



Lexmark™

Print Management Serverless Print Release

Installation Guide

November 2016

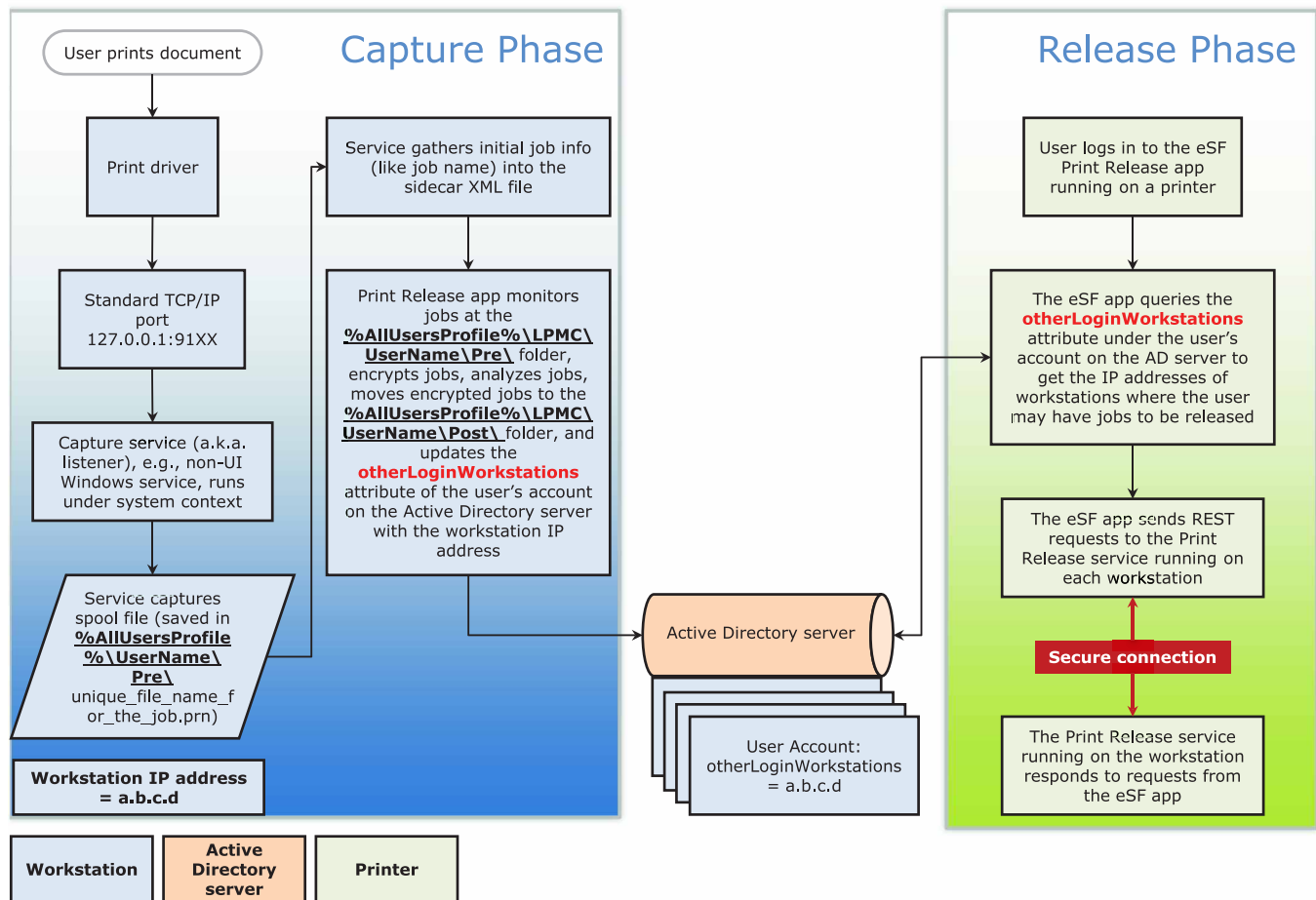
www.lexmark.com

Contents

- Overview..... 3**
 - Lexmark Print Management Client system requirements..... 4
- Setting up prerequisites.....5**
 - Setting up Active Directory..... 5
 - Installing client software for Windows operating system.....6
 - Installing client software for Mac operating system.....12
 - Configuring printer security settings..... 18
- Configuring the applications..... 21**
 - Accessing the configuration page for the application..... 21
 - Configuring LPM Serverless Print Release..... 21
 - Configuring Smart Card Authentication Client..... 21
 - Configuring Card Authentication..... 22
- Troubleshooting.....25**
 - Application error..... 25
 - License error.....26
 - Lexmark Print Management Print Release troubleshooting..... 26
 - Smart Card Authentication Client troubleshooting..... 30
 - Card Authentication troubleshooting.....31
- Appendix.....32**
- Notices..... 33**
- Index.....34**

Overview

Lexmark™ Print Management (LPM) Serverless Print Release is an enterprise-grade printing solution that uses a serverless Print Release infrastructure for managing print jobs. Using Lexmark Print Management Client (LPMC), users can send documents securely to the printer without routing through a print server. Print jobs are stored until they are released from a Print Release–enabled printer.



The solution works with the following Embedded Solutions Framework (eSF) applications:

- **LPM Serverless Print Release**
- **Smart Card Authentication bundle**
 - Smart Card Authentication
 - Smart Card Authentication Client
 - eSF Security Manager
- **Card Authentication**

