Print Management On-Premises

Version 2.14.2

Administrator's Guide

December 2024

www.lexmark.com

Contents

Overview

Use the Lexmark™ Print Management (LPM) On-Premises solution to send print jobs from anywhere to one central print queue. You can securely release jobs on any Lexmark printer in the system.

The solution supports the following features:

- Authenticate users when using the standard functions of the printer, such as copying, faxing, e-mailing, and scanning to FTP site or to a network.
- Let another user (called a delegate) print your jobs.
- Authenticate using your badge, card, PIN, or user name and password.
- Set user quotas and track usage.
- Send print jobs using the AirPrint software feature.

By using the Lexmark Document Distributor (LDD) platform, you can securely send your files to the server from the following, where they are held until printed:

- Computer
- Mobile device
- E-mail
- AirPrint
- Other systems that can submit print jobs to a Windows-based print queue

Depending on your configuration, jobs that are not printed after a specified period are deleted automatically.

The solution can also be used to do the following:

- Track jobs from a printer that is connected to the workstation using the USB port.
- Let workstations print jobs that are stored locally, and then release them at any printer using the LPM Serverless Print Release solution add-on. For more information, see "Configuring Serverless client registration" on page 203.

For information on how to print using this solution, see the *Lexmark Print Management On-Premises User's Guide*.

This document provides instructions on how to configure and troubleshoot the solution.

System components

- **Lexmark Document Distributor**—Enables document capture, processing, and routing.
- **Lexmark Print Management**—Lets you send jobs from anywhere to a central print queue, and then securely release them from any Lexmark printer in the system.
- **Database**—Maintains information about clients, solutions, settings, and jobs. The database can be Microsoft SQL Server or Firebird®.
- **User Directory**—Stores information on users and groups. The user directory can be any LDAP-compliant directory or the LPM database.
- **Embedded Solutions Framework (eSF) applications**—Provides the Print Release user interface buttons and prompts, authentication management, and activity tracking for copy, fax, e-mail, and scan functions.

System requirements

Recommended hardware

- The processor is at least dual 2.5GHz quad-core Intel Xeon or AMD Opteron.
- The available random access memory is at least 8GB.
- The available hard disk space on the server is at least 40GB.

Recommended software

- The operating system is Windows Server 2012 or later.
- The Windows Server operating system is 64-bit.
- The antivirus provides full control access privileges to the LDD installation path.
- The document conversion software is Microsoft Office, OpenOffice, or LibreOffice. The document conversion software is required only if installing Lexmark Print. For more information on document conversion, see "Document conversion software dependencies" on page 27.

Recommended hardware for Print Release

- The available space for the **ALLUSERSPROFILE** environment variable target path is at least 1GB for backup files.

  Note: The default path is **C:\ProgramData**.
- The server hard disk must be high speed with low latency.

ALLUSERSPROFILE

ALLUSERSPROFILE is an environment variable in Windows that indicates the folder to store application data that is shared by all users. Typically, this variable is mapped to **C:\ProgramData**.

To know the exact value, perform the following steps:

At the command prompt, type the following:

```
>echo %ALLUSERSPROFILE%
```

LDD server requirements

For a list of all LDD-related server and network requirements, see the *Lexmark Document Distributor Administrator's Guide*.

The following table shows the LPM versions that are compatible with specific LDD versions:

Lexmark Print Management version	Lexmark Document Distributor version
2.14.2	5.8.2
2.14.1	5.8.1
2.14	5.8
2.13.1	5.7.1
2.13	5.7
2.12	5.6
2.11	5.5
2.10	5.4

Lexmark Print Management version	Lexmark Document Distributor version
2.9	5.3
2.8	5.2
2.7	5.1
2.6	4.9
2.5.1.2 or later	
2.5.1.1 or earlier	4.8.5
2.4	

Supported Embedded Solutions Framework (eSF) applications

Note: For more information on e-Task printers, see "Supported printer models" on page 24.

Solution	eSF application	Description	Compatible eSF framework
LDD	advancedprompt	Provides basic prompts for the user at the printer display	• e-Task 5+ • e-Task 5 • e-Task 4 • e-Task 3
[1] For more information on the eSF application versions, see *Release Notes*.			

Solution	eSF application	Description	Compatible eSF framework
	badgeauth	Locks the printer until a user authenticates with a badge, PIN, or a username and password **Notes:** • This application is necessary only when securing the printer home screen. • After upgrading to LPM version 2.5.2 or later, manually configure each badgeauth application to deploy to the target printer family.	• e-Task 4 • e-Task 3
	cardAuth	Locks the printer until a user authenticates with a badge, PIN, or a username and password **Note:** This application is necessary only when securing the printer home screen.	• e-Task 5+ • e-Task 5
	deviceusage	Provides all usage data on the printer **Notes:** • This application is necessary only when tracking printer usage. • After upgrading to LPM version 2.5.2 or later, manually configure each Device Usage application to deploy to the target printer family.	• e-Task 5+ • e-Task 5 • e-Task 4 • e-Task 3
	omnikey5427ckdriver	The driver for the Omnikey card reader **Note:** This application is necessary only when using an Omnikey card reader that is configured in CCID (default) mode.	• e-Task 5+ • e-Task 5 • e-Task 4

[1] For more information on the eSF application versions, see *Release Notes*.

Solution	eSF application	Description	Compatible eSF framework
Print Release	omnikeydriver	The driver for the Omnikey card reader **Note:** This application is necessary only when using Omnikey 5321, 5125, or 5325 card readers that are configured in CCID (default) mode.	• e-Task 3
	guestlaunch	Provides authentication for the Guest Print feature **Notes:** • This application is necessary only when using the Guest Print feature. • Please refer to the Unsupported devices for Guest Print section.	• e-Task 5+ • e-Task 5 • e-Task 4 • e-Task 3
	printCryption2	Decrypts the encrypted print jobs when using Secure Print **Note:** This application is necessary only when using the Secure Print feature.	• e-Task 5+ • e-Task 5 • e-Task 4 • e-Task 3
[1] For more information on the eSF application versions, see *Release Notes*.			

Optional configurations

Configuring Print Release with rf IDEAS Ethernet 241 adapter

Note: For information on configuring rf IDEAS, see "Configuring Print Release with rf IDEAS" on page 139.

Before you begin, make sure that LPM version 2.3.11 or later is working correctly.

- At least one rf IDEAS Ethernet 241 adapter (serial, or serial and USB) with firmware version 1.1 or later

  Note: rf IDEAS Discovery Tool requires firmware version 2.02 or later.
- Network-ready printers that support the necessary document types

Configuring DNS servers

Configure DNS servers for AirPrint advertisement, service discovery for LPM, or to reply to Unicast DNS queries from an AirPrint-capable device.

Note: For information on configuring DNS servers, see "Configuring DNS servers" on page 124.

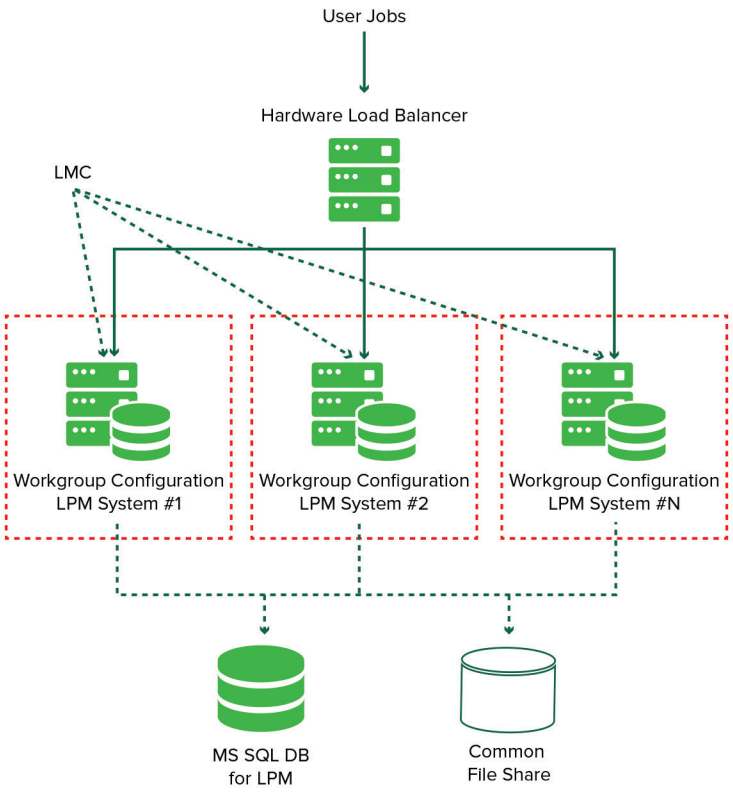
- Microsoft Windows Server (2012 with the latest service packs)
- An Apple device capable of the AirPrint software feature (running the iOS 6.2 or later or OS X 10.7 or later operating systems)
- BIND for Windows, if using BIND

  Note: You can download the BIND installation package at the Internet Systems Consortium website. For more information, go to **https://www.isc.org**.

Understanding the Lexmark Print Management system

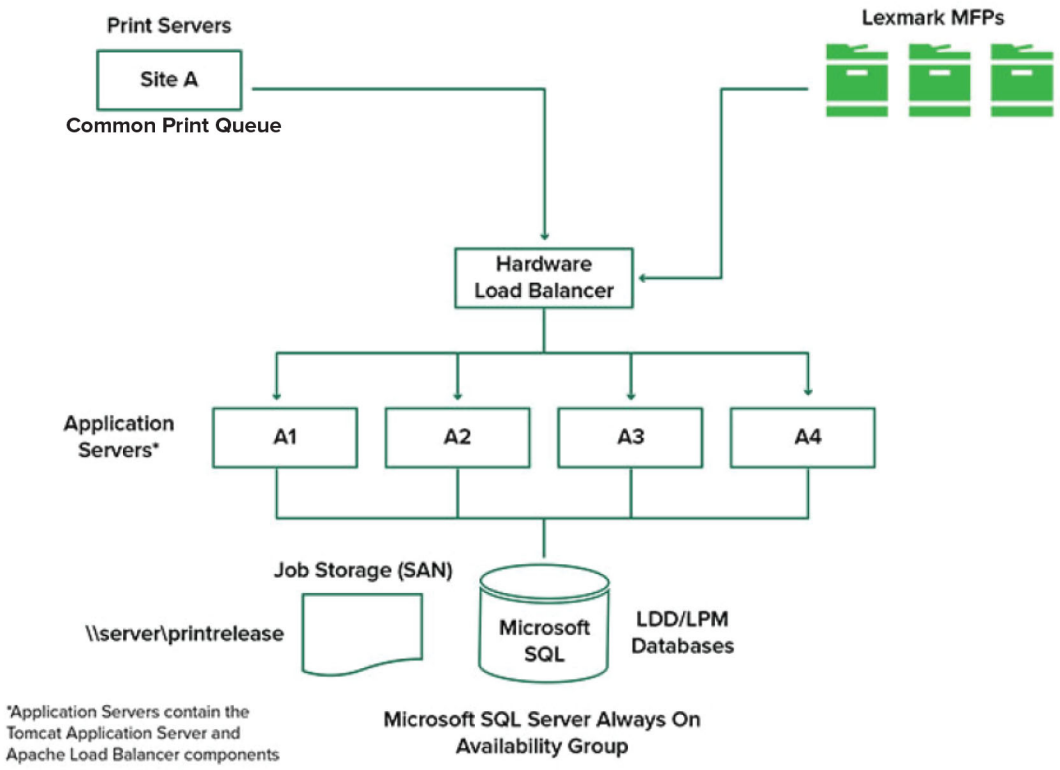
Understanding the solution architecture

The following shows a shared Microsoft SQL Server environment with a hardware load balancer and workgroup servers:

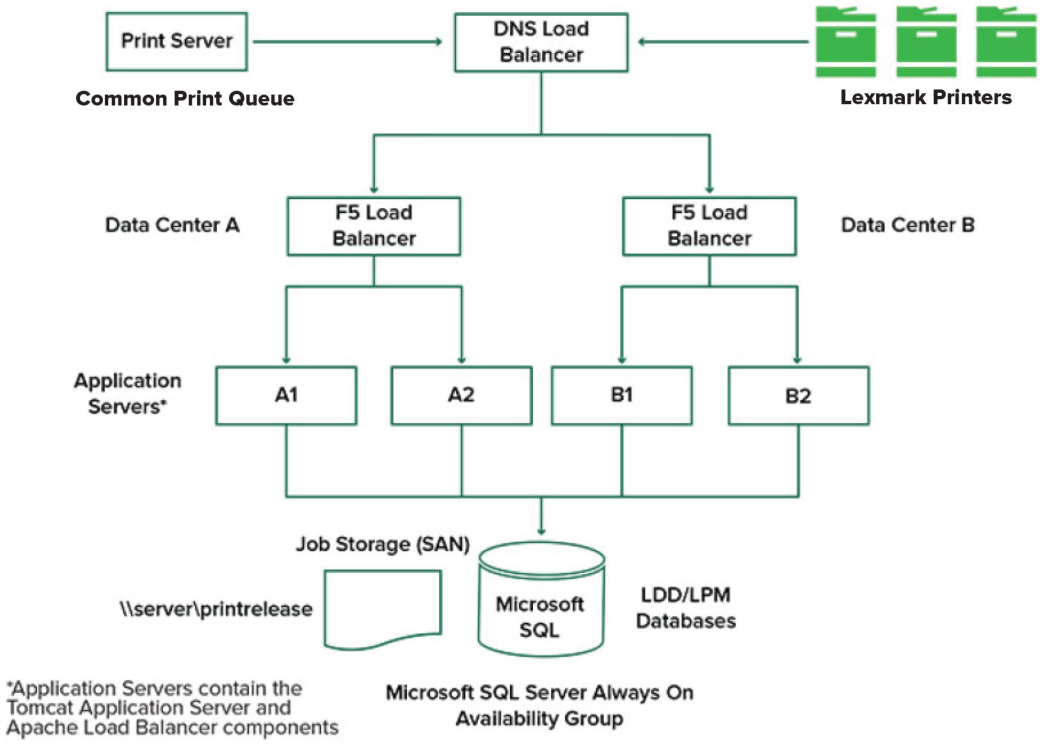


Note: We recommend using a configuration where the Print Delete script and the Reports Aggregator service run on only one workgroup.

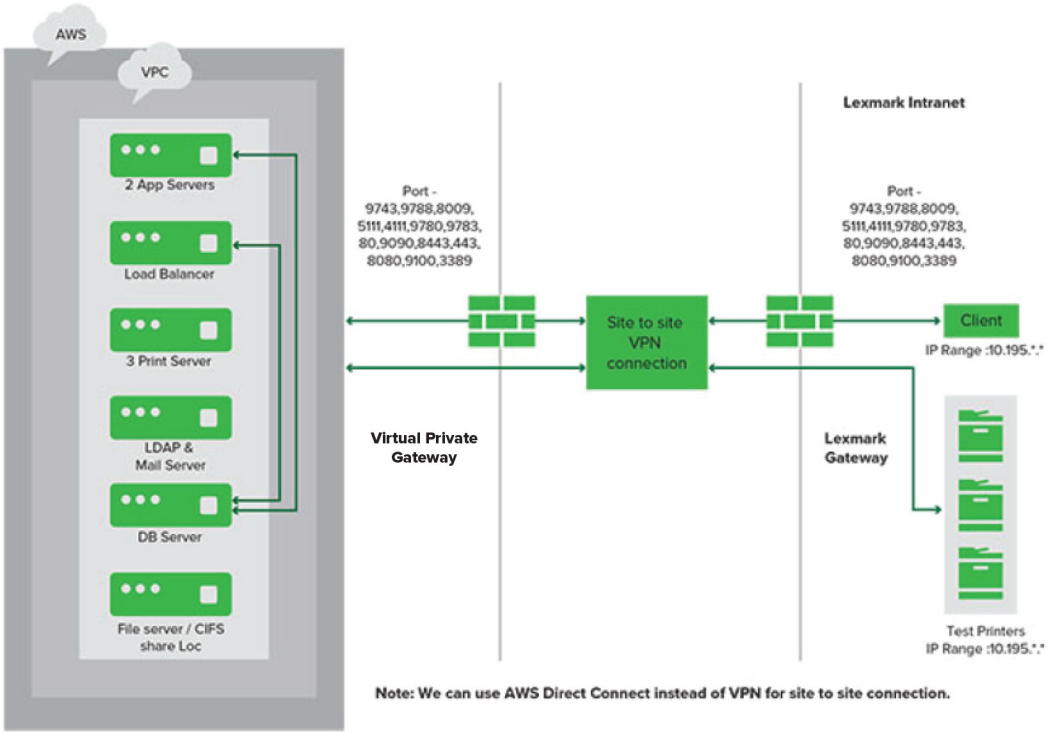
The following shows an environment with one data center:



