.

Note: An exported configuration file does not contain the client secret and service account password values.

Import a configuration file

1. Make sure to specify the client ID and client secret. Using a text editor, open the configuration file, and then edit the values for the following settings:
   - **esf.cloudAuth.settings_identityserver_client_id**
   - **esf.cloudAuth.settings_identityserver_client_secret**

   For the service account user name and password, edit the values for the following settings:
   - **esf.cloudAuth.settings_deviceAuth_userId**
   - **esf.cloudAuth.settings_deviceAuth_password**

   Note: Make sure to enclose the values in double quotation marks.
2. Browse to the configuration file, and then click **Import**.

For eSF version 4.0 or earlier

a. Click **Import/Export Configuration**.

b. Do either of the following:

Export a configuration file

Click **Export**.

Note: An exported configuration file does not contain the client secret and service account password values.

Import a configuration file

1. Make sure to specify the client ID and client secret. Using a text editor, open the configuration file, and then edit the values for the following settings:
   - **esf.cloudauth.settings.identityserver.client.id**
   - **esf.cloudauth.settings.identityserver.client.secret**

   For the service account user name and password, edit the values for the following settings:
   - **esf.cloudauth.settings.identityserver.deviceAuth.userId**
   - **esf.cloudauth.settings.identityserver.deviceAuth.password**

   Note: Make sure to enclose the values in double quotation marks.
2. Click **Import**.
3. Browse to the configuration file, and then click **Start**.

Updating the polling interval

If changes are made to the printer login configuration after the application has been deployed, then the new settings take effect after the next polling interval.

By default, the application checks for updates every 15 minutes (900 seconds).

You can update the polling interval using the application configuration file.

1. Export the configuration file.

   Note: For more information, see “Importing or exporting a configuration file” on page 12.
2. Using a text editor, open the configuration file, and then edit the values for the following settings:

Note: The value must be in seconds. For example, for 15 minutes, use **900**.

eSF version 5.0 or later

esf.cloudAuth.pollingInterval

eSF version 4.0 or earlier

esf.cloudauth.pollingInterval

3 Save, and then import the configuration file.

Configuring the printer proxy settings

Using the Embedded Web Server

If the organization is using an IP address for its proxy server for communication, then configure the HTTP/FTP settings.

1 From the Embedded Web Server, do either of the following:

For eSF version 5.0 or later

a Click **Device** > **Network/Ports** > **HTTP/FTP Settings**.

b Type the HTTP proxy server IP address.

For eSF version 4.0 or earlier

a Click **Settings** > **Network/Ports** > **TCP/IP**.

b From the HTTP/FTP Settings section, type the HTTP proxy server IP address.

2 Save the settings.

Configuring an authenticated proxy server

If the proxy server is configured using a host name or requires a user name and password, then do the following:

1 From the Embedded Web Server, do either of the following:

For eSF version 5.0 or later

a Click **Apps** > **App Framework Configuration**.

b In the Framework Configuration section, clear **Use printer's proxy settings**.

c Type the HTTP proxy server host name and the proxy credentials.

For eSF version 4.0 or earlier

a Depending on your printer model, do one of the following:

- Click **Settings** > **Apps** > **Apps Management** > **System** > **Configure**.
- Click **Settings** > **Device Solutions** > **Solutions (eSF)** > **System** > **Configure**.
- Click **Settings** > **Embedded Solutions** > **System** > **Configure**.

b Clear **Use printer's proxy settings**.

c Type the HTTP proxy server host name and proxy credentials.

2 Save the settings.

Using a configuration file

Import a UCF or VCC file containing the following settings:

```
<setting name="settings.useprinterproxy">
<setting name="settings.http.proxyurl">
<setting name="settings.http.proxyport">
<setting name="settings.proxyurl">
<setting name="settings.proxyport">
```

Sample values

```
<?xml version="1.0" encoding="UTF-8"?>
 <esfSettings>
  <app name="systemManagerImpl" settingVersion="6.2.0">
   <global>
     <setting name="settings.useprinterproxy">false</setting>
     <setting name="settings.http.proxyurl">http.proxy1.fmr.com</setting>
     <setting name="settings.http.proxyport">80</setting>
     <setting name="settings.proxyurl">http.proxy.fmr.com</setting>
     <setting name="settings.proxyport">8000</setting>
   </global>
  </app>
 </esfSettings>
```

Using the application

Registering a card

1. Tap your card on the card reader.
2. From the printer control panel, depending on the authentication configuration, do either of the following:
   - Enter the login code.
   - Enter your user credentials.

   Notes:

   - For more information, see "Obtaining the login code" on page 16.
   - You can also e-mail or print the instructions.
3. Touch **Register**.

Notes:

- Depending on the printer login configuration in Lexmark Cloud Services, you may be prompted to enter your PIN before you can proceed with the registration. For more information on configuring the printer login, see the *Lexmark Cloud Services Administrator's Guide*.
- A badge can be set as temporary or permanent.

Using an e-mail registration link

If **Secure Login** is disabled for the organization, then users can only register their badge through an e-mail registration link in the printer control panel.

For more information on configuring the printer login, see the *Lexmark Cloud Services Administrator's Guide*.