Lexmark Print Management Client system requirements

Hardware

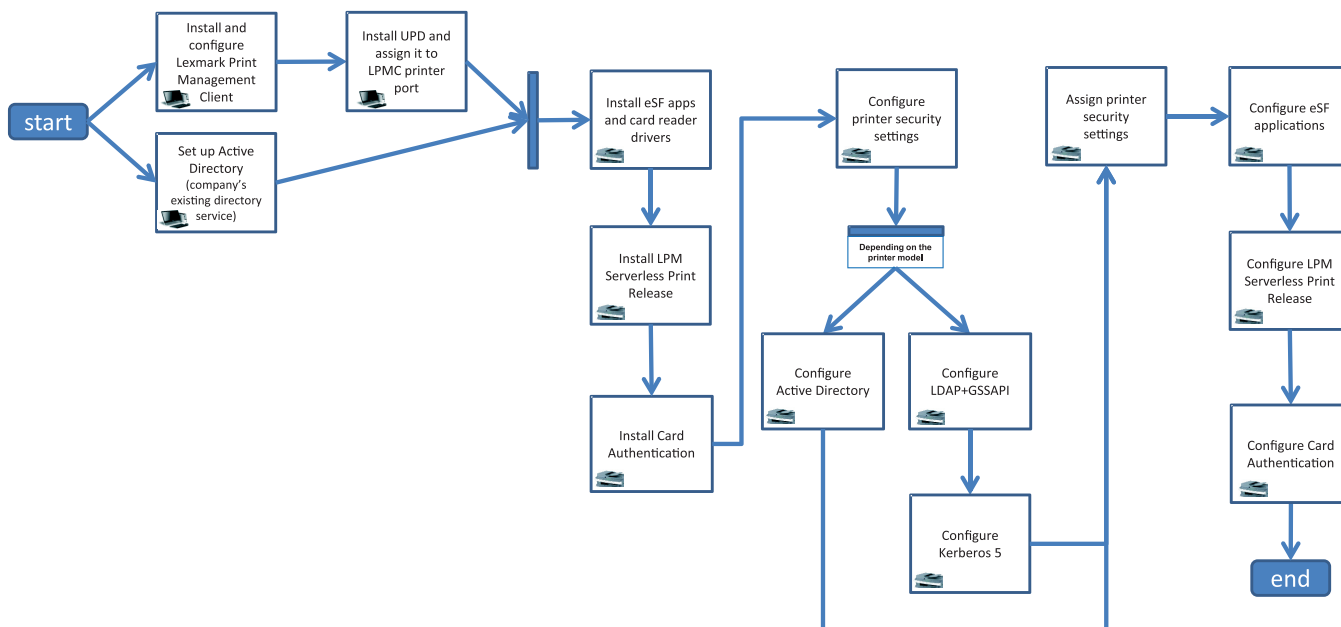
Category	Minimum requirement	Recommended for enterprise systems
Operating system	Windows Vista® or later Note: An x86-based system refers to a 32-bit operating system, while an x64-based system refers to a 64-bit operating system. Mac OS X 10.11, 10.10, and 10.9	Windows Vista or later Note: An x86-based system refers to a 32-bit operating system, while an x64-based system refers to a 64-bit operating system. Mac OS X 10.11, 10.10, and 10.9
Processor	1GHz 32-bit or 64-bit processor	Dual 2.5GHz quad-core processor, such as Intel Xeon or AMD Opteron
RAM	1GB 32-bit 2GB 64-bit	4GB
Hard disk drive	20GB	20GB
Network speed	100Mbps	Gigabit Ethernet
Network name resolution	DNS or WINS Notes: <ul style="list-style-type: none"> Local hosts files can be used instead of external DNS. For support of other network systems, contact your system administrator. 	

Software

- Microsoft® .NET Framework 4.0 (full version) or later
- Lexmark Universal Print Driver (UPD) version 2.7 or later
- Lexmark Mac UPD 1.0.50

Setting up prerequisites

Installation workflow diagram



Setting up Active Directory

Active Directory® is a directory service that manages user data, security, clients, and print jobs. LPMC uses Active Directory to track all workstations where a specific user may have print jobs ready to be released.

Each user has a set of attributes or properties that is kept on the Active Directory server. This information is accessible in the domain controller servers.

Note: The setup of Active Directory and its data replication configuration may delay the availability of jobs for release on the printer. To minimize this delay, reduce the replication interval.

Granting Active Directory permission to access specific user attributes

- 1 From the Active Directory server, open the Delegation of Control Wizard.
- 2 Add a group of users who want to access the attribute, and then click **OK > Next**.
- 3 Create a custom task to delegate, and then select **User objects** from the list.
- 4 Select **Property-specific**, **Read otherLoginWorkstations**, and **Write otherLoginWorkstations**.
- 5 Follow the instructions on the computer screen.

Creating user attributes for an Active Directory schema

By design, Active Directory lets you keep some domain user information. Some may be in use by the system, such as user name, description, and time of last login.

Administrators must review the attributes that are not in use in the current network configuration.

1 Open the registry key, and then edit it to enable attribute manipulation.

Note: If the registry key does not exist, then create it manually.

2 Install the Active Directory schema snap-in.

3 Add the schema to the console.

a At the command prompt, type **mmc**.

b Select **Active Directory Schema** from the list of snap-ins, and then add it.

4 Open the Active Directory Schema manager snap-in.

5 Right-click **Attributes**, and then click **Create Attribute**.

Note: If the setting is unavailable, then restart the server.

6 Confirm the changes.

7 From the Create New Attribute dialog box, enter the required information.

8 Add the new attribute to the appropriate schema class.

a Expand **Classes**.

b Right-click **user**, and then click **Properties**.

c From the Attributes tab, click **Add**.

d From the list, select the new attribute.

e Apply the changes.

Installing client software for Windows operating system

Before you begin, make sure that:

- Microsoft .NET Framework 4.0 (full version) or later is installed.
- The recommended print driver is installed.
- Active Directory is running.
- The computer where you installed LPMC is enrolled to an Active Directory domain.
- The administrator is logged in to an Active Directory domain and is granted administrative rights to access the domain.

Installing Lexmark Print Management Client

Lexmark Print Management Client (LPMC) is a software package deployed in client systems in a domain to provide secure releasing of print jobs. LPMC captures the print jobs from the print spooler and, if necessary, encrypts them. Print jobs are stored in the computer until they are released from a Print Release–enabled printer.

- 1 Obtain an installation package for LPMC, and then save it to a temporary local drive.
- 2 Copy the configuration file to the folder where you saved the installation package, and then if necessary, modify it. For more information, see [“Understanding configuration files for Windows operating system” on page 8](#).
- 3 Install the package by doing either of the following:
 - From the folder where you saved the package, double-click the MSI package.
 - At the command prompt, type `msiexec /i lpmc.msi`.
- 4 Follow the instructions on the computer screen.
- 5 After the installation is complete, do the following:

Check if LPMC is installed

- a Navigate to the programs and features folder of your operating system.
- b Look for **Lexmark Print Management Client**.

Check if the necessary services are installed and running

- a At the command prompt, type `services.msc`.
- b Check if the following services are running:
 - Lexmark Print Capture Service
 - Lexmark Print Release Service

- 6 Assign the recommended print driver to the LPMC printer port. For more information, see [“Installing the print driver and creating a print queue” on page 12](#) or contact your system administrator.

Notes:

- Executable files are saved in the Program Files folder.
- The configuration file, log file, and temporary deleted jobs tracking report are saved in the “%allusersprofile%\LPMC” folder.
- LPMC printer port 9167 and IP address 127.0.0.1 are created by default. Administrators can change the port number before installation.