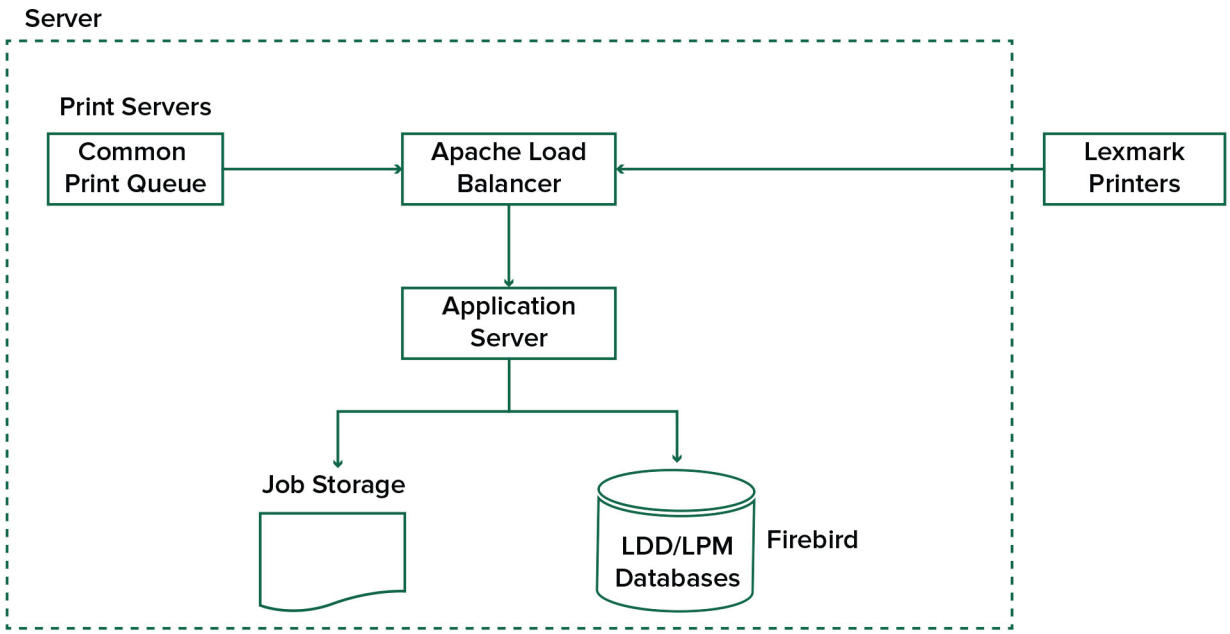
The following shows an environment with two data centers:



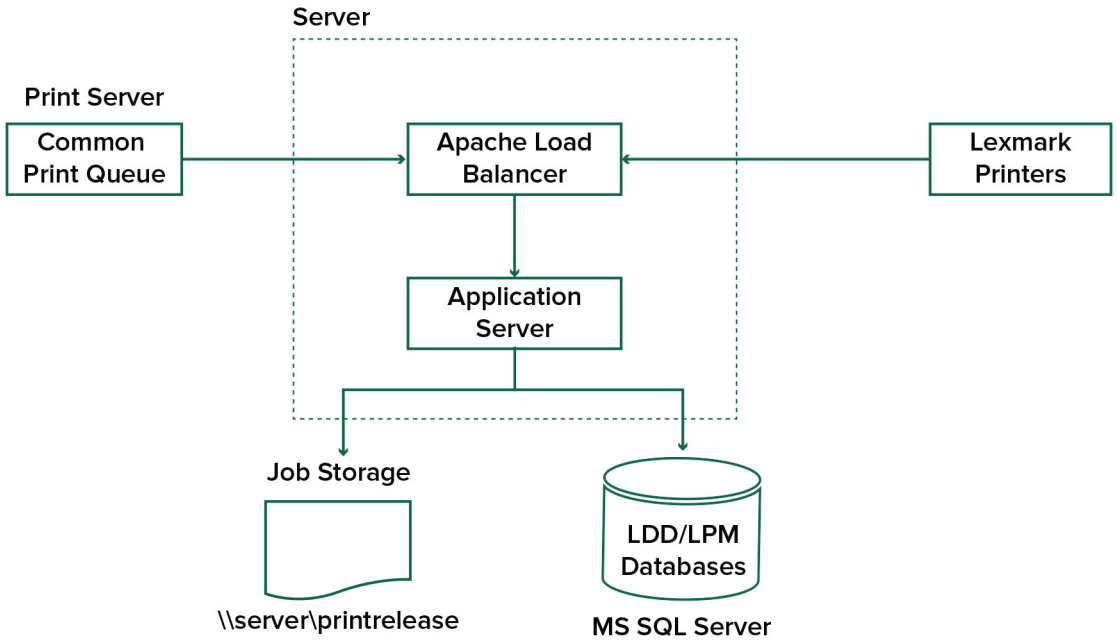
The following shows an environment where LPM is hosted in the cloud:



The following shows a typical workgroup with single-server installation and Firebird Database:



The following shows a workgroup installation with separate print server and Microsoft SQL Server:



Understanding the Print Release application

Print Release is an enterprise-grade printing solution for managing print jobs from your computer or mobile device. The application supports badge authentication, quota enforcement, and usage tracking.

When the Lexmark Universal Print Driver (UPD) is configured to print to the LDD port and a job is printed, the following occurs:

1. Print Release captures the user's Windows login name.
2. The PostScript® or PCL® output file is saved to the server with a date and time stamp.
3. A database table entry is made with the Windows login name (USERID) with the document name and time stamp.

When the print job is released, the Print Release application is called by the Lexmark printer and prompts users to authenticate using their card or badge. Print Release captures the card data, and then compares the badge or card number with the entries in the user directory. Users can also manually authenticate using their user name and password or a personal identification number (PIN).

If the entry is found, then the user name is captured, and the list of print jobs appears on the printer display.

After a job is selected, the Print Release application releases the selected jobs, and then deletes the files and the database entries for the printed jobs. The jobs that are not released are held for the configured time period, and then deleted.

No matter who releases the job, by default, it is automatically deleted from the server after being printed. However, if the reprint feature is enabled, it allows released print jobs to be held for an additional time before being automatically deleted. The job statistics include the user ID of the person who released the job.

Notes:

- When the Document Accounting feature is enabled, all job-related transactions are forwarded to the application server. The data is stored in a database for administrative reporting.
- Several reports are available for analysis and can be generated on an ad hoc basis or scheduled to run on defined intervals.

When using a Mac computer, configure printer share. For more information, see "Submitting jobs from a Mac computer" on page 201.

Understanding the mobile feature

Users can submit and release jobs using their mobile devices such as smart phones and tablets either using e-mail or a mobile application.

Users can send an e-mail to an account monitored by the Lexmark Solutions Email Watcher. When an e-mail arrives, it is sent to the LDD server, and then converted to a printable document based on predefined conversion settings and user-specified settings. It can be printed immediately to a user-specified printer, or it can be integrated with Lexmark Print Release and then printed later.

The Lexmark Print application and Lexmark Print Service Plug-in may also be used to submit documents to the server. The Lexmark Print application also enables the releasing of jobs to a printer. The application is useful for Lexmark printers that do not support eSF applications or for third-party printers. Lexmark Print provides access to both the logged in user's jobs and any delegated accounts.

Note: Lexmark Print application and Lexmark Print Service Plug-in can be downloaded from the Google Play® store or App Store online store.

For more information, see "Configuring mobile devices" on page 60.

Understanding user authentication and delegation

You have full control of your output environment when you incorporate user authentication at the printer or multifunction printer. LPM can be configured to require users to authenticate before retrieving prints or making copies and scans. Requiring user authentication at the printer improves document security by assuring that only the intended recipient retrieves the documents. It also enables tracking of each transaction.

User authentication can occur using a badge, user name and password, or PIN. Lexmark Print Release supports various badge readers.

In some environments, multiple users must access a common set of print jobs. For this environment, user delegation can be configured. Users can assign delegates to retrieve their print jobs. For example, an executive can specify an assistant as a delegate. When a job is delegated, the user who printed the job can release it. Also, when delegates log in, they are prompted whether they want to print their own jobs or the other user's jobs.

User authentication is designed to fit the requirements of the environment where the solution is installed.

Reliability, scalability, and disaster recovery

Load balancing and redundancy

Depending on the volume of transactions, the load balancer, database, and application server components may be installed on a single server or separately on multiple servers. While a single server may be able to handle the load, if it fails, the entire system becomes unavailable. For environments that require high availability, we recommend using multiple servers along with a hardware load balancer.

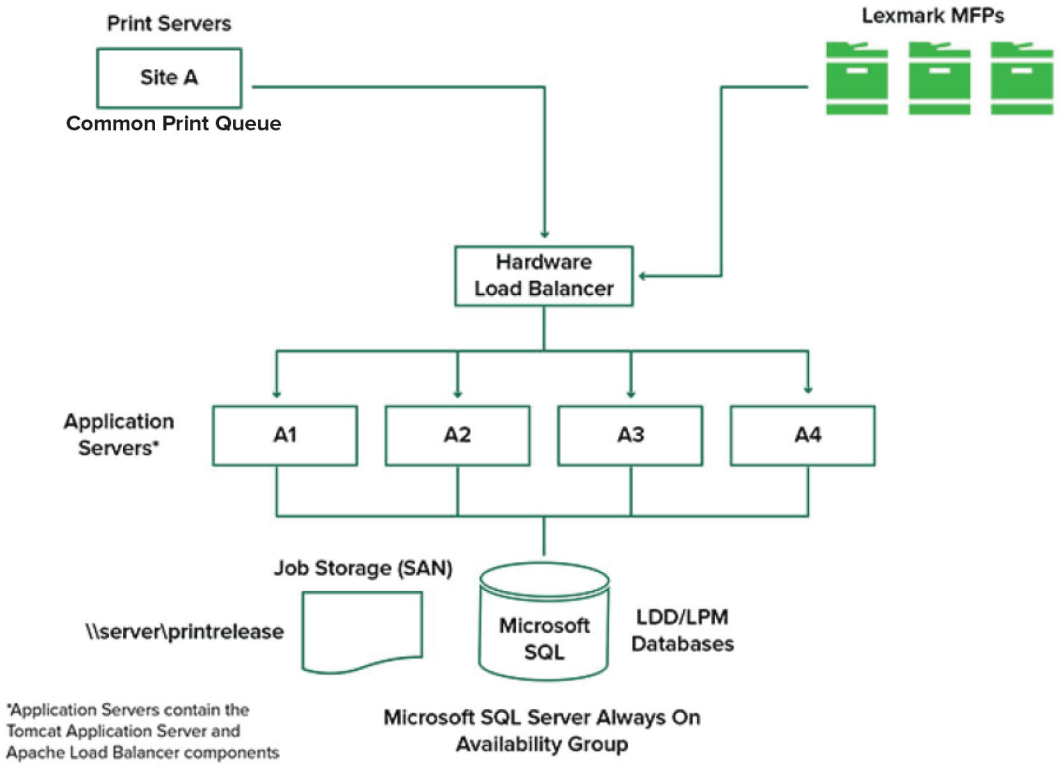
Load-balancing servers receive jobs from print clients, and then balance jobs across transaction servers using load-balancing workers and load estimates. The load balancing is based on the number of session requests.

Note: Make sure that the Lexmark Apache 2.4 service is used as the load-balancing component.

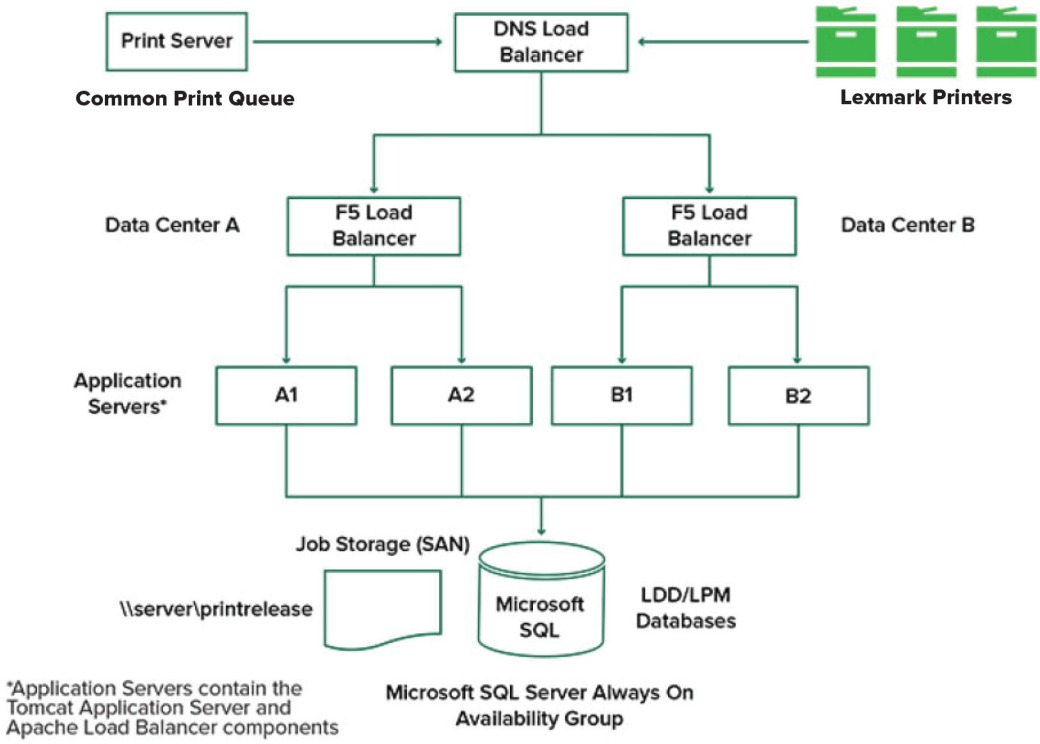
Multiple transaction servers are used to support an increasing number of users and to provide redundancy for continuous uptime when one of the servers fails. Having multiple servers also lets maintenance and upgrades occur without taking down the whole system.

If Firebird is used for the database, then system backups can be scheduled allowing you to restore the system easily in the event of a failure.

The following shows a sample diagram for achieving automated failover or redundancy using a single data center:



The following shows a sample diagram for achieving automated failover or redundancy using two data centers:



System sizing and scalability

LPM is scalable to support multiple clients, submitting jobs to as many servers as required to handle the load. The load balancer selects a server for each received job to distribute the total load and maintain system performance. Using multiple servers also increases system reliability. If one server fails, then the load balancer directs jobs to other servers until the failed server is back online.

The following can be used to determine the number of servers required to process jobs efficiently:

- **Peak demand**—Usually the deciding factor when the average execution time for a solution is under 30 seconds.
- **Concurrency**—Usually the deciding factor when the average execution time for a solution is over 30 seconds. Also, when the database is installed on the recommended hardware and connected using Gigabit Ethernet, it can process 200000 logged messages per hour. This number converts to approximately 40000 jobs per hour when using a typical solution (five logged messages per job). If this limit is reached, then it may be necessary to use multiple LDD systems.

Peak demand

To determine the number of servers necessary to handle peak load for a particular solution, use the following formulas:

- System-wide hourly job rate = (system printer capacity) x (jobs per printer per day) / (length of business day)
- Peak demand = 2 x (system-wide hourly job rate)
- Minimum number of servers = (peak demand) / (single-server throughput for current solution)

Sample scenario

Consider an environment with a system capacity of 300 printers, with each printer averaging 100 jobs per day. If each server processes up to 3000 jobs per hour using the solution, then do the following:

- Determine the system-wide hourly job rate.

  (300 printers) x (100 daily jobs per printer) / (8 hours per day) = 3750 jobs per hour
- Determine the peak demand.

  2 x (3750 jobs per hour) = 7500 jobs per hour
- Determine the minimum number of servers.

  (7500 jobs per hour) / (3000 jobs per hour) = 2.5 servers

To handle the peak load reliably for a solution with an average execution time of 30 seconds or less, your system must have three servers.

Solution processing load	Functions used	Average single-server throughput
Typical	• Some image processing • Printing	6000 to 8000 jobs per hour
Heavy	• Extensive image processing • Bar codes • External processes • Small to medium Document Producer (electronic forms) jobs	2000 to 3000 jobs per hour
Very heavy (optical character recognition)	• Optical character recognition • Large Document Producer (electronic forms) jobs	100 to 200 jobs per hour

Note: Using less than the recommended RAM significantly reduces throughput. For example, a dual-processor server with only 2GB of RAM can process only up to 600–800 jobs per hour when using a heavy solution. For more information, see the *Lexmark Document Distributor SDK Guide*.

Concurrency

Each server that meets the recommended requirements can process up to 30 concurrent jobs from clients. Use the following formula to determine the number of servers that are necessary to meet the concurrency requirements:

Minimum number of servers = (number of printers expected to submit jobs at the same time) / 30

For example, if 100 out of 300 printers are active at the same time, then:

100 / 30 = 3.33

To allow 100 active printers for a solution with an average execution time of 30 seconds or lesser, your system must have four servers.

Performance across geographic locations

Organizations that operate across many areas may have longer execution times as print data moves across the wide area network (WAN). To resolve this issue, configure separate instances of Print Release in each location. Configure one location as the major collection point for accounting data (the parent), and then configure the other locations to operate separately. The other locations must send report data to the parent only on a scheduled basis.