1. Depending on your printer model, touch **E-mail** or **Register via E-mail**.
2. Touch **Next**, and then type your e-mail address.

   An e-mail with a URL is sent to your e-mail address.
3. From your e-mail, click the URL.
4. From the Lexmark Cloud Services website, enter your credentials.

Obtaining the login code

A login code is required when your application is configured to authenticate users from a federated setup using SSO.

Using the web portal

1. Do either of the following:
   - Open a web browser, and then type **`cloud.lexmark.com/device`**.
   - From your mobile device, use a QR code reader application to scan the QR code from the printer control panel.

2 Enter your user credentials.

3 Take note of the login code.

Using the Lexmark Mobile Print application

For more information, see the *Lexmark Mobile Print User's Guide* for your mobile device.

1 From the application home screen, tap **Login Code**.

2 Take note of the login code.

Using Lexmark Cloud Services

For more information, see the *Lexmark Cloud Services User's Guide*.

1 From the Lexmark Cloud Services website, click your user name on the upper-right corner of the page, and then click **My Account**.

2 From the Personal Information section, click **Generate Login Code**.

3 Take note of the login code.

Notes:

- The login code refreshes automatically after 15 minutes.
- The login code can be used only once.

Logging in to the printer manually

For more information on configuring the printer login, see the *Lexmark Cloud Services Administrator's Guide*.

1 From the printer control panel, depending on the printer login configuration, do any of the following:

- Touch **Secure Login**, and then enter the login code.

  Notes:

  - For more information, see "Obtaining the login code" on page 16.
  - This button appears only when the organization authentication is configured with federated access.

- Touch **PIN Login**, and then enter your PIN.

  Note: Before logging in, make sure that you have your PIN. For more information, see "Obtaining a PIN" on page 18.

- Touch **Admin Login**, and enter your administrator credentials.

  Notes:

  - This button appears only when Show Admin Login on Lock screen is selected while creating a configuration in Lexmark Cloud Services Fleet Management.
  - For more information on administrator login, see "Configuring administrator login" on page 7.

2 Touch **Log In**.

Logging in to the printer using a card and two-factor authentication

1. Tap your card on the card reader.
2. Enter your PIN.

   Note: Before logging in, make sure that you have your PIN. For more information, see “Obtaining a PIN” on page 18.

Obtaining a PIN

This setting is available only if the PIN generation option in Lexmark Cloud Services is set to **User set**. For more information, see the *Lexmark Cloud Services Administrator’s Guide*.

1. From the Lexmark Cloud Services website, click your user name on the upper-right corner of the page, and then click **My Account**.
2. From the Printer Login section, click **Set PIN**.
3. Enter your PIN.
4. Click **Generate PIN**.

Resetting the PIN

1. From the Lexmark Cloud Services website, click your user name on the upper-right corner of the page, and then click **My Account**.
2. From the Printer Login section, click **Reset PIN**.
3. Enter your new PIN.
4. Click **Generate PIN**.

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:

Make sure that the printer is connected to the network

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

Make sure that the identity service provider is online and is not busy

For more information, contact your system administrator.

Badge registration is denied

Make sure that the identity service provider and the badge service provider are configured correctly

For more information, see “Configuring user authentication settings” on page 9.

Cannot e-mail the login code instructions

Make sure that the SMTP server is configured correctly

The e-mail function of the printer must be set up with the correct SMTP server address. For more information, contact your system administrator.

The Manual Login button appears when the organization authentication is federated

Try one or more of the following:

Make sure that the printer is connected to the network

The printer may have been disconnected from the network or the server is unreachable during installation. For more information, see the printer *User's Guide*.

Touch **Manual Login**. If the server is reachable, then the authentication process is the same as the Secure Login authentication. After logging out, the Secure Login button appears.

Configure the settings in the application configuration page again

Make sure that the client ID and the client secret are configured correctly

For more information, see “Configuring the client ID and the client secret” on page 10.

Cannot log in using the login code

Make sure that the login code has not been used, and is still valid

Notes:

- The login code refreshes automatically after 15 minutes.
- The login code can be used only once.

Cannot register badge using the email registration link

Register your badge only once

Your badge may have a pending badge registration request. You cannot register a badge using the email registration link multiple times.

Note: If the first email is deleted or never received, then you must register again.

No badge registration e-mail is received

Try one or more of the following:

Make sure to type the e-mail address correctly

Make sure that the e-mail address is valid

Contact your Lexmark representative

An application error or cloud server error may have occurred.

Cannot connect to the identity service provider

Increase the connection timeouts

For more information, see “Configuring the connection timeouts” on page 12.

Make sure that the proxy configuration is correct

For more information, see “Configuring the printer proxy settings” on page 14.

The PIN is expired

Reset the PIN

For more information, see “Obtaining a PIN” on page 18.

Contact your organization administrator

Too many failed attempts

Wait for the lockout period to expire

Wait for about five minutes before trying again.

Contact your organization administrator

Notices

Edition notice

December 2023

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**.

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.

Licensing notices

All licensing notices associated with this product can be viewed from the application package or from the Lexmark support site.

Index

U