Working with SSL Certificates

LPMC acts as a secure server that accepts and establishes connections over the HTTPS protocol. LPMC allows data encryption that connects to the regular network. To be able to accept an SSL connection, LPMC secures a certificate to confirm the identity of the server and serve as the basis for encryption.

Each certificate specifies the subject that a certificate identifies. For example, the workstation where LPMC is running may be defined as “workstation-name,” such as **John-PCXP**, or by a more generic name, such as **localhost**. The reserved name, **localhost**, is an alias for 127.0.0.1 network address.

When a certificate is created, it is added to the workstation and becomes available for all users who log in to the machine. LPMC also binds a certificate to the appropriate network connection and uses the port that is defined in the configuration file.

If the configured port is changed after the installation, then LPMC cannot establish an SSL connection. To reconnect over an SSL, reinstall LPMC, or manually rebind the certificate to the new port number.

Note: The creation and binding of the certificate occur during the LPMC installation process.

Understanding configuration files for Windows operating system

Logger

Setting	Default value	Description
LogFilePath	c:\ProgramData\LPMC\lpmc.log	The path where log files are saved.
LoggingEnabled	true	If set to false , then LPMC stops logging the file.

CaptureSettings

Setting	Default value	Description
LoopbackPort	9167	The port that the capture service communicates for incoming print jobs. If you want to use another port, then change the port that the print queue uses.
PrintJobFileNameFormat	%d_%i.prn	The file name format that the capture service uses to save the print jobs. %d is the time when a job is printed, and %i is the current tick count. You can use the following values as part of the file name: %u —The user name %pd —The print driver name %pq —The print queue name

ClientSettings

Setting	Default value	Description
PrintAndKeepLifespan	48	The number of hours before LPMC deletes the job after printing
UnprintedJobsLifespan	48	The number of hours before LPMC deletes a job that is not released on a print queue

ReleaseSettings

Setting	Default value	Description
EsfListenerPort	9443	The port where a job is released from the printer

ADServerSettings

Setting	Default value	Description
ActiveDirectoryUserProperty	otherLoginWorkstations	The Active Directory attribute that LPMC uses to save and retrieve data.
ServiceAccountUserName	N/A	The user name designated as the service account. The administrator sets this setting before the deployment.

ADWriteSettings

Setting	Default value	Description
ADWriteOption	AtPrintTime	<p>Determines when LPMC writes the workstation IP address to the Active Directory server.</p> <p>Use any of the following values:</p> <ul style="list-style-type: none"> • AtStartup—The workstation IP address is written only when LPMC starts. It is deleted when the workstation shuts down or enters a low-power state. • AtPrintTime—The workstation IP address is written only when a job is printed. It is deleted when the user has no more jobs held at the workstation, the workstation shuts down, or the workstation enters a low-power state. If a stored job is detected when LPMC starts, then the workstation IP address is written immediately. • AtStartupAndPrintTime—The workstation IP address is written when LPMC starts and when a job is printed. It is not deleted when the user has no more jobs held at the workstation. It is deleted when the workstation shuts down or enters a low-power state.

ServerSettings

Setting	Default value	Description
ServerIP	api.iss.lexmark.com/lpm-gateway	The release and tracking server address.
ServerPort	443	The port where a job is released from the printer.

ServerAPISettings

Setting	Default value	Description
APIVersion	2.0	The version of the application programming interface (API) used.
IDPServerSettings	idp.iss.lexmark.com	The Identity Service Provider address used to authenticate users.
ServerIP	443	
ServerPort		The port where a job is released from the printer.

DeleteJobTrackerSettings

Setting	Default value	Description
TrackDeletedJob	true	If set to false , then the deleted jobs are not tracked.
SendImmediately	true	If set to false , then LPMC sends the deleted jobs data using IntervalMode.
IntervalMode	Daily	Send the deleted jobs data after a specified interval of time. You can set the interval in minutes, hours, days, or weeks. If IntervalMode is enabled, then the deleted jobs data are temporarily saved in c:\ProgramData\LPMC\DJTReport.xml. When the set interval has elapsed, the deleted jobs data are sent to the report server, and the DJTReport.xml file is deleted.
SendInterval Minutes Hourly Daily Weekly Day Hour	1200	Specify when to send the deleted jobs data to the report server.
ServerSettings ServerIP ServerPort ServerSSL	10.194.107.109 9780 false	Contains the information about the report server where the deleted jobs data are stored.
OtherSettings	N/A	More information about the deleted jobs data.

LateBindingSettings

Setting	Default value	Description
LateBindingEnabled	false	If set to true , then the Color, Sides (Duplex), Staple, Hole Punch, and number of copies settings can be modified in the printer control panel.

DeleteEmptyUserFolders

Setting	Default value	Description
DeleteEmptyUserFolders	false	If set to true , then the User folders with no print jobs and valid User Tokens are automatically deleted.

Sample configuration file for Windows operating system

```
<?xml version="1.0" encoding="utf-8"?>
<Configuration xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema">
  <Logger>
    <LogFilePath>C:\ProgramData\LPMC\lpmc.log</LogFilePath>
    <LoggingEnabled>true</LoggingEnabled>
  </Logger>
  <CaptureSettings>
    <LoopbackPort>9167</LoopbackPort>
    <PrintJobFileNameFormat>%d_%i.prn</PrintJobFileNameFormat>
  </CaptureSettings>
</Configuration>
```

```

<ClientSettings>
  <PrintAndKeepLifespan>48</PrintAndKeepLifespan>
  <UnprintedJobsLifespan>48</UnprintedJobsLifespan>
</ClientSettings>
<ReleaseSettings>
  <EsfListenerPort>9443</EsfListenerPort>
  <ServiceAccountUsername></ServiceAccountUsername>
</ReleaseSettings>
  <ADServerSettings>
    <ActiveDirectoryUserProperty>otherLoginWorkstations</ActiveDirectoryUserProperty>
    <ServiceAccountUsername></ServiceAccountUsername>
  </ADServerSettings>
  <ADWriteSettings>
    <ADWriteOption>AtPrintTime</ADWriteOption>
  </ADWriteSettings>
<ServerSettings>
  <ServerIP>api.iss.lexmark.com/lpm-gateway</ServerIP>
  <ServerPort>443</ServerPort>
</ServerSettings>
<ServerAPISettings>
  <APIVersion>2.0</APIVersion>
  <IDPServerSettings>
    <ServerIP>idp.iss.lexmark.com</ServerIP>
    <ServerPort>443</ServerPort>
  </IDPServerSettings>
</ServerAPISettings>
<DeleteJobTrackerSettings>
  <TrackDeletedJob>true</TrackDeletedJob>
  <SendImmediately>true</SendImmediately>
  <IntervalMode>Minutes</IntervalMode>
  <SendInterval>
    <Minutes>5</Minutes>
    <Hourly>>false</Hourly>
    <Daily>1200</Daily>
    <Daily>2300</Daily>
    <Weekly>
      <Day>2</Day>
      <Day>3</Day>
      <Day>4</Day>
      <Day>5</Day>
      <Day>6</Day>
      <Hour>1000</Hour>
      <Hour>1500</Hour>
    </Weekly>
  </SendInterval>
  <ServerSettings>
    <ServerIP>10.194.107.109</ServerIP>
    <ServerPort>9780</ServerPort>
    <ServerSSL>>false</ServerSSL>
  </ServerSettings>
  <OtherSettings>
    <SiteName></SiteName>
    <Custom1></Custom1>
    <Custom2></Custom2>
    <Custom3></Custom3>
  </OtherSettings>
</DeleteJobTrackerSettings>
  <LateBindingSettings>
    <LateBindingEnabled>>false</LateBindingEnabled>
  </LateBindingSettings>