Note: When separate instances are hosted in multiple locations, configure the system to let users send print jobs from one location, and then release them in another. In this case, the print job is pulled across the WAN from the originating location to the destination location. The user does not have to register in the system again to release the print job.

Determining database and file sizing, and other considerations

Database sizing

To determine the database sizing, use the following:

(Transaction data per job) x (number of users) x (typical number of jobs per day) x (length of time to keep the job)

Sample computation

300 bytes per job x 2000 users x 10 jobs per day x 365 days = 2.2GB

To account for variations in print volume over time, we recommend doubling this number.

Job storage sizing

To determine the job storage sizing, use the following:

(Average page per job) x (size per job) x (number of users) x (typical number of jobs per day) x (length of time to keep the job)

Assume the following job size estimates per page:

- Color—2MB
- Monochrome—200KB

Sample computation

5 pages x 2MB x 2000 users x 10 jobs per day x 1 day = 200GB

To account for differences from average job sizes, we recommend doubling this number.

Estimated network bandwidth

Assume the following job size estimates per page:

- Color—2MB
- Monochrome—200KB

To determine the estimated network bandwidth, use the following:

1. *Y* = (number of pages per day x {(%Color x 2MB) + (%Mono x 0.5MB)}) / working hours in a day
2. (*Y* / 3600) x 2

This formula gives you a rough indication of the network traffic in MB per second. It includes assumptions that can cause a wide variance from this estimate. For example, when jobs are sent on a steady state basis throughout the day.

Other considerations

Firebird database

Firebird is the default system database that is bundled with LDD. This database can also be used for LPM. If Firebird is used, then LDD can be configured to back up the system periodically automatically. This configuration lets you easily restore the system in the event of a failure.

Job storage

For larger environments consisting of multiple application servers, we recommend that jobs be stored on a Storage Area Network (SAN) while single-server environments will typically use a local drive for job storage. Regardless of where the jobs are stored, safeguards must be put in place to protect against data loss.

Print server

Windows print servers claim to support up to 10000 users.

Understanding tracking, reporting, and quotas

Tracking

Lexmark Document Accounting tracks device-based transactions performed by users and stores this information centrally for reporting purposes. While the Print Release application only offers tracking of Print Release transactions, Document Accounting includes tracking of Copy, Fax, E-mail, and Scan.

The tracked usage data includes the following:

- User name (if authentication is enabled)
- Job type
- Job name (if enabled)
- Date and time
- Job metadata such as number of pages, color or mono, simplex or duplex, and others

Note: To avoid duplicate entries in the database for a single transaction, make sure that Device Usage and Print Release are not tracking simultaneously.

Reports

A series of reports can be run ad hoc or on a scheduled basis for analysis and reporting. Reports may be created over a specified period using the data stored in the Print Release database and produced as PDF or CSV files. Scheduled reports can be saved or e-mailed to defined users.

Lexmark Document Accounting reports

Report	Description
Top *x* copy users	These reports identify heavy users.
Top *x* fax users	
Top *x* print users	
Top *x* scan users	
Bottom *x* copy users	These reports identify light users.
Bottom *x* fax users	
Bottom *x* print users	
Bottom *x* scan users	
Page savings	This report shows the number of submitted pages sent by users.
Deleted page	This report shows the number of pages that are not printed, and then deleted.
Simplex and Duplex	These reports show the number of simplex and duplex print jobs.
Color and Mono	These reports let you monitor color usage and identify users who print color and monochrome.
Usage Report by Department	This report shows information on users' departments and can be used for planning cost allocation.
Detail Print Report	This report shows the list of printed jobs by user and other details.
Device Usage Report	This report shows the usage of various printer functions per printer.

Note: Information in these reports is provided for statistical analysis and not intended for billing purposes.

Quotas

LPM lets administrators define quotas for the maximum number of print and copy pages produced within a specified time. Quotas can be set per user or per group. Color quotas are the maximum number of color pages that can be printed or copied as a subset of the total user or group quota. For example, a user may have a maximum of 1000 total pages per month, of which 300 may be color pages.

The remaining number of pages available can be shown at the printer each time a user uses Print Release or the copy function. Quotas can also enforce a stop when the allotted page limit is met. A message informs the user that the quota is reached, but that the user is allowed to continue printing.

Understanding Print Management Console

The Lexmark Print Management solution includes Print Management Console, a web-based utility that lets you manage and monitor the solution. Print Management Console is installed with a desktop icon on the server during the installation of the LPM solution.

Print Management Console lets you do the following:

- View and manage current print jobs in the Print Release queue.
- View and manage user and group print delegates (users allowed to release jobs on behalf of another user), if this feature is enabled in your environment.
- View, manage, and register badges, if you are using badge authentication.

- View and manage user and group quotas, if quotas are enabled in your environment.
- View and manage alternate release stations (printers to which print jobs can be released from a given MFP), if this feature is enabled in your environment.

Supported printer models

e-Task 5+ printers	e-Task 5 printers[1]	e-Task 4 printers	e-Task 3 printers
MFPs • CX833se • CX833xse • CX961se • CX961tse • CX962se • CX962tse • CX963se • CX963xse • MX432adwe • MX532adwe • MX632adwe **SFPs** • CS963e • C9655	**7- or 10-inch-screen MFPs** • CX625 • CX635 • CX725 • CX730 • CX735 • CX820 • CX825 • CX860 • CX920 • CX921 • CX922 • CX923 • CX924 • CX930 • MX622 • MX632 • MX721 • MX722 • MX725 • MX822 • MX824 • MX826 • MX931	**7- or 10-inch-screen MFPs** • CX510 • MX610, MX611 • MX6500e • MX710, MX711 • MX810, MX811, MX812 • MX910, MX911, MX912 **4.3-inch-screen MFPs** • CX410 • MX410, MX510, MX511 **4.3-inch-screen SFPs** • CS510 • MS610de • MS810de, MS812de • MS911	**7- or 10-inch-screen MFPs** • 6500e • X548 • X746, X748 • X792 • X925 • X950, X952, X954 **4.3-inch-screen SFPs** • C748 • C792 • C925 • C950

[1] Only printers with firmware level 2 or later are supported.

[2] These printers do not support eSF applications used in hybrid solutions.

[3] These printers may be identified as “C,” “T,” or “W” models in Lexmark Management Console.

[4] These SFPs do not support all prompts that MFPs support.

e-Task 5 printers[1]	X642 printers
4.3-inch-screen MFPs • CX522 • CX532 • CX622 • MX421 • MX521 • MX522 • MX432 • MX532 **4.3-inch-screen SFPs** • CS622 • CS632 • CS720 • CS725 • CS730 • CS735 • CS820 • CS921 • CS923 • CS943 • MS622 • MS632 • MS822 • MS824 • MS826	**5.7-inch-screen MFPs** X642
[1] Only printers with firmware level 2 or later are supported. [2] These printers do not support eSF applications used in hybrid solutions. [3] These printers may be identified as “C,” “T,” or “W” models in Lexmark Management Console. [4] These SFPs do not support all prompts that MFPs support.	

Notes:

- For more information on the latest device and firmware level support, see the *Readme* file.
- Some printer models do not support double-byte characters.

Supported web browsers

- Google Chrome™
- Microsoft Edge
- Mozilla Firefox
- Safari (Mac OS only, not Windows)

Supported languages

- Brazilian Portuguese
- English
- French
- German
- Italian
- Japanese
- Korean
- Simplified Chinese
- Spanish
- Traditional Chinese

Installing Lexmark Print Management

Lexmark Print Management uses the Lexmark Document Distributor (LDD) platform. Before installing LPM, make sure that LDD is installed and that you can successfully log in through the Lexmark Management Console (LMC).

LPM lets you print to a central queue then release the job at any configured Lexmark MFP in your network. LPM provides various features, such as badge authentication, quota enforcement, and usage tracking.

The LPM installer can be used to install the Print Release application to an existing LDD instance. The installer contains the Print Release and Lexmark Print applications.

Notes:

- You can also install LPM silently.
- For more information on configuring the Lexmark Print application with LPM, see "Configuring mobile devices" on page 60.
- For more information on configuring LDD, see the *Lexmark Document Distributor Administrator's Guide*.

LDD dependencies

During installation, LPM detects the version of LDD and installation type. If the minimum LDD version is not detected, then the installer shows an error. For more information on the compatible LPM and LDD versions, see "Compatible LPM and LDD versions" on page 8.

Note: Make sure that the Lexmark Document Server Port (port monitor) is installed for driver submission. For more information, see "Installing the LDD Port monitor software" on page 49.

Document conversion software dependencies

Document conversions are required for e-mail and mobile application job submission. During installation, LPM detects the version of the installed document conversion software.

Note: Only the application servers require a document conversion software.

Before running the LPM installer, install a supported document conversion application on each Tomcat or application servers that are handling document conversions. We recommend installing the document conversion application before running the LPM installer for the solution to use it automatically.

Supported document conversion software and their versions

Application	Supported versions
Microsoft Office	• 2016 • 2013 • 2010 • 2007
Apache® OpenOffice	• 4.1 • 4 • 3.4

Application	Supported versions
LibreOffice	• 6.4.6 • 4 • 3.4

Note: OpenOffice or LibreOffice is required for e-mail or mobile application submissions. To improve the print fidelity of Microsoft Office document formats, use Microsoft Office.

Installing LPM

If you are using mobile or e-mail job submission methods, then make sure that a document conversion software is installed before you begin. For more information, see "Document conversion software dependencies" on page 27.

Note: Print Release does not require a document conversion software.

1. From your computer, run the LPM installer as an administrator.

   Note: The service account must be added to the local administrator group on the server. If the service account is not the part of the local administrator group, then the following steps must be performed to change the permissions.

   a. Right-click **C:\Program Files\Lexmark\Solutions** in the file explorer.
   b. Select the **Security** tab, and click the service account.
   c. Click **Advanced** > **Change Permission**.
   d. Select the service account, and then click **Replace all child object permissions**.
   e. Click **OK** > **Yes**.
   f. Stop and restart the Lexmark Solutions Application Server Service.

2. Select a language, and then click **OK**.
3. Select **Install**.
4. Read and accept the license agreement, and then click **Next**.
5. Select the following applicable components, and then click **Next**:
   - **Print Release**—Contains the core files and services to enable Print Release.
   - **Email**—Enables submission of print jobs through e-mail.
   - **Mobile App**—Enables submission of print jobs through mobile devices running on the iOS operating system and the Android™ platform.
   - **AirPrint**—Enables submission of print jobs through the Mac OS X operating system software and the iOS operating system using the AirPrint software feature.

   Note: To add a component after the initial installation, run the installer again, and then select the component. For more information on the components, see "Files and services index" on page 170.

6 Select any of the following advanced options, and then click **Next**:

- **Update Database**—Runs the Liquibase database-migration scripts, and then updates the database tables and columns.

  Note: Select this setting only when installing or upgrading the first application server.
- **Install Print Release Solution**—Installs the PrintReleasev2 solution.

  Note: This setting is selected by default. If you have a customized solution that is applicable only to your organization, then do not select this setting.
- **Install Mobile Solution**—Installs the mobile solution.

  Note: Select this setting to allow sending of print jobs using mobile devices. If you have a customized solution that is applicable only to your organization, then do not select this setting.

7 Specify the database information, and then click **Next**.

Notes:

- To store Print Release data in the same database as LDD, click **Import**.
- To store Print Release data in a separate Microsoft SQL Server database, select **MSSQL** as the database type.
- When using Microsoft SQL Server, create the instance and database for the Print Release tables.

When using Integrated Security as the authentication method, make sure that the user name and password have the following rights:

- Log on as a service
- Full control privileges to the LDD installation path on the application servers
- Database owner (dbo) to the Microsoft SQL Server Print Release tables

8 Click **Test Connection**.

9 Specify the search base and user attribute information, and then specify the user name and password for connecting to the LDAP server.

Notes:

- If LDAPS and SSL are used, then select **Ignore SSL Certificate Validation**.
- If LDAP information is detected in the backup files, then LPM uses that information and not the values specified in the LDAP Information window.
- When installing on a load balancer, the LDAP Information window is skipped.

10 Click **Install** > **Finish**.

After you install LPM, depending on the server, the Lexmark Solutions Application Server service may take several minutes to start. To check whether the LPM server is ready, do the following:

1 From your computer, open **Task Manager**.

2 Make sure that the CPU performance of the Tomcat7 process remains at less than 3% for more than 15 seconds.

Installing LPM using a backup file

Notes:

- Before you begin, make sure that LDD is working.
- If LDD is installed using Restore Install, then manually create the print job directory.

1 From your computer, run the LPM installer as an administrator.

Notes:

- The Backup feature requires LPM version 2.3.11 or later. If the minimum supported version is not detected, then the installer disables the Backup feature.
- For LPM version 2.4, the minimum supported version of LDD is version 4.8.5. For more information, see "Compatible LPM and LDD versions" on page 8.

2 Select a language, and then click **OK**.

3 Select **Backup Only**.

Note: To ensure that you have the current LDD and LPM configuration available during installation, perform the backup process before taking the LDD system offline.

4 Do either of the following:

Upgrading from LPM version 2.8 or later

a Upgrade LDD. For more information on upgrading LDD, see the *Lexmark Document Distributor Administrator's Guide*.

b Run the LPM installer again, and then select **Include backup during installation** > **Install**.

Upgrading from LPM version 2.7 or earlier

a Navigate to the properties file.

- If you are upgrading from LPM version 2.7 or earlier with backup, or from version 2.5 or earlier, then navigate to the ***<install-dir>*\Lexmark\Solutions\apps\idm\WEB-INF\classes\idm-production-config.properties** file. Here, ***<install-dir>*** is the installation folder of LDD.
- If you are upgrading from LPM version 2.5.0 or earlier, then navigate to the ***<install-dir>*\Lexmark\Solutions\apps\MFPAuth\WEB-INF\classes\database.properties** file, where ***<install-dir>*** is the installation folder of LDD.
- If you are upgrading from LPM version 2.5.0 or earlier to LPM 2.5.1 or later using Firebird database, then do the following:
  1 Navigate to the ***<install-dir>*\Lexmark\Solutions\apps\printrelease\WEB-INF\classes\database.properties** file, where ***<install-dir>*** is the installation folder of LDD.
  2 Update **`database.PIN.dataSource=PIN`** to **`database.PIN.dataSource=SOLUTIONINFO`**.
- If you are upgrading from LPM version 2.3.13 or earlier, or from version 2.3.8 to 2.3.15, then to version 2.6, then navigate to the ***<install-dir>*\Lexmark\Solutions\apps\printrelease\WEB-INF\classes\database.properties** file. Here ***<install-dir>*** is the installation folder of LDD.

b Do one of the following:

- If you are upgrading from LPM version 2.7 or earlier with backup, then in the idm-production-config.properties file, add the following:
  - **lpma-job-data-collector,*ClientSecret***
  - **esf-device-usage,*ClientSecret***
  - **idm-client,*ClientSecret***
  - **esf-cardauth-app,*ClientSecret***
  - **idp.client_credentials.*EntryNumber*=*ClientID*, *ClientSecret*,public**

    Where:

    - ***EntryNumber*** is the corresponding entry number.
    - ***ClientID*** is the client ID.
    - ***ClientSecret*** is the client secret.

    For example, **idp.client_credentials.1=lpma-job-data-collector, 4054bd0a-95e0-11ea-bb37-0242ac130002,public**.

    Notes:

    - If there are existing client IDs and secrets in the file, then continue the numbering.
    - Generate UUIDs (Universally Unique Identifiers) for the client secrets per client ID.
- If you are upgrading from LPM version 2.5 or earlier, then in the idm-production-config.properties file, do the following:
  - Add **primary** to each LDAP attribute. For example, **primary.idm.ldap.url=** and **primary.idm.ldap.base=**.
  - Add the **primary.idm.ldap.domain=\"\"** LDAP attribute.
- If you are upgrading from LPM version 2.5.0 or earlier, then in the database.properties file, add the following in the appropriate table locations before performing backup:
  - **database.BADGE.table=PR_BADGE**
  - **database.BADGE.colUserId=USERID**
  - **database.BADGE.colBadgeId=BADGEID**
  - **database.BADGE.type=*<dbType>***
    Where ***<dbType>*** is either **mssql** or **fb**, depending on the current installation.
- If you are upgrading from LPM version 2.3.13 or earlier, then in the database.properties file, add the following in the appropriate table locations before performing backup:
  - **database.FRAMEWORK.type=*<dbType>***
  - **database.WEBAPP.type=*<dbType>***

  Where ***<dbType>*** is either **mssql** or **fb**, depending on the current installation.
- If you are upgrading from LPM version 2.3.8 to 2.3.15, then to version 2.6, then in the database.properties file, do the following:
  - Replace **\/** with **/**.
  - Remove spaces before and after **=**.