```

```
<DeleteEmptyUserFolders>>false</DeleteEmptyUserFolders>  
</Configuration>
```

Installing the print driver and creating a print queue

Make sure to download any of the following print drivers for your operating system:

- Universal PostScript 3 Emulation Print Driver
- Universal PCL XL Emulation Print Driver
- Universal PCL5e Emulation Print Driver

Note: The print drivers can be downloaded at www.lexmark.com.

- 1 Run the installer file from your computer.
 - a Select **Extract**, and then clear **Start the installation software**.
 - b Copy the path to the UPD files.

Note: If you want to change the path, then browse to the folder where you want to save the UPD files.
 - c Click **Install**, and then follow the instructions on the computer screen.
- 2 Open the printers folder, and then click **Add a printer**.
- 3 From the Add Printer Wizard dialog box, select **Use an existing port**, select the LPMC printer port from the list, and then click **Next**.
- 4 When prompted to install the software, select **Have Disk**.
- 5 In the “Copy manufacturer’s files from” field, paste the location of the UPD files, or browse to the INF file for the driver.
- 6 Click **OK > Next**.
- 7 From the list, select the print driver, and then click **Next**.
- 8 Type a descriptive name for the print queue, select whether to use the new print queue as the default, and then share the printer.
- 9 Click **Finish**.

Installing client software for Mac operating system

Joining an Active Directory domain

Adding the Active Directory domain to the DNS servers list

- 1 From the computer, navigate to System Preferences, and then click **Network**.
- 2 Select the network, and then click **Advanced**.
- 3 Click **DNS**, and then from the DNS Servers section, click +, and then type the IP address of the Active Directory domain.
- 4 From the Search Domains section, click +, and then type the Active Directory domain name.

- 5 Click **OK**.
- 6 From the Network window, click **Apply**.

Joining the Active Directory domain

- 1 From the computer, navigate to System Preferences, and then click **Users & Groups**.
Note: If the settings are unavailable, then click the lock button. An administrator account is needed to unlock the settings.
- 2 Click **Login Options**, and then from the Network Account Server section, click **Join**.
- 3 Configure the settings.
 - **Server**—The Active Directory domain controller address
 - **Client Computer ID**—The name of the client computer
 - **AD Admin User**—The account name associated with the Active Directory domain
 - **AD Admin Password**—The password of the account associated with the Active Directory domain
- 4 Click **OK**.
- 5 Log out from the computer, and then log in again using the user ID and password associated with the Active Directory domain.

Installing the print driver

Note: We recommend installing Lexmark Mac UPD before installing LPMC.

- 1 Run the installer file from your computer.
- 2 Select **Extract**, and then clear **Start the installation software**.
- 3 Copy the path to the UPD files.
Note: If you want to change the path, then browse to the folder where you want to save the UPD files.
- 4 Click **Install**, and then follow the instructions on the computer screen.

Installing Lexmark Print Management Client

For Mac, LPMC is distributed as a single PKG file.

- 1 Copy the configuration file to the folder where you saved the installation package, and then if necessary, modify it. For more information, see [“Understanding configuration files for Mac operating system” on page 14](#).
- 2 Install the package. Do either of the following:
 - Double-click the PKG file.
 - At the Terminal, run **install.sh**.
- 3 Follow the instructions on the computer screen.
- 4 After the installation is complete, from Activity Monitor, check if the necessary services are running.
 - **LPMCapture**—The Lexmark Print Capture service
 - **LPMRelease**—The Lexmark Print Release service

- **LPMDeleteJobTracker**—The LPM Deleted Job Tracker service
- **LPMApp**—The LPM user-level background application

Note: After installation, the executable files, the configuration.xml file, and SSL certificates are saved in the “/Library/Lexmark/LPMC” folder. The log file is saved in “/var/tmp” as lpmc.log by default.

Understanding configuration files for Mac operating system

Logger

Setting	Default value	Description
LogFilePath	/var/tmp/lpmc.log	The path where the log files are saved.
LoggingEnabled	false	If set to true , then the LPMC events are logged. If set to debug , then more information is logged.

CaptureSettings

Setting	Default value	Description
LoopbackPort	9167	The port that the capture service communicates for incoming print jobs. If you want to use another port, then change the port that the print queue uses.
PrintJobFileNameFormat	%d_%i.prn	The file name format that the capture service uses to save the print jobs. %d is the time when a job is printed, and %i is the current tick count. You can use the following values as part of the file name: %u —The user name %pd —The print driver name %pq —The print queue name

ClientSettings

Setting	Default value	Description
PrintAndKeepLifespan	48	The number of hours before LPMC deletes the job after printing
UnprintedJobsLifespan	48	The number of hours before LPMC deletes a job that is not released on a print queue

ReleaseSettings

Setting	Default value	Description
EsfListenerPort	9443	The port where a job is released from the printer.
UseSSL	true	Determines whether the communication with Print Release uses SSL or not. If ServerPort is set to 80 , then set the value to false to establish a non-SSL connection.

ServerSettings

Setting	Default value	Description
ActiveDirectoryUserProperty	otherLoginWorkstations	The Active Directory attribute that LPMC uses to save and retrieve data. If otherLoginWorkstations is not available, then use customAttributeName to use a custom user attribute.
ServiceAccountUserName	N/A	The user name designated as the service account. The administrator sets this setting before the deployment.

ADWriteSettings

Setting	Default value	Description
ADWriteOption	AtPrintTime	<p>Determines when LPMC writes the workstation IP address to the Active Directory server.</p> <p>Use any of the following values:</p> <ul style="list-style-type: none"> • AtStartup—The workstation IP address is written only when LPMC starts. It is deleted when the workstation shuts down or enters a low-power state. • AtPrintTime—The workstation IP address is written only when a job is printed. It is deleted when the user has no more jobs held at the workstation, the workstation shuts down, or the workstation enters a low-power state. If a stored job is detected when LPMC starts, then the workstation IP address is written immediately. • AtStartupAndPrintTime—The workstation IP address is written when LPMC starts and when a job is printed. It is not deleted when the user has no more jobs held at the workstation. It is deleted when the workstation shuts down or enters a low-power state.

ServerSettings

Setting	Default value	Description
ServerIP	api.iss.lexmark.com/lpm-gateway	The release and tracking server address.
ServerPort	443	The port where a job is released from the printer.

Setting	Default value	Description
UseSSL	true	Determines whether the communication with Print Release uses SSL or not.

ServerAPISettings

Setting	Default value	Description
APIVersion	2.0	The version of the application programming interface (API) used.
IDPServerSettings ServerIP ServerPort	idp.iss.lexmark.com 443	The Identity Service Provider address used to authenticate users. The port where a job is released from the printer.
UseSSL	true	Determines whether the communication with Print Release uses SSL or not.

DeleteJobTrackerSettings

Setting	Default value	Description
TrackDeletedJob	true	If set to false , then the deleted jobs are not tracked.
SendImmediately	true	If set to false , then LPMC sends the deleted jobs data using IntervalMode.
IntervalMode	minutes	Send the deleted jobs data after a specified interval of time. You can set the interval in minutes, hours, days, or weeks.
SendInterval Minutes Daily Weekly Day Hour	1200	Specify when to send the deleted jobs data to the report server. Minutes —Set any value equal to or greater than 1. Daily —Set the value in hours with the HHMM format. The interval runs every day based on the set hour. You can set multiple instances of the Daily setting. This setting triggers the deleted jobs tracker to run multiple times during the day. Weekly —Consists of Day and Hour values. Day —Set any value from 1 to 7, where 1 is Sunday, and 7 is Saturday. Hour —Set the value in HHMM format, where the interval runs based on the indicated hour of the day. Day and Hour settings can have multiple instances.

Setting	Default value	Description
ServerSettings ServerIP ServerPort ServerSSL	0.0.0.0 9743 true	Contains the information about the report server where the deleted jobs data are stored.
OtherSettings SiteName	N/A	More information about the deleted jobs data. SiteName —The name of the site where the job was submitted from.

Sample configuration file for Mac operating system

```

<?xml version="1.0" encoding="utf-8"?>
<Configuration xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema">
  <Logger>
    <LogFilePath>var/tmp/lpmc.log</LogFilePath>
    <LoggingEnabled>>false</LoggingEnabled>
  </Logger>
  <LPMServerlessADSettings>
    <CaptureSettings>
      <LoopbackPort>9167</LoopbackPort>
      <PrintJobFileNameFormat>%d_%i.prn</PrintJobFileNameFormat>
    </CaptureSettings>
    <ClientSettings>
      <PrintAndKeepLifespan>48</PrintAndKeepLifespan>
      <UnprintedJobsLifespan>48</UnprintedJobsLifespan>
    </ClientSettings>
    <ReleaseSettings>
      <EsflistenerPort>9443</EsflistenerPort>
      <UseSSL>>true</UseSSL>
    </ReleaseSettings>
    <ADServerSettings>
      <ActiveDirectoryUserProperty>otherLoginWorkstations</ActiveDirectoryUserProperty>
      <ServiceAccountUsername></ServiceAccountUsername>
    </ADServerSettings>
    <ADWriteSettings>
      <ADWriteOption>AtPrintTime</ADWriteOption>
    </ADWriteSettings>
  </LPMServerlessADSettings>
  <ServerSettings>
    <ServerIP>api.iss.lexmark.com/lpm-gateway</ServerIP>
    <ServerPort>443</ServerPort>
    <UseSSL>>true</UseSSL>
  </ServerSettings>
  <ServerAPISettings>
    <APIVersion>2.0</APIVersion>
    <IDPServerSettings>
      <ServerIP>idp.iss.lexmark.com</ServerIP>
      <ServerPort>443</ServerPort>
      <UseSSL>>true</UseSSL>
    </IDPServerSettings>
  </ServerAPISettings>
  <DeleteJobTrackerSettings>
    <TrackDeletedJob>>true</TrackDeletedJob>
    <SendImmediately>>true</SendImmediately>
    <IntervalMode>minutes</IntervalMode>
    <SendInterval>
  
```

```

    <Minutes>5</Minutes>
    <Hourly>>false</Hourly>
    <Daily>1200</Daily>
    <Daily>2300</Daily>
    <Weekly>
      <Day>2</Day>
      <Day>3</Day>
      <Day>4</Day>
      <Day>5</Day>
      <Day>6</Day>
      <Hour>1000</Hour>
      <Hour>1500</Hour>
    </Weekly>
  </SendInterval>
  <ServerSettings>
    <ServerIP>0.0.0.0</ServerIP>
    <ServerPort>9780</ServerPort>
    <ServerSSL>>false</ServerSSL>
  </ServerSettings>
  <OtherSettings>
    <SiteName></SiteName>
  </OtherSettings>
</DeleteJobTrackerSettings>
</Configuration>

```

Creating a print queue

- 1 From the computer, navigate to System Preferences, and then click **Printers and Scanners**.
- 2 Click **+**, and then from the Add window, click **IP**.
- 3 In the Address field, type **127.0.0.1:9167**.
- 4 In the Protocol menu, select **HP Jetdirect - Socket**.
- 5 In the Name field, type the name of the print queue.
- 6 In the Use menu, select **Lexmark Generic Laser Printer Mono** or **Lexmark Generic Laser Printer Color**.
- 7 Click **Add**.

Configuring printer security settings

Before you begin, make sure to install the following:

- LPM Serverless Print Release
- Card Authentication
- Smart Card Authentication bundle

Configuring Active Directory

Notes:

- This feature is available only in some printer models.
- Use HTTPS to protect the credentials that are used to connect the printer to the domain.

- Make sure to select **Enable NTP**. From the Embedded Web Server, click **Settings** or **Configuration**, and then click **Security > Set Date and Time > Enable NTP**.
- 1 Open a Web browser, and then type the printer IP address.
Note: View the IP address in the TCP/IP section of the Network/Ports menu.
 - 2 Click **Settings** or **Configuration**, and then click **Security > Security Setup > Active Directory > Join an Active Directory Domain**.
 - 3 Type the domain name or the realm name that you want to use.
 - 4 If necessary, type the domain controllers, separated by commas.
 - 5 Type the credentials of the user who has the rights to add computers to a network.
Note: Passwords are case-sensitive, but these are not cached by the device.
 - 6 Apply the changes.