  For example, if the current line is **database.WEBAPP.connect = jdbc:firebirdsql:*IPaddress*\/3050:SOLUTIONINFO**, then the updated line must be **database.WEBAPP.connect=jdbc:firebirdsql:*IPaddress*/3050:SOLUTIONINFO**.

c Upgrade LDD. For more information on upgrading LDD, see the *Lexmark Document Distributor Administrator's Guide*.

d Run the LPM installer again, and then select **Include backup during installation** > **Install**.

Installing LPM silently

Understanding the database settings for silent installation

Note: Silent installation supports workgroups only.

LDD database settings

For Firebird

Setting	Description	Required value
_installOption	The type of installation.	Install
_lddDatabaseType	The type of database that LDD is installed on.	FIREBIRD
_lddLoadBalancerIp	The IP address of the load balancer where LDD is installed.	N/A
_lddDatabaseIp	The IP address of the internal database where LDD is installed.	N/A
_lddDatabasePassword	The password for the database.	N/A
_lddDatabasePasswordEncrypted	The encrypted password of the database. If this setting is not applicable, then provide the value of **_lddDatabasePassword**.	N/A

For Microsoft SQL Server

Setting	Description	Required value
_installOption	The type of installation.	Install
_lddDatabaseType	The type of database that LDD is installed on.	MSSQL
_lddLoadBalancerIp	The IP address of the load balancer where LDD is installed.	N/A
_lddDatabasePort	The port number of the Microsoft SQL Server database that LDD is using.	N/A
_lddDatabaseIp	The IP address of the internal database where LDD is installed.	N/A
_lddDatabasePassword	The password for the database.	N/A
_lddDatabasePasswordEncrypted	The encrypted password of the database. If this setting is not applicable, then provide the value of **_lddDatabasePassword**.	N/A
_lddInstanceName	The instance name of the Microsoft SQL Server database that LDD is using.	N/A

Setting	Description	Required value
_lddDBIntegratedSecurity	Determines whether LDD is using Integrated Security.	integratedSecurity=true;

LPM database settings

For Firebird

Setting	Description	Required value
_DBProduct	The database that LPM is using.	Internal Database
_DBProductName	The type of database that LPM is using.	firebirdsql
_DBIp	The IP address or host name of the database that LPM is using.	N/A
_DBName	The name of the database that LPM is using.	/3050:SOLUTIONINFO
_DBUsername	The user name for the database that LPM is using.	framework
_DBPassword	The password for the database that LPM is using.	Refer to the **connectionPassword** attribute in ***<install-Dir>*\Lexmark\Solutions\apps\wf-ldss\WEB-INF\classes\server.xml** file, where ***<install-Dir>*** is the installation folder of LDD.
_DBPasswordEncrypted	The encrypted password of the database that LPM is using. If this setting is not applicable, then provide the value of **_DBPassword**.	Refer to the **connectionPassword** attribute in ***<install-Dir>*\Lexmark\Solutions\apps\wf-ldss\WEB-INF\classes\server.xml** file, where ***<install-Dir>*** is the installation folder of LDD.

For Microsoft SQL Server

Setting	Description	Required value
_DBIp	The IP address or host name of the database that LPM is using.	N/A
_DBIntegratedSecurity	If MSSQL is using Integrated Security.	integratedSecurity=true;
_DBName	The name of the database that LPM is using.	databasename=<DB Name>;
_DBUsername	The user name for the database.	N/A
_DBPassword	The password for the database.	N/A
_DBDriver	The driver for the database that LPM is using.	com.microsoft.sqlserver.jdbc.SQLServerDriver

Setting	Description	Required value
_DBDialect	The database dialect that LPM is using.	org.hibernate.dialect.SQLServer2008Dialect
_DBValidationQuery	The query used to validate the database.	1
_DBQuartzDriverDelegate	The driver for Quartz that LPM is using.	org.quartz.impl.jdbcjobstore.MSSQLDelegate
_DBForwardSlashes	The other characters to put in Java Database Connectivity for Microsoft SQL Server.	//
_DBProduct	The database that LPM is using.	MSSQL
_DBProductName	The type of database that LPM is using.	sqlserver
_DBPort	The port number of the database that LPM is using.	N/A
_DBInstanceName	The instance name of the Microsoft SQL Server database that LPM is using.	N/A
_MSDBName	The database name of Microsoft SQL Server.	N/A
_MSDBUserName	The user name for Microsoft SQL Server.	N/A
_MSDBPassword	The password for Microsoft SQL Server.	N/A

LPM LDAP settings

Setting	Description	Required value
_LDAPURL	The IP address or host name of the LDAP server.	Use either of the following formats for its value: • **ldap://*IPaddress*** • **ldaps://*IPaddress*** Where ***IPaddress*** is the host name or IP address of the LDAP server.
_LDAPPort	The port number of the LDAP server.	N/A
_LDAPSearchBase	The search base of the LDAP server.	N/A
_LDAPUserAttribute	The user attribute of the LDAP server.	N/A

Setting	Description	Required value
_LDAPUserName	The user name for the LDAP server when anonymous bind is not enabled.	N/A
_LDAPPassword	The password for the LDAP server when anonymous bind is not enabled.	N/A
_LDAPPasswordConfirm	The password for the LDAP server when anonymous bind is not enabled.	N/A
_LDAPPasswordEncrypted	The encrypted password of the LDAP server when anonymous bind is not enabled. If this setting is not applicable, then provide the value of **_LDAPPassword**.	N/A
_LDAPAuthMethodState	The method for LDAP authentication.	• Username • Anonymous
_LDAPIgnoreSSLCertificateValidationFlag	Disables certificate validation for LDAP. This setting is only used when using LDAPS.	• true (Ignores the certificate) • false (Validates the certificate)

LPM installation settings

Setting	Description	Required value
_silentEmailComponent	Installs the e-mail component.	• 1 (Install) • 0 (Do not install)
_silentMobileComponent	Installs the mobile component.	• 1 (Install) • 0 (Do not install)
_silentAirprintComponent	Installs the AirPrint component.	• 1 (Install) • 0 (Do not install)
_silentInstallPRSolution	Installs the Print Release solution.	• 1 (Install) • 0 (Do not install)
_silentInstallMobileSolution	Installs the mobile solution. **Note:** Make sure that either **_silentMobileComponent** or **_silentAirprintComponent** is set to 1.	• 1 (Install) • 0 (Do not install)

Setting	Description	Required value
_silentInstallLiquibase	Runs the Liquibase migration.	• 1 (Install) • 0 (Do not install)

Installing LPM silently

1 Using a text editor, create the **silent-settings.ini** file.

2 Specify the correct configuration.

Sample code for LDD and LPM using Firebird and Microsoft SQL Server database

Sample code for Firebird

```
_installOption=Install
_lddDatabaseType=FIREBIRD
_lddLoadBalancerIp=<IP_address>
_lddDatabaseIp=<IP_address>
_lddDatabasePassword=<Firebird_Database_Password>
_lddDatabasePasswordEncrypted=<Firebird_Database_Password>

_LDAPURL=ldap://<IP_address>
_LDAPPort=<LDAP_port>
_LDAPSearchBase=dc=kinton,dc=com
_LDAPUserAttribute=sAMAccountName
_LDAPUserName=<username@kinton.com>
_LDAPPassword=<Password>
_LDAPPasswordConfirm=<Password>
_LDAPPasswordEncrypted=<Password>
_LDAPAuthMethodState=Username

_DBProduct=Internal Database
_DBProductName=firebirdsql
_DBIp=<IP_address>
_DBName=/3050:SOLUTIONINFO
_DBUserName=framework
_DBPassword=<Firebird_Database_Password>
_DBPasswordEncrypted=<Firebird_Database_Password>
_DBDriver=org.firebirdsql.jdbc.FBDriver
_DBDialect=org.hibernate.dialect.FirebirdDialect
_DBValidationQuery=select 1 from RDB$DATABASE
_DBQuartzDriverDelegate=org.quartz.impl.jdbcjobstore.StdJDBCDelegate
_DBPort=<Port_number>

_silentEmailComponent=1
_silentMobileComponent=1
_silentAirprintComponent=0
_silentInstallPRSolution=1
_silentInstallMobileSolution=1
_silentInstallLiquibase=1
```

Sample code for Micro Server

```
_installOption=Install
_lddDatabaseType=MSSQL
_lddLoadBalancerIp=<IP_address>
_lddDatabasePort=<Port number>
_lddDatabaseIp=<IP_address>
_lddDatabaseUsername=ktest@lrdc.lexmark.ds
_lddDatabasePasswordEncrypted=<Password>
_lddDBInstanceName=
_lddDBIntegratedSecurity=integratedSecurity=true;

_LDAPURL=ldap://<IP_address>
_LDAPPort=<Port number>
_LDAPSearchBase=dc=kinton,dc=com
```

```
_LDAPUserAttribute=sAMAccountName
_LDAPUserName=username@kinton.com
_LDAPPassword=<Password>
_LDAPPasswordConfirm=<Password>
_LDAPPasswordEncrypted=<Password>
_LDAPAuthMethodState=Username

_DBIp=<IP_address>
_DBIntegratedSecurity=integratedSecurity=true;
_DBName=;databasename=SOLUTIONINFO;
_DBUserName=<Username>
_DBPassword=<Password>
_DBDriver=com.microsoft.sqlserver.jdbc.SQLServerDriver
_DBDialect=org.hibernate.dialect.SQLServer2008Dialect
_DBValidationQuery=select 1
_DBQuartzDriverDelegate=org.quartz.impl.jdbcjobstore.MSSQLDelegate
_DBForwardSlashes=//
_DBProduct=MSSQL
_DBProductName=sqlserver
_DBPort=<Port_number>
_DBInstanceName=

_MSDBName=SOLUTIONINFO
_MSDBUserName=<Username>
_MSDBPassword=<Password>

_silentEmailComponent=1
_silentMobileComponent=1
_silentAirprintComponent=0
_silentInstallPRSolution=1
_silentInstallMobileSolution=1
_silentInstallLiquibase=1
```

Sample code for Serverless environment

```
_installOption=Install
_lddLoadBalancerIp=<IP_address>
_lddDatabaseType=FIREBIRD
_lddDatabaseIp=<IP_address>
_lddDatabasePasswordEncrypted=<Firebird_Database_Password>

_LDAPURL=ldap://<IP_address>
_LDAPPort=389
_LDAPSearchBase=dc=kinton,dc=com
_LDAPUserAttribute=sAMAccountName
_LDAPUserName=username@kinton.com
_LDAPPassword=<Password>
_LDAPPasswordConfirm=<Password>
_LDAPPasswordEncrypted=<Password>
_LDAPAuthMethodState=Username

_DBIp=<IP_address>
_DBIntegratedSecurity=integratedSecurity=true;
_DBName=;databasename=HYBRID;
_DBUserName=<Username>
_DBPassword=<Password>
_DBDriver=com.microsoft.sqlserver.jdbc.SQLServerDriver
_DBDialect=org.hibernate.dialect.SQLServer2008Dialect
_DBValidationQuery=select 1
_DBQuartzDriverDelegate=org.quartz.impl.jdbcjobstore.MSSQLDelegate
_DBForwardSlashes=//
_DBProduct=MSSQL
_DBProductName=sqlserver
_DBPort=3341
_DBInstanceName=<Instance_name>

_MSDBIp=<IP_address>
_MSDBName=HYBRID
_MSDBUserName=<Username>
_MSDBPassword=<Password>
_MSDBInstanceName=<Instance_name>
```

```
_silentEmailComponent=1
_silentMobileComponent=1
_silentAirprintComponent=0
_silentInstallPRSolution=1
_silentInstallMobileSolution=1
_silentInstallLiquibase=1
```

Sample code for LDD and LPM using a Firebird database

```
_installOption=Install
_lddLoadBalancerIp=<LB IP Address>
_lddDatabasePassword=<Firebird_Database_Password>
_lddDatabasePasswordEncrypted=ENC (qJj0mHFqIm6dfigOL/57tw==)
_lddDatabaseType=FIREBIRD
_LDAPURL=<LDAP IP Address>
_LDAPPort=<LDAP Port>
_LDAPSearchBase=<LDAP Search Base>
_LDAPUserAttribute=<LDAP User Attribute>
_LDAPUserName=<LDAP Username>
_LDAPPassword=<LDAP Password>
_LDAPPasswordConfirm=<LDAP Password>
_LDAPPasswordEncrypted=ENC (4dw4psQIC/uas/H7HMcqOQ==)
_LDAPAuthMethodState=
_DBIp=<DB IP Address>
_DBName=/3050:SOLUTIONINFO
_DBUserName=framework
_DBPassword=<Firebird_Database_Password>
_DBPasswordEncrypted=ENC (qJj0mHFqIm6dfigOL/57tw==)
_DBProductName=firebirdsql
_DBdriver=org.firebirdsql.jdbc.FBDriver
_DBDialect=org.hibernate.dialect.FirebirdDialect
_DBValidationQuery=select 1 from RDB$DATABASE
_DBQuartzDriverDelegate=org.quartz.impl.jdbcjobstore.StdJDBCDelegate
_DBForwardSlashes=
_DBPRoduct=Internal Database
_DBInstanceName=
_DBPort=3050
_MSDBName=
_MSDBUserName=
_MSDBPassword=
_silentEmailComponent=1
_silentMobileComponent=1
_silentAirprintComponent=1
_silentInstallPRSolution=1
_silentInstallMobileSolution=1
_silentInstallLiquibase=1
```

3. Save the file.
4. In the command line, type the following:

   ***LPMinstaller*\LexmarkPrintManagement-*version*.exe /S /SILENTCONFIG=*Path*\silent-settings.ini**

   Where:

   - ***LPMinstaller*** is the folder path of the LPM installer.
   - ***version*** is the version of the LPM installer.
   - ***Path*** is the folder path of the silent-settings.ini file.

Understanding the LPM installer backup feature

The backup feature of the installer copies the LPM configuration files in the **%allusersprofile%\Lexmark \PrintManagement\backuprestore** folder.

The following files are saved:

Load balancer	Server
• ActiveMQ wrapper.conf • Apache2 – httpd.conf – httpd-ssl.conf • EmailWatcher – config_EmailWatcher.properties – l4j_EmailWatcher.xml • Aggregator Report service Application.properties	• IDM – *.properties – log4j-config.groovy • LPM – *.properties – log4j-config.groovy • Mobile – *.properties – log4j-config.groovy • MFPAuth *.properties • PrintRelease *.properties • wf-ldss – OpenOfficeToPDFClass.properties – MsOfficeDocConvClass.properties

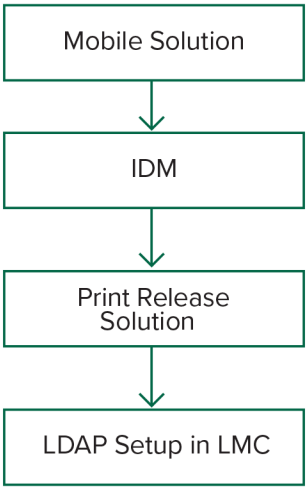
The following files are saved and are used to pre-populate fields and restore settings during the installation:

Load balancer	Server
• EmailWatcher config_EmailWatcher.properties	• PrintRelease – ldap.properties – ldss.properties – paper.properties – scan.properties • wf-ldss – OpenOfficeToPDFClass.properties – MsOfficeDocConvClass.properties

When uninstalling LPM, the original Apache configuration files are restored. To make sure that the current LPM configuration is available during installation, perform the backup before taking the system offline.

Understanding the LDAP backup process

The following is the lookup order for LDAP information:



The LDAP information is stored in the **%allusersprofile%\Lexmark\PrintManagement\backupRestore \ldapinfo.txt** file.

Note: The password in this file is encrypted.

If LDAP information is detected from a source, then LPM uses that information for the backup and stops searching from other LDAP sources. For example, if LDAP information is detected from the Mobile Print solution, then it does not proceed to searching the IDM.

Supported versions

The backup feature is available for LDD version 4.8.0, and LPM version 2.3.11 or later.

If you are upgrading from earlier versions of LPM, then the installation does not proceed until LDD version 4.8.5 or later is detected. For more information, see “Compatible LPM and LDD versions” on page 8.

Understanding the database

Notes:

- The Print Release tables are created automatically during installation.
- It is not necessary to run the SQL scripts manually.

When using Microsoft SQL Server, make sure that:

- The instance and database are created using the Microsoft SQL Server Management Console before running the installer.
- The database account used when accessing the Print Release tables is a database owner.

Microsoft SQL Server and Firebird

Firebird is the default system database that is bundled with LDD and it can also be used for LPM. Microsoft SQL Server can also be used as an alternate for Firebird. For Microsoft SQL Server, manually create the LPM database before launching the LPM Installer. During the installation, LPM populates the various LPM database properties files with the appropriate connection strings. It also automatically creates the LPM tables in the specified database. Depending on whether the installation is a non-serverless setup or a serverless setup, the data sources may vary. In a non-serverless setup, the same database is used for both LDD and LPM. In a serverless setup, Firebird is used for LDD, and Microsoft SQL Server is used for LPM.