Configuring LDAP+GSSAPI

Notes:

- This feature requires you to configure Kerberos 5 settings.
 - For authentication that relies on an external server, users cannot access protected printer functions if an outage prevents the printer from authenticating to the server.
 - To help prevent unauthorized access, log out from the printer after each session.
 - Make sure to select **Enable NTP**. From the Embedded Web Server, click **Settings** or **Configuration**, and then click **Security > Set Date and Time > Enable NTP**.
- 1 Open a Web browser, and then type the printer IP address.
Note: View the IP address in the TCP/IP section of the Network/Ports menu.
 - 2 Click **Settings** or **Configuration**.
 - 3 Create an LDAP+GSSAPI configuration.
Note: You can store a maximum of five configurations.
 - a Click **Security > Security Setup > LDAP+GSSAPI > Add an LDAP+GSSAPI Setup**.
 - b Specify the required configuration settings.
 - c Apply the changes.
 - 4 Click **Security Template > Add a Security Template**.
 - 5 Type an LDAP security template name, and then select the custom building block name that you created for LDAP+GSSAPI.
 - 6 Save the template.

Configuring Kerberos 5 for use with LDAP+GSSAPI

Note: This feature is available only in some printer models.

Kerberos 5 is used in conjunction with the LDAP+GSSAPI building block. While only one Kerberos configuration file (krb5.conf) can be stored on a supported device, the file can apply to multiple realms and Kerberos Domain Controllers (KDCs).

Notes:

- Because only one krb5.conf file is used, uploading or resubmitting a simple Kerberos file overwrites the configuration file.
- The krb5.conf file can specify a default realm. But if a realm is unspecified in the configuration file, then the first realm specified in the Embedded Web Server is used as the default realm.
- Make sure that krb5.conf status is verified. If not, click **Test Setup**.
- For authentication that relies on an external server, users cannot access protected printer functions if an outage prevents the printer from authenticating to the server.
- To help prevent unauthorized access, log out from the printer after each session.

1 Open a Web browser, and then type the printer IP address.

Note: View the IP address in the TCP/IP section of the Network/Ports menu.

2 Click **Settings** or **Configuration**.

3 Create a Kerberos configuration file.

a Click **Security** > **Security Setup** > **Kerberos 5**.

b Specify the required configuration settings.

c Apply the changes.

4 Import the new configuration file.

a Click **Security** > **Security Setup** > **Kerberos 5**.

b From the Import Kerberos File section, browse to the folder where the configuration file is stored.

c Apply the changes.

Assigning security templates

1 Open a Web browser, and then type the printer IP address.

Note: View the IP address in the TCP/IP section of the Network/Ports menu.

2 Click **Settings** or **Configuration**, and then click **Security** > **Security Setup** > **Access Controls**.

3 Click **Device Apps** or **Device Solutions**.

4 Set the following functions to the appropriate security template:

- App 1 or Solution 1 for Active Directory or LDAP+GSSASPI
- App 2 or Solution 2 for Card Authentication
- App 3 or Solution 3 for Smart Card Authentication Client

5 Apply the changes.

Configuring the applications

Accessing the configuration page for the application

1 Open a Web browser, and then type the printer IP address.

Note: View the IP address in the TCP/IP section of the Network/Ports menu.

2 Click **Settings** or **Configuration**.

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

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

4 Select the application from the list, and then click **Configure**.

Configuring LPM Serverless Print Release

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

2 Specify the text and image that you want to appear on the home screen.

3 Specify how long before the application disconnects from the network.

4 Enable basic and detailed logging.

5 Specify what type of connection to use.

- **Auto**—Allow the application to retrieve the jobs from LPMC configured to an SSL connection (port 9443) or to a non-SSL connection (port 80).
- **SSL Only**—Allow the application to retrieve the jobs from SSL-configured LPMC.

6 Specify whether to print an error log when a print release error occurs.

- **Do Not Print Errors**
- **Printing Errors Only**
- **Deletion Errors Only**
- **Printing and Deletion Errors**

7 Apply the changes.

Configuring Smart Card Authentication Client

For more information, see the *Smart Card Authentication Client Administrator's Guide*.

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

2 Configure the login screen.

- a Select what login type to use.
- b Set User Validation Mode to **Active Directory**.

- 4 Configure user authentication.
 - a Specify the card authentication or validation method to use.
 - b Set the card registration access control to **App 1** or **Solution 1**.
 - c Set the manual login access control.
 - For Active Directory, or LDAP+GSAPPI, set it to **App 1** or **Solution 1**.
 - For Smart Card Authentication Client, set it to **App 3** or **Solution 3**. Also set Card Validation to **None**.
 - d Set the session access control to **App 2** or **Solution 2**.

Note: For more information, see [“Assigning security templates” on page 20](#).
- 5 From the Serverless Print Release Service section, set Server Location Lookup to **Active Directory**.
- 6 Do one of the following:
 - If you selected a printer-based authentication, then set up the role for the printer. For more information, see [“Setting up the role for the printer” on page 23](#).
 - If you selected an LDAP authentication, then see [“Configuring LDAP card validation” on page 24](#).
 - If you selected a Web-Service authentication, then see [“Configuring Web service card validation” on page 24](#).
- 7 Apply the changes.

Setting up the role for the printer

Notes:

- Before you begin, make sure to set up the master printer first, then the backup printer, and then the client printers.
- If a master printer has a registered client printer, then a backup printer is required.
- A client printer requires a master printer and a backup printer.
- A license is required. For more information, contact your Lexmark representative.

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

2 In the User Authentication section, set Card Validation to **Printer-based**.

3 In the Printer-based Card Validation section, select a role for the printer.

- **Master**—Maintains a list of registered users.
- **Backup**—Stores a copy of registered users from the master printer. If the master printer is offline, then the backup printer functions as the master printer.
- **Client**—Lets users badge in, although authentication occurs at the master printer. This printer does not store user information.

Notes:

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

4 Type the host names or IP addresses of the master printer and the 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 the client printer from the old one.

5 Apply the changes.

Configuring LDAP card validation

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

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

3 From the LDAP Server Setup section, do the following:

a Clear **Use Address Book**.

b Type the LDAP server address and the port number.

c Clear **Use SSL**, and then type the search base from which the LDAP search begins.

d Type the login information.