Note: For Firebird, the tables are automatically put in the **SOLUTIONSINFO** database. For Microsoft SQL Server, we recommend using the customer name as the **PRINTRELEASE** database.

LPM references the following three database properties files:

- ***<Install-Dir>*\Lexmark\Solutions\apps\printrelease\WEB-INF\classes\database.properties**—Contains the database configuration that is referenced by the PrintReleasev2 solution during execution.
- ***<Install-Dir>*\Lexmark\Solutions\apps\lpm\WEB-INF\classes\database-production-config.properties**—Contains the database configuration for the LPM Admin Portal.
- ***<Install-Dir>*\Lexmark\Solutions\apps\idm\WEB-INF\classes\database-production-config.properties**—Contains the database configuration for the Identity Management Service.

For example, the database configuration for the LPM Admin Portal, contains a default and secondary datasource section. In a non-serverless setup, the default and secondary datasources point to the same database. In a serverless setup, the default datasource points to the LPM Microsoft SQL database, and the secondary datasource points to the LDD Firebird database.

Database information

During installation, LPM determines database information from the backup files and pre-populates the fields with the data. Make sure that the information is correct. If a backup file is not available, then the fields are empty.

LPM supports the following:

- Workgroup installation for LPM and LDD on Firebird
- Serverless installation for LDD on Firebird and LPM on Microsoft SQL Server
- Full LDD and LPM installation on Microsoft SQL Server

Note: In LPM version 2.7 or later, installation on the load balancer requires providing database information for use by the Lexmark Solutions Aggregator service.

Instance name

When using Microsoft SQL Server, you may specify an instance name for the Print Release database. If the instance name and port number are not specified, then the default instance and port number are used. If you have changed the port number, then specify it. The most common default port number is 1433.

To use a named instance, enter the name in the Instance Name field. Specifying a port number is optional. However, when specified, make sure that the port number is correct for the specified instance name.

Security type

When using Microsoft SQL Server, select **Integrated Security** to use Windows authentication or **Microsoft SQL Server** authentication. If you select **Microsoft SQL Server**, then provide the user name and password.

If you select **Integrated Security**, then you must run the LPM installer as a user with db_owner permissions to the database. Then you must enter the credentials in the Username and Password fields.

Note: When you select **Integrated Security**, any LPM services that communicate directly with the database are automatically configured to use these credentials.

Updating the password

When using Microsoft SQL Server authentication and Microsoft SQL Server is used only for LPM, then do the following:

1. Using a text editor, open the following files:
   - **apps\printrelease\WEB-INF\classes\database.properties**
   - **apps\idm\WEB-INF\classes\database-production-config.properties**
   - **apps\lpm\WEB-INF\classes\database-production-config.properties**
   - **apps\MFPAuth\WEB-INF\classes\database.properties**
2. Update the encrypted password using plain text:

   From:

   ```
   dataSource.password = ENC(TO86KjCYKsH7XoInQ1gj/gxj9390+C/g)
   ```

   To:

   ```
   dataSource.password = newpassword
   ```

   Note: The password is automatically encrypted after the Lexmark Solutions Application Server is restarted.
3. Restart the Lexmark Solutions Application Server service.
4. Using a text editor, open the **services\lpm-reports-service\application.properties** file.
5. Update the encrypted password using plain text:

   From:

   ```
   dataSource.password = ENC(TO86KjCYKsH7XoInQ1gj/gxj9390+C/g)
   ```

   To:

   ```
   dataSource.password = newpassword
   ```
6. Restart the Lexmark Reports Aggregator Service.
7. Using a text editor, open the **services\lpm-user-data-management-service\config\application.properties** file.
8. Update the encrypted password using plain text:

   From:

   ```
   dataSource.password = ENC(TO86KjCYKsH7XoInQ1gj/gxj9390+C/g)
   ```

   To:

   ```
   dataSource.password = newpassword
   ```
9. Restart the Lexmark User Data Management Service.

When using Integrated Security authentication

1. Navigate to the Services dialog.
2. Locate the following:
   - Lexmark Solutions Application Server
   - Lexmark Solutions Apache Agent
   - Lexmark Reports Aggregator Service
3. Right-click the service, and then click the **Log On** tab.
4. Make sure that **This Account** is selected, and then type your password.
5. Click **OK**.

Understanding LPM installation using a Microsoft SQL database

To install LPM using M SQL, the following are required:

1. The user must be a member of the **dbcreator** server role to create the databases when executing the script.
2. For installation, the DB service account must have the following roles:
   - db_ddladmin
   - db_datawriter
   - db_datareader

Understanding the LDAP information

During installation, the LPM installer lets you enter LDAP information and writes information to appropriate locations. Passwords are encrypted in each location. LPM determines LDAP information from the backup files and pre-populates the fields with the data. Make sure that the information is correct. If a backup file is not available, then the fields are empty.

Note: If LDAP information is detected in the backup files, then the installer uses that information, and then populates them in the LDAP information window. You cannot edit this information.

Enter the LDAP information that must be used to validate a user's access to LPM. Enter the full URL to the LDAP server. For example, **`ldap://server.company.com`** or **`ldap://`*`IPaddress`***, where ***`IPaddress`*** is the IP address of the LDAP server.

Note: You may use LDAP or LDAPS.

The LDAP port number is collected as a separate field and must not be entered in the URL field. For more information on the supported port numbers for LDAP and LDAPS, see "Standard port numbers for LDAP and LDAPS" on page 122. You may use an anonymous connection or provide credentials for connecting to the LDAP server.

Note: Many Active Directory and LDAP servers are configured to block anonymous LDAP bind requests. Make sure that your LDAPS settings are configured correctly.

If LDAPS is used, then untrusted SSL certificates can cause the test to fail. Before attempting a connection, install SSL certificates on your server. You can also set the LPM installer to ignore LDAP SSL validation by selecting **Ignore SSL certification validation** during installation.

Specifying the LDAP configuration is optional for Print Release, but it is required for the following:

- Accessing Print Management Console
- Submitting jobs using a mobile device
- Submitting jobs using AirPrint

During installation, the LDAP settings are written to property files. Make sure that the solution settings are configured after the installation.

When updating LDAP settings in a multiple-domain environment, update the ldap.properties file in the ***<install-Dir>*\Lexmark\Solutions\apps\printrelease\WEB-INF\classes** folder, where ***<install-Dir>*** is the installation folder of LPM. Restart the Lexmark Solutions Application Server service after the update.

Notes:

- In a multiple-domain environment, make sure that the LDAP settings in the LPM administrator portal and the ldap.properties file match.
- In a single-domain environment, only the solution LDAP settings and the LPM administrator portal settings must match.

Installing LDAP SSL certificates on LPM server

If LDAP certificate is self-signed, then add the certificate to the Java keystore.

Note: This is not required for CA-signed certificates.

1. From the command prompt, navigate to ***<LDD-Install-Dir>*\Lexmark\Solutions\jre\bin**.
2. Type **>keytool -import -alias *<any-cert-alias>* -keystore "*<LDD-Install-Dir>*\Lexmark\Solutions\jre\lib\security\cacerts" -file "*<path-to-cert-file>*"**.

   where:

   - ***<LDD-Install-Dir>*** is the LDD installation path.
   - ***<any-cert-alias>***is any unique alphanumeric string to be the alias of the certificate in the keystore.
   - ***<path-to-cert-file>*** is the path to the certificate file.
3. Restart the Lexmark Solutions Application Server (LSAS) service.

Configuring post-installation settings

Configuring multiple domains

This section is optional and applicable only If your environment has multiple domains.

Configuring multiple domain support for solutions

If multiple domain support is enabled in Solutions Configuration, then do the following:

1. Using a text editor, open the ***<install-Dir>*\Lexmark\Solutions\apps\printrelease\WEB-INF\classes\ldap.properties** file, where ***<install-Dir>*** is the installation folder of LDD.
2. Configure the following entries:

```
# comma-separated list of all fully qualified domain name (all in lower case, no spaces)
ldap.domainNames=

# determines how we search for direct print user's domain otherwise, use name as is
# 0 = don't search; use name as is
# 1 = stop search at first match
# 2 = search all domains and select only if one match found;
ldap.searchUsers=
```

   Note: Make sure to add and configure the following entries for each domain in your environment with their appropriate values.

```
# ldap settings for each domain; all entries required but can be left blank if not
needed/applicable.
# Change <domain> to appropriate value, for example, if domain is
"somegroup.somecompany.com", then
# ldap.somegroup.somecompany.com.server=somevalue
ldap.<domain>.server=
ldap.<domain>.port=

#valid value for the ssl is either 0 or 1
ldap.<domain>.ssl=

ldap.<domain>.searchbase=
ldap.<domain>.domain=
ldap.<domain>.loginuser=
ldap.<domain>.loginpw=
ldap.<domain>.userattr=
ldap.<domain>.mailattr=
ldap.<domain>.homedirattr=
ldap.<domain>.custom1attr=
ldap.<domain>.custom2attr=
ldap.<domain>.custom3attr=

# LPM-Scan To Network settings domain is always required; should be the short domain name
snf.<domain>.domain=

# user and pw can be left blank if not using a service account
snf.<domain>.user=
snf.<domain>.pw=

# fileshare can be left blank if not using one of the Fileshare destination options
snf.<domain>.fileshare=
```

3. Save the file.
4. Restart the Lexmark Solutions Application Server service.

Configuring multiple domain support for LPM user portal

1. Using a text editor, open the ***<install-Dir>*Lexmark\Solutions\apps\idm\WEB-INF\classes\idm-production-config.properties** file, where ***<install-Dir>*** is the installation folder of LDD.
2. Configure the following entries:

```
# This section SHOULD always be present
primary.idm.ldap.url=
primary.idm.ldap.base=
primary.idm.ldap.userAttribute=
primary.idm.ldap.userDn=
primary.idm.ldap.password=
primary.idm.ldap.domain=
primary.idm.ldap.custom1attr=
primary.idm.ldap.custom2attr =
primary.idm.ldap.custom3attr =

# Make sure to add and configure the following entries for each domain in your
environment with their appropriate values, where <domain> is the short name for the domain
<domain>.idm.ldap.url=
<domain>.idm.ldap.base=
<domain>.idm.ldap.userAttribute=
<domain>.idm.ldap.userDn=
<domain>.idm.ldap.password=
<domain>.idm.ldap.domain=
<domain>.idm.ldap.custom1attr=
<domain>.idm.ldap.custom2attr =
<domain>.idm.ldap.custom3attr =

# These are the common properties
idm.token.expirationInMinutes=60
idm.token.maxTokensToPrune=1000

idm.lddLoadBalancer=
idm.ldd.baseUri=
grails.server.port.http=
grails.server.port.https=
grails.plugins.springsecurity.portMapper.httpPort=
grails.plugins.springsecurity.portMapper.httpsPort=
tomcat.keystorePath =
tomcat.keystorePassword =

idp.client_credentials.1=
idp.client_credentials.2=
```

3. Save the file.
4. Restart the Lexmark Solutions Application Server service.

Note: When the Lexmark Solutions Application Server service is restarted, LDAP configuration resets based on the idm-production-config.properties file. Any changes done on the LDAP configuration using the LPM administrator portal rolls back. This is applicable only to versions earlier than LPM 2.8.

Configuring the "LPM Premise for Google Chrome" extension

1. From your computer, unzip the **LPM Premise Chrome Extension** package.

   Note: To obtain the package, contact your Lexmark representative.
2. Using a text editor, open the **staticVariables.js** file.
3. Update the following variables:
   - **url_idp = *x***
   - **url_lpm = *y***

Where:

- ***x*** is the IDP URL.
- ***y*** is the LPM URL.

Sample variables

```
var url_idp = "https://<LDD-load-balancer-address>"
var url_lpm = "https://<LDD-load-balancer-address>"
Or
var url_idp = "http://<LDD-load-balancer-address>:9780"
var url_lpm = "http://<LDD-load-balancer-address>:9780"
```

4 Package the **LPM Premise Chrome Extension** to a .zip file, and then distribute to users for installation.

Installing the "LPM Premise for Google Chrome" extension

1 From your computer, unzip the **LPM Premise Chrome Extension** package.

2 Open **Google Chrome**, and then type **`chrome://extensions/`**.

3 Set the browser to developer mode.

4 Click **LOAD UNPACKED**, and then select the unzipped folder of the extension.

Configuring Lexmark Print Management

Accessing Lexmark Management Console

Before you begin, make sure that web browser cookies are enabled.

1. Open a web browser, and then type either of the following URLs:
   - **http://*hostname*:9780/lmc**
   - **https://*hostname*/lmc**

   Where ***hostname*** is the host name or IP address of the load balancer.
2. Log in as an administrator.

   Notes:

   - The default user name and password is **admin**.
   - If Lexmark Management Console is configured to connect to an LDAP server, then use your LDAP user name and password.

It may take several minutes to start all services when the server is first booted. If the Lexmark Management Console cannot be accessed immediately after booting the system, then wait a few minutes, and then try again.

Changing the status of the server

LPM lets you control whether jobs from the load balancer are sent to the server by setting the server online or offline. In an enterprise environment, you can see the status of all application servers from all workgroup systems in the System Status page within the LMC. However, to set a server online or offline, you must connect to the LMC of the specific server that you want to manage.

1. From Lexmark Management Console, click **System** > **System Status**.
2. Select a server.
3. Click **Set Online** or **Set Offline**.

   Notes:

   - Make sure that your printers and servers have sufficient licenses. For more information on purchasing licenses, contact your Lexmark Technical Program Manager.
   - Setting the server offline still allows administrators to stay connected to the server.

Adding a print server to a software client group

Configure the LDD server to communicate with the print server where print jobs are sent. In a single-server setup, the IP addresses of the LDD server and the print server are the same.

1. From Lexmark Management Console, click the **Software Client Groups** tab.
2. From the Software Client Groups section, select **Print Server**.
3. From the Tasks section, select **Client Profiles**.

4 In the Address field, enter the IP address of the print server.

5 Click **Add** > **Save**.

Creating the Print Release queue

Installing the LDD Port monitor software

1 From the server that must host the Windows-based Print Release queue, navigate to the LDD installation package.

2 Run **Setup.exe** as an administrator.

3 Select a language for the installation, and then click **OK**.

4 From the LDD Setup window, select **Install Client Software**, and then click **Next**.

5 Select **Install LDD system components**, and then click **Next**.

6 Read and accept the license agreement, and then click **Next**.

7 From the list of components, select **Client Software** and **Print and Send**, and then click **Next**.

8 Specify a location for the installation, and then click **Next**.

9 From the Client Software Type window, select the client software type.

10 From the Install Lexmark Client Software window, do the following:
- In the LoadBalancer IP Address field, type the load balancer address.
- From the Profile Name menu, select the profile.

11 Click **Next**.

12 From the Install Lexmark Client Service window, do the following:
- Select **Enable Secure Print Support**.
- Select **Allow Unencrypted print job submission**.

13 Click **Next** > **Install**.

14 If the print spooler is configured as a clustered resource, then move the cluster group to the node where the port monitor software is installed.

15 Repeat step 1 through step 7 on the node where the port monitor software is installed.

16 If necessary, move the cluster group back to the original active node.

Configuring the print queue

Note: To encrypt your print jobs securely, install UPD version 3.0.

1 From your computer, run the UPD administrator installer.

Note: Download UPD from **http://lexmark.com**.

2 When prompted for the installation type, select **Extract**, and then clear **Start the installation software**.

3. Browse to the location of the extracted UPD files.

   Note: We recommend extracting files to the root of C:\ drive or a directory off C:\ drive.

4. Click **Add a printer using TCP/IP address or host name**, and click **Next**.

5. Enter the following information:
   a. **Device type**—Select the device type.
   b. **Hostname or IP address**—Type the client IP address or host name.
   c. **Port name**—Type the name of the port.

      Note: Query the printer and automatically select the driver to use is selected by default.

6. From the **Device type** menu, click Standard and then select **Generic Network Card**.

7. Click **Next**.

8. When prompted to select a printer, select **Have Disk**, and then browse to the ***<extract_path>*** **\InstallationPackage\Drivers\Print\GDI** folder, where ***<extract_path>*** is the location of the extracted UPD files.

   Note: We recommend extracting files to the root of C:\ drive or to a directory of C:\ drive.

9. Run any of the .inf files.

10. Type a descriptive printer name, and click **Next**.

11. Right-click the new print queue, and then select **Printer properties**.

12. Accept the certificate.

13. From the Printer properties window, click **Encryption** tab.

14. Select **Always encrypt**, to encrypt print jobs.

15. Click **Apply**.

16. Click **Sharing** tab, and then click **Additional Drivers**.

17. Select the necessary alternative print drivers, and then click **OK**.

    Note: When using a 64-bit server, the most common alternative print driver is x86 Type 3 User Mode.

18. When prompted for the x86 processor, browse to the ***<extract_path>*****\InstallationPackage\Drivers\Print \GDI** folder, where ***<extract_path>*** is the location of the extracted UPD files.

19. Run any of the .inf files.

20. When prompted for the print processor file, browse to the ***<extract_path>*****\InstallationPackage\Drivers \Print\GDI\i386** folder, where ***<extract_path>*** is the location of the extracted UPD files.