4 Fill in the appropriate LDAP attributes.

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

5 Apply the changes.

Configuring Web service card validation

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

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

3 In the Web Service Validation section, type the LDD server address.

4 Set the time for the application to wait for a response from the LDD server.

5 Set the values for registration and lookup interfaces.

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

6 Apply the changes.

Troubleshooting

Application error

Try one or more of the following:

Check the system log

- 1 Open a Web browser, and then type the printer IP address.
Note: View the IP address in the TCP/IP section of the Network/Ports menu.
- 2 Click **Settings** or **Configuration**.
- 3 Depending on your printer model, do one of the following:
 - Click **Apps > Apps Management**.
 - Click **Device Solutions > Solutions (eSF)**.
 - Click **Embedded Solutions**.
- 4 Click **System > Log**.
- 5 Select and submit the appropriate filters to view the log entries.
- 6 Analyze the log, and then resolve the problem.

Check the LPMC log

You can enable the logging of LPMC events by modifying the Logger element in the LPMC configuration file.

For Windows operating system

```
<Logger>  
  <LogFilePath>C:\ProgramData\LPMC\lpmc.log</LogFilePath>  
  <LoggingEnabled>>true</LoggingEnabled>  
</Logger>
```

Note: For more information, see [“Understanding configuration files for Windows operating system” on page 8](#).

For Mac operating system

```
<Logger>  
  <LogFilePath>/var/tmp/lpmc.log</LogFilePath>  
  <LoggingEnabled>>true</LoggingEnabled>  
</Logger>
```

Note: For more information, see [“Understanding configuration files for Mac operating system” on page 14](#).

- To enable logging, set the LoggingEnabled value to **true**, or **debug** for a more detailed log.
- To view the log file, navigate to the folder specified in LogFilePath. Analyze the log, and then resolve the problem.

Note: Setting the LoggingEnabled value to **false** disables logging, but some critical errors are still logged.

Contact your Lexmark representative

License error

Try one or more of the following:

Make sure that the application is licensed

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

Make sure that the license is up-to-date

- 1 Open a Web browser, and then type the printer IP address.
Note: View the printer IP address in the TCP/IP section of the Network/Ports menu.
- 2 Click **Settings** or **Configuration**.
- 3 Depending on your printer model, do one of the following:
 - Click **Apps > Apps Management**.
 - Click **Device Solutions > Solutions (eSF)**.
 - Click **Embedded Solutions**.
- 4 Click the license status of the application from the list.
- 5 Update the license.

Lexmark Print Management Print Release troubleshooting

Jobs do not appear in the Print Release queue

Try one or more of the following:

Make sure to send the print job to the print queue

Make sure that the user account used when sending the print job is the same account logged in to the Print Release–enabled printer

For more information, contact your system administrator.

Make sure that LPM Serverless Print Release is installed on the printer to which you are sending the print job

For more information, contact your system administrator.

Make sure that the computer and the printer are connected to the same network

For more information, contact your system administrator.

Make sure that the user is granted read and write access to the Active Directory attribute

For more information, contact your system administrator.

Add a firewall exception to the LPMC port

A firewall may be blocking the communication between the printer and the workstation. The blocking happens when you have a non-Windows firewall for workstations using Windows operating system, or a non-Mac firewall for workstations using Mac operating system. The default port for LPMC is 9443. For more information, contact your system administrator.

Make sure that the user is granted access to the computer where LPMC is installed

Note: The following instructions are applicable only to Windows operating system users.

- 1 From the computer where LPMC is installed, run the command prompt as an administrator, and then type **secpol.msc**.
- 2 From the Security Settings menu, click **Local Policies > User Rights Assignment > Access this computer from the network**.
- 3 Set the security policy to its default value, or manually add a user or group to the policy.
Note: If the domain group policy is managing the security policy, then add them at the domain group policy level. Otherwise, your changes are overwritten the next time the group policy is modified.
- 4 Click **Apply**.

Cannot connect to the Print Release server

Try one or more of the following:

Make sure to set Serverless Print Release Service to the appropriate server location lookup from the Card Authentication configuration page

For more information, see [“Configuring user login and authentication” on page 22](#).

Make sure that your account from the Active Directory has write access to the otherLoginWorkstations attribute

For more information, see [“Setting up Active Directory” on page 5](#), or contact your system administrator.

Remove the proxy settings used for your printer

For more information, contact your system administrator.

Make sure that LPMC and the printer are connected to the same network

For more information, contact your system administrator.

Make sure that LPMC is not in Sleep or Hibernate mode

For more information, contact your system administrator.

Make sure that the user sending the print job from the printer is the same user logged in to LPMC

For more information, contact your system administrator.

Make sure that the LPMC services are running when you access Print Release on the printer

- Lexmark Print Capture Service
- Lexmark Print Release Application
- Lexmark Print Release Service

When using the Card login method, make sure to use the user account with administrator privilege in Active Directory and LPMC

For more information, contact your system administrator.

Make sure that NTP is enabled

- 1 Open a Web browser, and then type the printer IP address.
Note: View the IP address in the TCP/IP section of the Network/Ports menu.
- 2 Click **Settings** or **Configuration**, and then click **Security** > **Set Date and Time**.
- 3 Select **Enable NTP**.
- 4 Apply the changes.

Make sure that the password created for Certificate Authority is correct

For more information, contact the system administrator.

Make sure that the service account user name set for Card Authentication matches the user name in the LPMC configuration file

For more information, see [“Configuring Card Authentication” on page 22](#).

For more information on configuring LPMC, see [“Installing Lexmark Print Management Client” on page 7](#).

Make sure that the user is granted access to the computer where LPMC is installed

- 1 From the computer where LPMC is installed, run the command prompt as an administrator, and then type **secpol.msc**.
- 2 From the Security Settings menu, click **Local Policies** > **User Rights Assignment** > **Access this computer from the network**.
- 3 Set the security policy to its default value, or manually add a user or group to the policy.
Note: If the policy is managed by domain group policy settings, then add them at the domain group policy level. Otherwise, your changes will be overwritten the next time the group policy is modified.
- 4 Apply the changes.

Cannot determine the user ID

Make sure that you have assigned the appropriate security template for LDAP+GSSAPI, Smart Card Authentication Client, and Card Authentication

For more information, see [“Configuring printer security settings” on page 18](#).

Cannot connect to the LDAP server

Try one or more of the following:

When using Card Authentication, make sure to configure it to the correct settings

- Clear **Use Address Book**.
- Enter the correct information in the LDAP settings.
- From the Serverless Print Release Service, set Server Location Lookup to **Active Directory**.