21. Run the **ntprint.inf** file.

22. Click **OK**.

Configuring the print driver

1. Depending on the operating system of your server, from your computer, navigate to the Print Management console.

   Note: For Windows Server 2012, you can also navigate to the Devices and Printers window.

2. Right-click the printer icon, and then select **Properties**.
3. Click the **Sharing** tab, and then clear **Render print jobs on client computers**.
4. Click the **Advanced** tab, and then select **Start printing after last page is spooled**.
5. Click the **Configuration** tab, and then clear **Update Configuration from Printer**.
6. Click **Set Printer Model**, and then select **Universal Color Laser**.

   Note: If only monochrome printers are available in the fleet, then select **Universal Mono Laser**.

7. From the Configuration Options list, select the options that are available in the fleet.
8. Select **Apply** > **OK**.

Configuring the print options

Note: The following instructions are commonly used for optimum cost savings.

1. Depending on whether the Print Server Role has been added to your server, perform the following steps:

   ### If Printer Server Role is added

   a. From the Windows Administrative Tools window, launch **Print Management**, locate the local Print Server, and expand it.
   b. Select **Printers** and right-click on the **Print Release** printer object.
   c. Click the **Advanced** tab, and then click **Printing Defaults**.

   ### If Printer Server Role is not added

   a. From the Control Panel window, launch **Devices and Printers**.
   b. Right-click the printer icon, and then click **Printer Properties**.
   c. Click the **Advanced** tab, and then click **Printing Defaults**.

2. Click the **Layout** tab.
3. From the Print on Both Sides (Duplex) menu, select **Print on both sides**, and then select **Long edge**.

   Note: Users can override this setting when printing jobs.

4. Click the **Paper/Finishing** tab.
5. From the Offset menu, select **Off**.
6. Click the **Quality** tab.
7. Select **Print in black and white**.

   Note: Users can override this setting when printing jobs.

8. Click the **Other Options** tab.

9 When using only a PostScript emulation print driver, select **Generate PostScript in driver**.

10 When using computers running on a Windows 8 or Windows 8.1 operating system, from the Metafile spooling menu, select **On**.

11 Select **Apply** > **OK**.

Adding LDD Client Service

These instructions are applicable only if the print spooler is configured as a clustered resource.

1 From your computer, navigate to the Windows Administrative Tools window, and then open the Windows Failover Cluster Management console.

2 Right-click the print spooler cluster group, and then click **Add a resource** > **Generic Service**.

3 Select **LDD Client Service**, and then click **Next**.

4 Click **Next** > **Finish**.

5 From the Windows Failover Cluster Management console home screen, right-click **LDD Client Service**, and then click **Properties**.

6 Click the **Dependencies** tab, and then select the print spooler resource.

7 Click **Apply** > **OK**.

8 Right-click **LDD Client Service**, and then click **Bring this resource online**.

Configuring the Print Release solution in Lexmark Management Console

Configuring the application settings

1 From Lexmark Management Console, click the **Solutions** tab.

2 From the Solutions section, select **PrintReleasev2**.

3 From the Tasks section, select **Configuration**, and then change the settings.

4 Click **Apply**.

After configuring the application settings, configure the deployment settings for the application. For more information, see “Solutions setting index” on page 171.

Understanding print job queue filtering based on job site name

Print jobs that are shown in the Print Release application are filtered based on their site name. There are two settings under the PrintReleasev2 solution that can be configured:

- **Site to Exclude in Print Queue**
  - Print jobs with a site name that matches the value specified in this setting are not shown in the Print Release application.
  - An empty or blank value means that no print jobs are excluded.

  - When automatic or quick print release is enabled, excluded jobs are not released.
- **Site to Include in Print Queue**
  - Print jobs with a site name that matches the value specified in this setting are not shown in the Print Release application.
  - An empty or blank value means that all jobs are shown.
  - When automatic or quick print release is enabled, only included jobs are released.
  - When a site name value to include is also specified to be excluded under Site to Exclude in Print Queue, the latter prevails. Thus, print jobs with the specified site name are not be shown.

Notes:

- The input fields accept comma-separated values that are used to filter the jobs to show in the Print Release application based on the site name.
- These features are available in both global and local PrintReleasev2 solution configuration.
- Local configuration supersedes global configuration. The local values of these settings are checked first over the global ones.
- Other areas that can show the job list are not affected by these settings, such as LPM administrator and user portals, and mobile applications.
- When an identical site name is specified in print queues both for sites to exclude and include, jobs with that name are excluded in the queue. The Site to Exclude in Print Queue setting takes precedence.

Configuring printer security

For printers with restricted access to various features or functions such as Remote Management and Firmware Update, configure Authentication Type from Lexmark Management Console. The setting must match the Security Template or Login Method settings that are configured on your printers. This configuration lets the server authenticate printers during printer discovery and policy update. By default, Lexmark Management Console uses the global Device Security setting in the Services tab > DeviceSecurity task. This setting is initially configured with a value of None.

Note: LDD version 5.3 supports the User name + Password authentication type. Make sure that the printer security settings match the authentication type and credentials that are configured in Lexmark Management Console.

Configuring the global Device Security settings

If all printers in your environment are secured with a common Security Template or Login Method, then do the following:

1. From Lexmark Management Console, click the **Services** tab.
2. From the Services section, select **DeviceSecurity**.
3. From the Tasks section, select **Parameters**.
4. Select the authentication type for the printer.
5. Type the appropriate authentication value.

   Note: If LDAP or LDAP+GSSAPI is used, then make sure that the LDAP setup name is configured when using an e-Task 5 printer.
6. Click **Apply**.

Configuring the Device Security settings at the Device Group level

If some printers in your environment are secured with a different Security Template or Login Method, then you may organize your printers into separate device groups. The groups must share a common Security Template or Login Method. Do the following:

1. From Lexmark Management Console, click the **Device Groups** tab.
2. From the Device Groups section, select the appropriate device group.
3. From the Tasks section, select **Security**, and then clear **Use Global**.
4. Select the authentication type for the printer.
5. Type the appropriate authentication value.

   Note: If LDAP or LDAP+GSSAPI is used, then make sure that the LDAP setup name is configured when using an e-Task 5 printer.
6. Click **Apply**.

Adding printers to a device group

Before adding devices to the solution, make sure that you have obtained licenses from your Lexmark Technical Program Manager.

Add devices to the existing device group to have the same local settings as all other devices in the group. Creating groups also lets you organize all your devices, such as by location, and modify different configurations in the local settings, such as Site or Touchscreen - Print All.

1. From Lexmark Management Console, click the **Device Groups** tab.
2. From the Device Groups section, click **+**, and then type a unique name.

   Note: To use the existing group, select the name of your device.
3. From the Tasks section, select **Discovery Profiles**.
4. In the Address field, type the IP address of the printer, and then click **Add**.

   Note: Do not fill up any information in the fields unless that information is already configured on the added printers.
5. Click **Discover**.
6. From the Discovery section, select **Discover new devices only**, and then click **Discover**.
7. Click **Done**.

Note: To verify that your printer is successfully added, click **Summary** or **Discovered Devices** from the Tasks section.

Customizing the home screen for a device group

1. From Lexmark Management Console, click the **Device Groups** tab.
2. From the Device Groups section, select **Print Release**.
3. From the Tasks section, select **Home Screen**.
4. Click the tab for each device class that you want to customize.

5 Select **Use this home screen as part of the device groups policy**.

6 Configure the settings.

- For touch-screen printers, do the following:
  a In the Layout menu, select the number of buttons to include.
  b If necessary, select a page, and then select a button.
  c In the Action menu, select an action for the button.

  Notes:

  - Make sure that an action is selected for all the buttons that you want to appear on the home screen.
  - If you have customized the home screen in your previous sessions, then reset the actions of the buttons on all pages before applying the new settings. Standard functions such as copy, fax, and e-mail do not automatically appear on the home screen. For these functions to appear on the home screen, assign an action.

Function	Available selections[1]
Execute a standard MFP function.	– Address Book – Bookmarks – Change Language – Copy – Copy Shortcuts – Email – Email Shortcuts – Fax – Fax Shortcuts – FTP – FTP Shortcuts – Held Faxes – Held Jobs – Jobs by User – Job Queue – Lock Device – Printer Panel – Release Held Faxes – Scan Profiles – Search Held Jobs – Settings – Shortcuts – Status or Supplies – USB Drive
Show a list of profiles.	– App Profiles – Profiles
Execute a specific profile.	Single Profile
Override a standard function with a profile.[2]	– Copy + Profile – Email + Profile – Fax + Profile – FTP + Profile
Execute a printer shortcut.	– Shortcut

[1] Some selections may not be available in some models.

[2] A standard function overrides itself when configured with a profile. For example, Copy + Profile performs the same function as Copy.

[3] Lexmark Management Console cannot access eSF application icons directly. To provide locations for eSF application icons in the default order, use placeholders. To designate a location for the icon of an eSF application identified by name and set the profile name of the application, use App Reservation. For example, the profile name for the Scan to Network application is **`scnToNet`**. If a placeholder or the App Reservation setting is not specified, then installed eSF applications appear on the first page after the pages defined in the custom home screen.

Function	Available selections[1]
Provide a placeholder for an eSF application icon.[3]	– App Reservation – Placeholder
Leave a blank space.	None

[1] Some selections may not be available in some models.

[2] A standard function overrides itself when configured with a profile. For example, Copy + Profile performs the same function as Copy.

[3] Lexmark Management Console cannot access eSF application icons directly. To provide locations for eSF application icons in the default order, use placeholders. To designate a location for the icon of an eSF application identified by name and set the profile name of the application, use App Reservation. For example, the profile name for the Scan to Network application is **`scnToNet`**. If a placeholder or the App Reservation setting is not specified, then installed eSF applications appear on the first page after the pages defined in the custom home screen.

d If necessary, specify the details of the action. Do any of the following:

– To track copy jobs, select the icon that you added for Copy, and then in the Action menu, select **Copy + Profile**. In the Profiles menu, select **CopyTrack**.

Notes:

- If you are using Device Usage to track copy jobs, then see "Configuring Device Usage" on page 192. This setting does not override the copy configuration and only sets the Copy icon to use the Copy function. We recommend using Device Usage if you are not using quotas or do not want to use any of the Advanced Copy features of Print Release.
- When tracking jobs with quotas, use CopyTrack. Select the icon that you added for Copy, and then in the Action menu, select **Copy + Profile**. In the Profiles menu, select **CopyTrack**. To track canceled copy jobs, Device Usage must also be installed with Copy Track Cancel enabled. For more information, see "Configuring Device Usage" on page 192.
- To track copy jobs without quotas, do not override the copy configuration. Set the Copy icon to use the Copy function.

– The printer can automatically populate the authenticated user's e-mail address in the From and To fields of the e-mail. Select an icon for Email, and then in the Action menu, select **Email + Profile**. In the Profiles menu, select **EmailTrack**.

Note: The EmailTrack profile also tracks the e-mail transaction, so if you select it, make sure that you clear **Track Email** within the Device Usage configuration.

– If you want to track outgoing fax jobs, select an icon for Fax, and then in the Action menu, select **Fax + Profile**. In the Profiles menu, select **FaxTrackAnalog** or **FaxServerTrack**.

e Select the remaining button.

f In the Action menu, select **Single Profile**.

g In the Profiles menu, select **Print Release**.

Note: To use the Scan to Network application, select **Scan to Network** as the profile.

- For non-touch-screen printers, do the following:

a In the Layout menu, select **Custom**.

b Following the list of buttons, click **Add**.

Notes:

– The only action available is Single Profile. You cannot modify other menu items on a printer without a touch screen.

- To remove a button, select it in the list, and then click **Remove**.

c If necessary, type a custom text.

d Select a profile to associate with the button.

7 Configure the remaining buttons on the home screen.

8 Click **Apply**.

Note: Make sure to click **Apply** on each tab to apply the settings.

Single Sign-On for AD FS and PKCE

Active Directory Federation Services (AD FS) is a software component that provides single sign-on (SSO) authorization services to users. This feature lets users access multiple applications on the server by authenticating only in one of the applications.

For example, a user who is logged in to Lexmark Management Console (LMC) can already access Lexmark Print Management Console.

Proof Key for Code Exchange (PKCE) is a lightweight mechanism implemented in the application that requests an authorization code. LPM and LDD support it as a simple extension to the Authorization 2.0 authorization code grant. With the integration of the third-party open source application Keycloak, PKCE allows users to authenticate once and access multiple applications without reentering their credentials.

Notes:

- ADFS Servers 2019 and 2022 are supported in LPM or LDD application.
- If the AD FS SSO login type is enabled, then users are redirected to the AD FS logout screen after logging out. To log in again, users must go to the Print Management Console URL.

Configuring the AD FS server

For LMC, when creating a client-server application, select **web browser accessing a web application** as the application type.

Make sure to add the following:

- **Redirect URI**—**`https://<load-balancer-hostname-or-ipaddress>/lmc/login/oauth2/code/adfs`**
- **Logout URI**—**`https:/</load-balancer-hostname-or-ipaddress>/lmc/lmc-logout.do`**

For LPM, when creating a client-server application, select **Native application** or **Native application accessing a web API** as the application type.

Make sure to add the following:

- **Redirect URI**—**`https://<load-balancer-hostname-or-ipaddress>/printrelease/callback.html`**
- **Logout URI**—**`https:/</load-balancer-hostname-or-ipaddress>//printrelease/logout.html`**

Updating Apache configuration

1 Open Windows Explorer.

2 Navigate to **`<LDD-install-path>/Apache2/conf`**.

3 Edit **httpd-lpm-csp.conf**.

4 From the Location /printrelease/ block, append the following before the closing double quotes (replace the value of **<adfs-server-address>**):

```
frame-ancestors 'self' https://<adfs-server-address>/;
```

5 Add the following at the end of the file (replace the value of **<adfs-server-address>**):

```
<Location ~ "^/lmc/(.*)">
Header set Content-Security-Policy "frame-ancestors 'self' https://<adfs-server-address>/;"
</Location>
```

6 Save the file.

7 Restart the Apache2.4 service.

Configuring AD FS login

1 On the upper-right corner of Print Management Console, click .

2 Click **Login**.

3 From the Type menu, select **AD FS SSO**.

4 In the Login Group text field, type the name of the Active Directory or LDAP group that is provided with administrator access or privilege to Print Management Console.

Note: If the user logging in is a member of the Login Group, then the user must have administrator access. Otherwise, the user is redirected to the user portal.

5 Click **Save Changes.**

Note: If the AD FS SSO login type is enabled, then users are redirected to the AD FS logout screen after logging out. To log in again, users must go to the Print Management Console URL.

Configuring Print Management Console settings

1 Click on the upper-right corner of Print Management Console.

2 Configure the AD FS and LDAP server settings:

For AD FS settings:

a Type the address of the AD FS server.

b Import the SSL certificate for LPM to communicate to the AD FS server.

c Type the client ID.

d Type the client secret.

Note: This field is not required.

e Type the scope of the client.

Note: The default value is openid.

f Click **Save Changes**.

For LDAP settings:

a Click **Add**.

Note: If there is no existing LDAP entry which is the Active Directory pointed to by the AD FS, then configure the server details.

b Configure the server details.

Note: In the LDAP settings, add the Active Directory pointed to by the AD FS.

c Click **Save Changes**.

Configuring mobile devices

Lexmark Print adds user functionality to an existing LPM system:

- **Lexmark Print application support**
  - View, print, or delete documents and print jobs in a user's print queue.
  - View quota in a user's queue.
  - Allow delegate printing from a user's print queue.
  - Send documents to LPM for conversion and future printing.
- **E-mail document submissions**—Lets users send an e-mail to an account that the Lexmark Email Watcher monitors. When an e-mail is received, it is sent to LPM, and then converted to a printable document based on predefined conversion settings and user-specified settings. The job can be printed immediately on the specified printer, or it can be integrated with LPM and then printed later.
- **AirPrint document submissions**—Lets users of Apple devices running the iOS 6.1 or later or OS X 10.7 or later operating system software send documents to LPM. Users can send documents wirelessly to LPM, and then print the jobs later. In Print Management Console, AirPrint jobs are listed under the Site column as IPP Print.

Mobile Single Sign-On

Mobile Single Sign-On or Mobile SSO is a feature that allows the use of the organization's authentication token to access the LPM system. This feature reduces the number of times that a user has to log in when printing. This feature is supported only in the Android Print Plug-in application.

Configuring SSO with the mobile plug-in

Apply the following configuration in the plug-in application:

```
<?xml version="1.0" encoding="UTF-8"?>

<config>

  <providers>
    <provider>
      <name>Prem Mobile SSO</name>
      <address>10.100.101.11></address>
      <providerType>server-premise</providerType>
      <auto-discover>true</auto-discover>
    </provider>
  </providers>

  <premise-server-config>
    <sso-url>orcton.eastasia.cloudapp.abc.com</sso-url>
    <sso-client-id>clientid</sso-client-id>
  </premise-server-config>
```

```
   <behavior
    <import-configList>reset_all/<import-configList>
  </behavior>

</config>
```

Note: <address>—Type the server IP address of the load balancer.

As an administrator, introduce the following settings in Lexmark Print configuration file to hide the Logout option:

```
  <settings>
    ...
    <hide-logout>true</hide-logout>
  </settings>
```

Notes:

- Set the value to **true** to hide Logout option.
- This setting is not dependent on AD FS settings.
- By default, the Logout option is shown.
- The plug-in application imports the new configuration settings.

AD FS Management Console

Notes:

- While creating a client-server application, select **Server application** or **Server application accessing a web API**.
- In the Redirect URL field, type **lxkmobile://plugin.callback**.

Print Management Console Settings

1. Click on the upper-right corner of Print Management Console.
2. Configure the ADFS and LDAP server settings:

   For ADFS Settings:

   a. Type the server address of the ADFS server.
   b. Import the SSL certificate for LPM to communicate to the ADFS server.
   c. Click **Save Changes**.

   For LDAP Settings:

   a. Click **Add**.

      Note: If the AD FS points to an existing Active Directory as the LDAP entry, then there is no need to follow the next steps.

   b. Configure the server details.

      Note: In the LDAP settings, add the Active Directory that the AD FS points to.

   c. Click **Save Changes**.

Understanding the system requirements

Supported e-mail protocols

If the e-mail submission functionality is used, then the e-mail server that hosts the account for LPM monitoring must support one of the following protocols:

- IMAP4
- POP3
- Exchange Web Services (EWS)

Supported printers for mobile device usage

Network printers that support PostScript emulation are supported as an output device. However, for the best and fastest output, we recommend any Lexmark printer that supports the PDF format.

Advanced finishing options such as staple and hole punch work only on Lexmark printers. Options for two-sided (duplex) printing may not work on non-Lexmark printers because of vendor-specific implementation.

Supported file formats

The following file formats are supported for document conversion:

Note: You can print the documents later.

For Lexmark Print application	For e-mail submission
Adobe PDF (*.pdf)[1]	Adobe PDF (*.pdf)[1]
ASCII Text (*.txt)	ASCII Text (*.txt)
GIF (*.gif)	CSV Files (*.csv)
HTML (*.htm, *.html)	GIF (*.gif)
JPEG (*.jpg, *.jpeg)	HTML (*.htm, *.html)
Microsoft Excel 97-2003, 2007, 2010, 2013, 2016 (*.xls, *.xlsx)[2]	JPEG (*.jpg, *.jpeg)
Microsoft PowerPoint 97-2003, 2007, 2010, 2013, 2016 (*.ppt, *.pptx)[2]	Microsoft Excel 97-2003, 2007, 2010, 2013, 2016 (*.xls, *.xlsx)[2]
Microsoft Word 97-2003, 2007, 2010, 2013, 2016 (*.doc, *.docx)[2]	Microsoft PowerPoint 97-2003, 2007, 2010, 2013, 2016 (*.ppt, *.pptx)[2]
OpenDocument Spreadsheet (*.ods)[2]	Microsoft Word 97-2003, 2007, 2010, 2013, 2016 (*.doc, *.docx)[2]
OpenDocument Presentation (*.odp)[2]	OpenDocument Spreadsheet (*.ods)[2]
OpenDocument Text/Writer (*.odt)[2]	OpenDocument Presentation (*.odp)[2]

[1] Documents are not converted.

[2] Documents with SmartArt, external images, or content references may not convert or may partially convert.

For Lexmark Print application	For e-mail submission
TIFF (*.tif, *.tiff)[1]	OpenDocument Text/Writer (*.odt)[2]
	PNG (*.png)
	Rich Text Format (*.rtf)
	TIFF (*.tif, *.tiff)[1]

[1] Documents are not converted.

[2] Documents with SmartArt, external images, or content references may not convert or may partially convert.

Configuring Lexmark Print

Document conversion software dependencies

Document conversion is required for submission of e-mail and mobile application jobs. During installation, LPM detects the version of the installed document conversion software.

Note: Only the application servers require a document conversion software.

Before running the LPM installer, make sure that a supported document conversion application is installed on each Tomcat or application server that handles document conversions. We recommend installing the document conversion application before running the LPM installer for the solution to use it automatically.

Supported document conversion software and versions

Application	Supported versions
Microsoft Office	• 2016 • 2013 • 2010 • 2007
Apache OpenOffice	• 4.1 • 4.0 • 3.4
LibreOffice	• 6.4.6 • 4.0 • 3.4

Note: OpenOffice or LibreOffice is required for e-mail or mobile application submissions. To improve the print fidelity of Microsoft Office document formats, use Microsoft Office.

Configuring the Lexmark Print application settings

1. From Lexmark Management Console, click the **Solutions** tab.
2. From the Solutions section, select **mobileprint**.
3. From the Tasks section, select **Configuration**, and then configure the settings.
4. Click **Apply**.

Understanding the mobile and e-mail configuration data

Note: The LDAP and Print Release settings are used only when one of the Print Release integration methods is selected. Otherwise, leave the fields blank.

Setting name	Setting for	Possible values	Notes
Allowed Sender Domains	E-mail	N/A	To process only e-mails that are sent from specific domains, use a comma-separated list. Any e-mail sent from a domain that is not included in the list is discarded. If none is specified, then all e-mails are processed.
Confirmation Email Disclaimer	E-mail	**Note:** Do NOT reply to this e-mail. Please contact the Help Desk for further assistance.*	This setting is added to the end of confirmation e-mails.
Confirmation Email Domains	E-mail	N/A	To send confirmation e-mails only to users in specific domains, use a comma-separated list.
Confirmation Email From Address	E-mail	*name@company.com*	The e-mail address that appears in confirmation e-mails.
Confirmation Email Subject	E-mail	Lexmark Print Confirmation*	The subject used in confirmation e-mails.
Confirmation Error Email	E-mail	• Disabled* • To All Users • To Users in Specified Domains	Determines whether a confirmation e-mail is sent to users when an error is encountered and the job cannot be processed. If **Disabled** is selected, then an e-mail is not sent. If **To All Users** is selected, then the confirmation e-mail is sent to all users. If **To Users in Specified Domains** is selected, then the confirmation e-mail is sent only to users specified in the Confirmation Email Domains field.
Confirmation Print Release Name	E-mail	Lexmark Print Release*	The name of the Print Release system where the confirmation e-mail is released.
Confirmation Success Email	E-mail	• Disabled* • To All Users • To Users in Specified Domains OpenOffice	Determines whether a confirmation e-mail is sent to users when the job is successfully sent to the printer. If **Disabled** is selected, then an e-mail is not sent. If **To All Users** is selected, then the confirmation e-mail is sent to all users. If **To Users in Specified Domains** is selected, then the confirmation e-mail is sent only to users specified in the Confirmation Email Domains field.

* Indicates the default value.

Setting name	Setting for	Possible values	Notes
Conversion Method	Lexmark Print and E-mail	• MS Office and • OpenOffice Only* **Note:** We recommend using only Microsoft Office. It is not necessary to install OpenOffice. For information on the supported file types, see "Supported file formats" on page 62.	Specifies the method used to convert attachments. If **OpenOffice Only** is selected, then all file types are converted using OpenOffice or LibreOffice. If **MS Office and OpenOffice** is selected, then Microsoft Office is used to convert Microsoft Office file types, and then OpenOffice or LibreOffice is used to convert all other file types. **Note:** To improve the print fidelity of Microsoft Office document formats, we recommend selecting **MS Office and OpenOffice**.
Conversion Format	Lexmark Print and E-mail	• PDF • PostScript	Specifies the format used for document conversions.
Device ID	E-mail	• First Word of Subject* • Last Word of Subject • First Word of Message Body	Determines the location of the printer nickname or IP address in the subject of the e-mail sent by the user. Print options can only be used when the device ID is the first word of the subject or message body.
Direct IP Printer Type	E-mail	• PostScript • TIFF*	When using Direct IP Printing, select the format that all printers using your solution support.
Device To Printer IP Lookup	E-mail	• Lexmark Database* • Direct IP Printing	When using printer nicknames, select **Lexmark Database**. If only the IP address or host name of the printer is used, then select **Direct IP Printing**.
LDAP Follow Referrals	E-mail	• Yes* • No	Specifies whether referrals to other LDAP servers are processed. If **No** is selected, then only responses from the specified LDAP server are used.
LDAP Login Password	E-mail	N/A	The password used for accessing the LDAP server.
LDAP Login Username	E-mail	N/A	The account name used for accessing the LDAP server.
LDAP Mail Attribute	E-mail	mail*	The LDAP attribute that corresponds to the user's e-mail address.
LDAP Port	E-mail	N/A	The port number used for communicating with the LDAP server. The most common port number used is 389.
LDAP Search Base	E-mail	N/A	The search base used for looking up e-mail accounts. The value for this setting must be able to look up all possible user accounts.
LDAP Server	E-mail	N/A	The IP address or host name of the LDAP server used for looking up e-mail addresses and user IDs.
LDAP User Object	E-mail	User*	The objectclass attribute in LDAP used by user accounts.
* Indicates the default value.			

Setting name	Setting for	Possible values	Notes
LDAP Userid Attribute	E-mail	• Samaccountname* • uid	The LDAP attribute that corresponds to the user's Windows user ID.
Log Information	Lexmark Print and E-mail	• Disabled* • Enabled	Shows the detailed logs in the Log page of Lexmark Management Console.
Mode	E-mail	• Standard* • Print Release (Internal Users Only) • Print Release (Guest Support) • Print Release (Guest Support 2)	If **Standard Mode** is selected, then specify the printer in the Device ID field. Configure the LDAP and Print Release settings for all Print Release options. If **Print Release (Internal Users Only)** is selected, then all users in LDAP can print. If **Print Release (Guest Support)** is selected and the user is not in LDAP, then the solution functions as Standard Mode for that e-mail. If **Print Release (Guest Support 2)** is selected, then the device ID is checked whether it corresponds to a printer nickname. If it does, then the print job is sent directly to that printer. If not, then this setting functions the same as the Print Release (Internal Users Only) mode. **Note:** To use Print Release (Guest Support 2), make sure that Device to Printer IP Lookup is set to **Lexmark Database**.
Print Attachments	E-mail	• Always (User cannot change) • Yes (User can change)* • No (User can change) • Never (User cannot change)	Determines the default operation when printing all attachments in an e-mail. If **Yes (User can change)** or **No (User can change)** is selected, then users can modify this setting when sending an e-mail.
Print Body	E-mail	• Always (User cannot change) • Yes (User can change)* • No (User can change) • Never (User cannot change)	Determines the default operation when printing the message body in an e-mail. If **Yes (User can change)** or **No (User can change)** is selected, then users can modify this setting when sending an e-mail. **Note:** When releasing jobs that are submitted using e-mail from mobile devices, select **No (User can change)** or **Never (User cannot change)** to print the first attachment. Otherwise, only the message body in an e-mail is printed and not the attachment.
Print File Operations	Lexmark Print and E-mail	• Use Standard Method* • Use Alternate Method	Specifies the alternative way for saving files when the standard method conflicts with your environment. If **Use Standard Method** is selected, then the alternative method is FileClass (jcifs). If **Use Alternate Method** is selected, then the alternative method is TISFile.
* Indicates the default value.			

Setting name	Setting for	Possible values	Notes
Print in Duplex	E-mail	• Always (User cannot change) • Yes (User can change)* • No (User can change) • Never (User cannot change)	For duplex-capable printers, this setting determines whether all e-mails (message body and attachments) are printed in duplex. If **Yes (User can change)** or **No (User can change)** is selected, then users can modify this setting when sending an e-mail.
Print Max Copies	E-mail	1*	By default, one copy of the message body and attachment is printed. This setting is the maximum number of copies that can be printed from one e-mail. Users can specify the number of copies when sending the e-mail.
Print Release Directory	Lexmark Print and E-mail	C:\lexmark\printrelease*	The file share information used in the Lexmark Print Management solution. If installing all LPM components on a workgroup environment that uses a local file system to hold documents, then leave the Print Release login fields blank. If installing on an enterprise environment using a common file share, then enter the credentials of an administrator or user who has write access to the file share. **Note:** This setting must have the same value as the Print Release Solution setting. If the directory is on a file share, then type a UNC path. For example, ***\\ServerName\ShareName]***. **Note:** If the server is not a member of a domain, then the host name of the server with the file share on its local file system must be used as the domain name.
Print Release Password	Lexmark Print and E-mail	N/A	The password used for saving files to the Print Release directory. **Note:** This setting must have the same value as the Print Release Solution setting.
Print Release Username	Lexmark Print and E-mail	N/A	The user name used for saving files to the Print Release directory. **Note:** This setting must have the same value as the Print Release Solution setting.
Release Jobs Directly	Lexmark Print and E-mail	N/A	Release jobs directly to the printer from the server. Otherwise, jobs are downloaded to and released from the mobile device. **Note:** Disabling the Release Jobs Directly setting results in slower performance when releasing jobs using a mobile device.
Use SSL for LDAP	E-mail	• Yes • No*	Specifies whether the solution uses SSL when querying LDAP. Specify the port number used for SSL communication. The most common port number used is 636.
* Indicates the default value.			

Limiting the maximum file size for each job submission

By default, the maximum file size for each job submission is 1GB. To change the default maximum file size, do the following:

1. From your computer, navigate to ***<Install-Dir>*\Solutions\apps\lpm\WEB-INF\classes**.
2. Using a text editor, open the **application.yml** file.
3. Set the **`maxFileSize`** and **`maxRequestSize`**.
4. Restart the Lexmark Solutions Application Server (LSAS) service.

Adding Lexmark Print to a software client group

Note: Make sure that you have a software client license.

1. From Lexmark Management Console, click the **Software Client Groups** tab.
2. From the Software Client Groups section, select **Mobile Print**.
3. From the Tasks section, select **Client Profiles**.
4. In the Address field, type the IP address (for example, **`10.10.2.100`**) or subnet (for example, **`10.10.*.*`**) of the mobile device or e-mail watcher server.

   Notes:

   - You can also import a CSV file of IP addresses or subnets.
   - Use the asterisk wildcard character (**`*`**) at the end of the IP address to search for all devices in that subnet. For example, type **`10.10.*.*`** to accept incoming requests from devices within the range 10.10.0.1–10.10.255.255.
5. Click **Add** > **Save**.

Configuring document conversion software

To enable document conversion, perform the following instructions on each of the LPM Tomcat and application servers that are expected to handle document conversions. For information on the supported document types, see “Supported file formats” on page 62.

We recommend installing the document conversion software before installing Lexmark Print.

Installing .NET framework

To enable interaction between LPM and Microsoft Office document conversion applications when using Lexmark Print version 3.0 or later, install .NET Framework 4.

Document conversion requires .NET Framework 4 to work properly. If .NET Framework 3.5 SP1 is already installed on the machine, then WIC is not necessary for installing .NET Framework 4.

Installing OpenOffice or LibreOffice

Note: You must install the same document conversion software on each Tomcat and application server. Do not use a different document conversion software on different servers.

1. Download, and then run the setup wizard for OpenOffice or LibreOffice.
2. During installation, select **Install this Application for Anyone who uses this computer**.
3. Do either of the following:
   - For typical installation, make sure that the default installation path is accepted, and then install all the applications.
   - For custom installation, make sure that all main office applications are installed. The optional components can be installed at your discretion.

If OpenOffice or LibreOffice is installed after installing Lexmark Print, then after performing the previous instructions, do the following:

1. Stop the Lexmark Solutions Application Server service.
2. Navigate to the **%SOLUTIONS_INSTALL_DIR%\apps\wf-ldss\WEB-INF\classes** folder.
3. Using a text editor, open the **OpenOfficeToPDFClass.properties** file.
4. Set **`officeToPDF.defaultOfficeHomeDirectory`** to the location where OpenOffice or LibreOffice is installed.

   Note: For a typical LibreOffice 4 installation, the path is usually **C:\Program Files (x86)\LibreOffice 4**. Make sure that there is no trailing slash. Also, all backslashes in the path must be replaced with forward slashes.
5. Save the file.
6. Start the Lexmark Solutions Application Server service.
7. From the Lexmark Print application, update the conversion method setting to use the appropriate document converter.

Installing Microsoft Office

Note: Install the same document conversion software on each Tomcat and application server. Do not use a different document conversion software on different servers.

1. Download, and then run the setup wizard for Microsoft Office.
2. During installation, select **Install this Application for Anyone who uses this computer**.
3. Do either of the following:
   - For typical installation, make sure that the default installation path is accepted, and then install all the applications.
   - For custom installation, make sure that all main office applications are installed. The optional components can be installed at your discretion.
4. Do either of the following:
   - For 64-bit operating systems, navigate to **C:\Windows\SysWOW64\config\systemprofile** <folder>.
   - For 32-bit operating systems, navigate to **C:\WINDOWS\system32\config\systemprofile**< folder>.
5. Create a directory or a folder inside the "systemprofile" path with the name **`Desktop`**.