Note: For more information, see [“Configuring Card Authentication” on page 22](#).

Make sure that the printer is not configured to a different Active Directory server

Make sure that you have configured Kerberos 5 server to use LDAP+GSSAPI authentication

For more information, see [“Configuring Kerberos 5 for use with LDAP+GSSAPI” on page 19](#).

Loading the print jobs takes a long time

Try one or more of the following:

Make sure that the workstations containing the print jobs are turned on

The application may be trying to connect to the workstations that are turned off. The application waits for three timeouts before they stop communicating to a workstation.

Contact your Lexmark representative

Jobs do not finish printing

Try one or more of the following:

Make sure that your printer is connected to the network

Release the print job again

Cannot connect to LPMC when using Mac workstations

Try one or more of the following:

Make sure that the computer is connected to the network whether a user is logged in or not

Some Mac computers cannot connect to the network after being turned on and before any user is logged in. A network connection is needed to connect to LPMC.

Contact your Lexmark representative

Cannot print large files when the Color, Sides (Duplex), Staple, Hole Punch, or multiple copies settings are enabled

Try one or more of the following:

Disable or increase the socket timeout value

- 1 From the Embedded Web Server, access the configuration page for the application.
- 2 In the Socket Timeout field, increase the value, or enter **0** to disable the timeout.
- 3 Apply the changes.

Contact your Lexmark representative

Smart Card Authentication Client troubleshooting

Card has been locked out from future login attempts

Try one or more of the following:

Restart the printer

Replace the card

An error occurs when using a smart card reader

Try one or more of the following:

Make sure that a supported smart card reader is attached

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

Make sure that the required firmware version is installed

For a list of required firmware versions, see the *Readme* file.

Install Smart Card Authentication Client, eSF Security Manager, and the authentication token for your smart card before attaching a supported card reader

For more information, see the *Smart Card Authentication Client Administrator's Guide*.

Card Authentication troubleshooting

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, access the status page for the application.

Make sure that the master printer and the backup printer are properly set up

For more information, see the chapter on setting up the prerequisites in the *Card Authentication Administrator's Guide*.

Delete printers from the list to be able to add a client printer

You may have exceeded the allowable number of client printers in the list. For more information, see the topic on managing client printers in the *Card Authentication Administrator's Guide*.

Contact your solutions provider

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

Cannot authenticate using a badge

Try one or more of the following:

Set Login Method to Card or Manual Login

For more information, see [“Configuring user login and authentication” on page 22](#).

Contact your solutions provider

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

Appendix

Licensing applications

Applications require an electronic license to run on some printers.

For more information, contact your Lexmark representative.

Exporting or importing a configuration file

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

2 Export or import the configuration file.

Notes:

- If a **JVM Out of Memory** error occurs, then repeat the export process until the configuration file is saved.
- If a timeout occurs and a blank screen appears, then refresh the Web browser, and then click **Apply**.

Checking the version of the Embedded Solutions Framework

1 From the Embedded Web Server, click **Reports > Device Settings**.

2 In the Embedded Solutions section, note the value associated with “Framework =.”

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

Notices

Edition notice

November 2016

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.

© 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.

Mac and OS X are trademarks of Apple Inc.

Microsoft, Windows, Windows Vista, 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

A

- accessing the configuration page 21
- Active Directory
 - configuring 18
 - creating attribute 5
 - granting permissions 5
 - setting up 5
- Active Directory domain joining 12
- Active Directory schema
 - creating 5
- application error 25
- applications
 - licensing 32
- assigning security templates 20

B

- backup printer
 - setting up 23

C

- cannot authenticate a badge 31
- cannot connect to LPMC when using Mac workstations 30
- cannot connect to the LDAP server 29
- cannot connect to the Print Release server 27
- cannot determine the user ID 29
- cannot print large files when the Color, Sides (Duplex), Staple, Hole Punch, or multiple copies settings are enabled 30
- cannot register a client printer 31
- Card Authentication
 - configuring 22
- card has been locked out from future login attempts 30
- client printers
 - setting up 23
- configuration file 7
 - exporting or importing 32
- configuration files
 - understanding 14

- configuration page for the application
 - accessing 21
- configuring
 - Active Directory 18
 - Card Authentication 22
 - Kerberos 5 19
 - LDAP card validation 24
 - LDAP server 24
 - LDAP+GSSAPI authentication 19
 - LDD server 24
 - Lexmark Print Management Serverless Print Release 21
 - Smart Card Authentication Client 21
 - Web service card validation 24
- configuring Lexmark Print Management Client 7, 13
- connection to Print Release server failed 27
- creating a print queue 12, 18
- creating Active Directory schema 5

E

- Embedded Solutions Framework
 - checking version number 32
- error occurs when using a smart card reader 30
- exporting a configuration file 32

I

- importing a configuration file 32
- installing
 - print driver 12
- installing Lexmark Print Management Client 7, 13
- installing the print driver 13

J

- jobs do not appear in the Print Release queue 26
- jobs do not finish printing 29
- joining an Active Directory domain 12

K

- Kerberos 5
 - configuring 19

L

- LDAP card validation
 - configuring 24
- LDAP+GSSAPI authentication
 - configuring 19
- Lexmark Print Management Client
 - configuring 7, 13
 - installing 7, 13
- Lexmark Print Management Serverless Print Release
 - configuring 21
- license error 26
- licensing applications 32
- loading the print jobs takes a long time 29

M

- master printer
 - setting up 23
- minimum system requirements 4

O

- overview 3

P

- print driver
 - installing 12, 13
- print queue
 - creating 12, 18
- printers
 - setting up 23

R

- recommended system requirements 4

S

- security templates
 - assigning for Card Authentication 20

- assigning for internal accounts 20
- assigning for Smart Card Authentication Client 20
- setting up
 - printers 23
- setting up Active Directory 5
- Smart Card Authentication Client
 - configuring 21
- system requirements 4

T

- troubleshooting
 - application error 25
 - cannot authenticate a badge 31
 - cannot connect to LPMC when using Mac workstations 30
 - cannot connect to the LDAP server 29
 - cannot connect to the Print Release server 27
 - cannot determine the user ID 29
 - cannot print large files when the Color, Sides (Duplex), Staple, Hole Punch, or multiple copies settings are enabled 30
 - cannot register a client printer 31
 - card has been locked out from future login attempts 30
 - error occurs when using a smart card reader 30
 - jobs do not appear in the Print Release queue 26
 - jobs do not finish printing 29
 - license error 26
 - loading the print jobs takes a long time 29

U

- understanding configuration files 14

W

- Web service card validation
 - configuring 24