6 If you are using Microsoft Office 2007, then install the Microsoft Save as PDF or XPS add-in.

7 If you want to convert Microsoft Excel documents (.xls and .xlsx), do the following:

   a Navigate to the **%SOLUTIONS_INSTALL_DIR%\lpm\msoffice** folder.

   b Run the **createLsasUser.bat** file as an administrator.

   c Type your username and password.

   Note: This step creates a user account with administrative privileges.

   d Log in to the created account, open the Microsoft Office components, and then complete the setup process.

   Note: This step creates the necessary folders for the user profile.

   e Change the Lexmark Solution Application Server service to run as this user, and then restart the service.

If Microsoft Office is installed after installing Lexmark Print, then after performing the previous instructions, do the following:

1 Stop the Lexmark Solutions Application Server service.

2 Navigate to the **%SOLUTIONS_INSTALL_DIR%\apps\wf-ldss\WEB-INF\classes** folder.

3 Using a text editor, open the **MsOfficeDocConvClass.properties** file.

4 Set **`officeConv.execName`** to use one of the following executable files:

   - For Microsoft Office 2013, specify **`MsOffice2013DocConverter.exe`**.
   - For Microsoft Office 2010, specify **`MsOffice2010DocConverter.exe`**.
   - For Microsoft Office 2007, specify **`MsOffice2007DocConverter.exe`**.

5 Save the file.

6 Start the Lexmark Solutions Application Server service.

7 From the Lexmark Print application, update the conversion method setting to use the appropriate document converter.

Adding Lexmark Print Management to Lexmark Print

Note: Before you begin, make sure that you have added Lexmark Print as a software client in Lexmark Management Console. For more information, see “Adding Lexmark Print to a software client group” on page 68.

1 From your mobile device, open Lexmark Print.

2 From the application home screen, tap **Find Device**.

3 Tap **Network Address**, and then in the Address field, type ***`IPaddress`*`/mobile`**, where ***`IPaddress`*** is the IP address of the load balancer.

   Note: If your environment has a hardware or software load balancer in front of several subsystems, then type the hardware or software load balancer address.

4 Depending on your configuration, log in using your LDAP or Active Directory credentials. For more information, see “Understanding the mobile and e-mail configuration data” on page 64.

Configuring Lexmark Email Watcher

We recommend installing the document conversion software before installing Lexmark Print.

When you install Lexmark Print Management, selecting the e-mail component also installs Lexmark Email Watcher on the load balancer.

Lexmark Email Watcher is a Windows service that can be seen in the Windows Services control panel applet. Lexmark Email Watcher is not started during the Lexmark Print Management load balancer installation because the service must be configured before it is started. When a configuration change is made to this service, restart it for the update to take effect. Also, to enable the service to start after reboots, set its startup type to **Automatic**.

Understanding the Lexmark Email Watcher configuration data

Lexmark Email Watcher is installed in the base Lexmark Solutions folder that is selected when installing the load balancer. By default, the location is **%ProgramFiles%\Lexmark\Solutions\EmailWatcher**. The configuration file is **config_EmailWatcher.properties** and is located in the **conf** subfolder. A file that contains sample properties is installed. Some of the properties are commented out, and some are not in the file yet. Add the necessary properties for your email server.

Notes:

- Lexmark Email Watcher must be restarted if any changes are made to the configuration file. The changes do not take effect until the service is restarted.
- When troubleshooting, the log files are located in the **.\EmailWatcher\logs** folder. If the configuration file enables debugging, then the emailwatcher.log file contains extra logging. To enable more logging, open the **.\EmailWatcher\conf\l4j_EmailWatcher.xml** file. From the bottom of the file, change the level value for **`com.lexmark.tis.tools.emailwatcher`** and **`javax.mail`** to **`debug`**. Make sure that the properties are changed to **`info`** after the issue is resolved.
- To change the username or password, using a text editor, edit the property file, and then replace the encrypted entries with the new credentials. Restart Lexmark Email Watcher to read and re-encrypt the password.

Setting	Valid values	Notes
`ldd.server`	**`http://`*`IPaddress`*`:9780`** Where ***`IPaddress`*** is the IP address or host name of the load balancer.	A sample URL is **`http://my-lpm-server:9780`**.
`ldd.profile`	**`mobileprint`**	The name of the profile when the job is submitted to LPM. Do not change this setting.
`mail.type`	• **`imap`** • **`pop3`** • **`ews`**	The type of email server on which the email account is located. We recommend using IMAP.
`mail.server`	N/A	For IMAP or POP3, this setting is the IP address or host name of the mail server.

Setting	Valid values	Notes
mail.port	• **143** (IMAP) • **993** (IMAP over SSL) • **110** (POP3) • **995** (POP3 over SSL)	For IMAP or POP3, the common ports are listed. If necessary, use another value.
mail.tls	• **0** (no TLS) • **1** (use TLS)	For IMAP or POP3, this setting determines whether TLS must be used when communicating with the mail server. Only TLS or SSL can be used, not both. If TLS is enabled, then the SSL setting is ignored.
mail.ssl	• **0** (no TLS) • **1** (use TLS)	For IMAP or POP3, this setting determines whether SSL must be used when communicating with the mail server. Only TLS or SSL can be used, not both. If TLS is enabled, then the SSL setting is ignored.
mail.folder	**INBOX**	For IMAP or POP3, this setting specifies the folder where new mail appears. We recommend not changing this setting.
mail.allowNTLM	• **0** (Do not allow) • **1** (Allow)	For IMAP or POP3, this setting determines whether the user can authenticate using NTLM. We recommend not changing this setting.
mail.domain	N/A	For IMAP or POP3, this setting is the domain of the user account.
mail.user	N/A	For IMAP or POP3, this setting is the username of the monitored account.
mail.pw	N/A	For IMAP or POP3, this setting is the password of the monitored account.
mail.allowIdle	• **0** (Do not allow) • **1** (Allow)	If the mail server supports automatic notification of new emails, then this setting specifies whether to enable automatic notification. If disabled, then set the poll value of the **mail.poll** setting. **Note:** Typically, only IMAP servers support automatic notification of new emails.
mail.poll	**60**	The time in seconds before new email is checked. The default is 60 seconds. **Note:** If your server supports automatic notification on new emails, then polling is not necessary.
Debug	• **0** (Off) • **1** (On)	Determines whether extra logging must be written to the log file. We recommend enabling this setting only when troubleshooting an issue because the amount of data being logged can slow down the processing.

Sample Lexmark Email Watcher config_emailwatcher.properties configurations

For IMAP

```
# Mandatory Properties
ldd.server=http://[ldd-lb-addr]:9780
ldd.profile=mobileprint
```

```
mail.server=imap.gmail.com
mail.user=test@company.com
mail.pw=notTheRealPassword

# Optional Properties.
mail.type=imap
mail.ssl=1
mail.tls=0
mail.port=993
mail.folder=INBOX
mail.allowIdle=1

debug=1
```

For Microsoft Exchange

```
# Mandatory Properties
ldd.server=http://[ldd-lb-addr]:9780
ldd.profile=mobileprint
mail.server=ews.mail.com
mail.domain=test_domain
mail.user=test_ews@company.com
mail.pw=notTheRealPassword

# Optional Properties.
mail.type=ews
mail.ssl=1
mail.folder=INBOX
mail.ignoreSSLCert=1

debug=1
```

Sample `config_emailwatcher.properties` file for Microsoft Exchange Online modern authentication in `<LDD-install-path>\EmailWatcher\conf`

Modern authentication authenticates the user through a single browser-based application, tenant ID, user ID, and the required details. The following is a sample batch file for Microsoft Exchange Online modern authentication.

```
# GENERAL CONFIGURATION
ldd.server=http://<Put LDD Server/LB IP>:9780

# STANDARD PRINT CONFIGURATION.
# This is the existing email watcher feature and is enabled by default.
# Do not use the same email account with guest print.
# Do not change the value of "ldd.profile".debug=1
#
standard.print.enable=1
ldd.profile=mobileprint

### Required only if not using Exchange Online.
### "mail.user" and "mail.pw" values will be replaced with encrypted text
### when EmailWatcher service is started. To change either of the values,
### simply replace the encrypted value with the new value. Please make sure
### that the values do not start with "ENC(" and end with ")".
mail.user=
mail.pw=

# GUEST PRINT CONFIGURATION
# Using the email service account specified below, EmailWatcher can monitor
# incoming print jobs from guest users. This feature is disabled by default.
# To enable, set "guest.print.enable" to 1.
#
# Do not use the same email account with standard print.
# Do not change the value of "ldd.profile.guest".
#
guest.print.enable=1
ldd.profile.guest=guestrelease
```

```
### Required only if not using Exchange Online.
### Specify the values for "mail.user.guest" and "mail.pwd.guest". Values will
### be replaced with encrypted text when EmailWatcher service is started.
### Make sure that the values do not start with "ENC(" and end with ")".
mail.user.guest=
mail.pw.guest=

# MAIL SERVER CONFIGURATION
# Uncomment then provide values for the applicable properties.
# If not applicable, keep it being commented out.
#
### Specify mail server address for IMAP, POP3, Exchange Premise mail types
### For Exchange Online, value is not required.
mail.server=

mail.type=ews
#mail.domain=<mail domain>
#mail.ssl=< 0 or 1>
#mail.port=<mail server port>
mail.folder=INBOX
#mail.ignoreSSLCert=< 0 or 1 >
mail.poll=60
#mail.allowIdle=1  #If  Mail Server supports IMAP IDLE
mail.hideUserAndJobInfo=1

# ADDITIONAL SERVER CONFIGURATION FOR MS EXCHANGE
# Uncomment then provide values for the applicable properties.
# If not applicable, keep it being commented out.

### Authentication types:
###   basic     - For username/password authentication
###   oauth2    - Modern authentication (OAuth 2.0)
ews.auth.type=oauth2

### Authorization flows:
###   auth-code-with-client-id-secret     - OAuth 2.0 authorization code grant type, or auth
code flow
ews.auth.grantType=auth-code-with-client-id-secret

### The generated application (client) ID of your registered
### app in Azure Active Directory.
ews.aad.clientId=076c7620-10e8-4418-9592-1f7a1a80868b

### The generated application (client) secret of your registered
### app in Azure Active Directory.
ews.aad.clientSecret=KeX8Q~Xd~wo.49fFqE_a6S.lMn~Pu6tQHhmE-a2c

### Identity platform endpoint to acquire security tokens
### For <tenant>, valid values are common, organizations, consumers, and tenant identifiers.
ews.aad.authority=https://login.microsoftonline.com/12709065-6e6c-41c9-9e4d-fb0a436969ce

### The redirect URI of your app, where authentication responses
### can be sent and received by your app. It must exactly match one
### of the redirect URIs you registered in the portal.
### You must specify a port in the URI. For example: https://localhost:5000/
ews.aad.redirectUri=http://localhost:9991/

### A space-separated list of scopes that you want the user to consent to.
### This value allows your app to get consent for multiple web APIs you want to call.
ews.aad.scopes=openid offline_access https://graph.microsoft.com/Mail.ReadWrite

### Indicates the type of user interaction that is required
### when authenticating the user.
### Valid values: login, consent, select_account
ews.aad.prompt=select_account

### The timeout (milliseconds) to wait for the user to input and validate their
### credentials for authentication.
ews.socket.timeout=300000

### Messages that will be printed in the oauth2 login tab of browser after acquiring the
auth code.
ews.afterLoginMessage.standard=Authorization code for Email Watcher Standard Print service
```

```
account has been successfully acquired. You can now close this tab.
ews.afterLoginMessage.guest=Authorization code for Email Watcher Guest Print service account
has been successfully acquired. You can now close this tab.

### The delay (milliseconds) between authentication prompts
### when both standard and guest print features are enabled.
ews.auth.prompt.delay=5000
```

Modern authentication support for Lexmark Email Watcher

Modern authentication support for Lexmark Email Watcher

This feature authenticates the user through a single browser-based application, tenant ID, user ID, Azure ID, password, and other details. This feature applies only to Microsoft Exchange Online.

Understanding the authentication support requirements

Before you begin, make sure that modern authentication for LPM server is configured as follows:

Requirement	Execution
An account with permissions to register new client application in Azure Active Directory (AD).	1 Navigate to Microsoft Azure Portal. **Note:** The current URL of the Microsoft Azure Portal is **`https://portal.azure.com/#home`**. 2 Click **Azure Active Directory** > **App registrations**.
Registered client application in Azure Active Directory.	Go to **https://learn.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app**. Before you begin, make sure that you know how to configure a client application and API permissions. For more information, see “Configuring client application and API permissions ” on page 76. Configure the following: • **Client secret** **Note:** Take note of the value while adding the client secret, as it will be masked after saving it. • **Redirect URI** **Note:** Specify the port details. For instance, the port number can be 9100. Take note of the following: • Application (client) ID • Directory (tenant) ID
Set API permissions for the registered client application.	For more information on setting API permissions, go to **https://learn.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app** and refer to the Setting API Permissions for Registered Client Application section.
Service accounts in Microsoft Exchange with mailbox enabled.	Separate accounts for standard and guest print. Email Watcher watches or reads the inbox of this account.
Configured MobilePrint solution.	Same configuration with previous Email Watcher versions.

Requirement	Execution
Office converter software already installed.	Can be Microsoft Office, OpenOffice, or LibreOffice.
From Lexmark Management Console, click **Services** > **Mail configured to point to Exchange Online server**.	Make sure that SMTP configuration is selected.

Configuring client application and API permissions

1. Navigate to Microsoft Azure Portal.

   Note: The current URL of Microsoft Azure Portal is **https://portal.azure.com /#home**.

2. Click **Azure Active Directory** > **App registrations**.

   Note: If you want to register a new client, then click **New registration**.

3. Select the registered client application.

4. To add or generate a client secret for the application, do the following:
   a. Click **Client credentials** > **New client secret**.
   b. Type the description, and then specify the expiry date.
   c. Click **Add**.

      Note: Take note of the actual value of client secret as it will be masked after saving it.

5. To add Redirect URIs, do the following:
   a. Select **Redirect URIs**.
   b. Click **Add a platform** > **Web**.
   c. Enter a valid URI for the application.

      Note: The port details must be specified.
   d. Click **Configure**.

Setting API permissions for registered client applications

1. Navigate to Microsoft Azure Portal.

   Note: The current URL of Microsoft Azure Portal is **https://portal.azure.com /#home**.

2. Click **Azure Active Directory** > **App registrations**.

3. Select the registered client application.

4. In the left pane, select **API permissions** > **Add a permission**.

5. In the Microsoft APIs section, select **Microsoft Graph** > **Delegated permissions**.

6. In the Opened permissions section, select the following:
   - **email**
   - **offline_access**
   - **openid**

7. In the Mail section, select **Mail.ReadWrite**.

8. Select **Add permissions**.

Configuring modern authentication for LPM server

1. Configure the properties file of the application.

   Note: For more information on authentication settings and values, see "Lexmark Modern Authentication for LPM server" on page 77.

2. Run the command prompt as an administrator.

   Note: For more information on parameters, see "Parameters" on page 78.

3. From the User Account Control window, click **Yes**.

4. Navigate to the Email Watcher root directory: **<C:\Program Files\Lexmark\Solutions\EmailWatcher\conf_>**.

5. At the command prompt, type **EmailWatcher.bat**.

   Note: If the standard print feature is enabled, then the default browser is launched. If the default browser is already open, then a new tab is launched.

6. Type the user ID and password.

   Note: The credentials must be the same as that of the Microsoft Exchange Online mail user.

7. Click **Sign in**.

   Notes:

   - If the guest print feature is enabled, then the browser prompts you to enter the credentials of the service account for guest print.
   - After successful authentication, the application continues running in the background.

Lexmark Modern Authentication for LPM server

Setting	Valid values
General	ldd.server=http://<LDD LB Server IP>:<port> **Note:** Replace the text in brackets with the actual value.
Standard Print	• standard.print.enable=<0 or 1>, where 0 is disable and 1 is enable. • ldd.profile=mobileprint **Note:** Username and password are not required in modern authentication.
Guest Print	• guest.print.enable=<0 or 1>,where 0 is disable and 1 is enable. • ldd.profile.guest=guestrelease **Note:** Username and password are not required in modern authentication.
Mail Server	• mail.type=ews • mail.folder=INBOX • mail.poll=<frequency to query mailbox for mails, default 60> • mail.hideUserAndJobInfo=<0 or 1> **Note:** Set to 1 to hide user info, or 0 to show information in logs.

Setting	Valid values
Exchange Online	• ews.auth.type=oauth2 • ews.auth.grantType=auth-code-with-client-id-secret • ews.aad.clientId=<client ID of registered application in Azure AD> • ews.aad.clientSecret=<client secret of registered application in Azure AD> • ews.aad.authority=https://login.microsoftonline.com/<tenant> • ews.aad.redirectUri=<redirect URI configured for the registered application in Azure AD. You must specify a port. Example: http://locahost:5000/> • ews.aad.scopes=openid offline_access https://graph.microsoft.com/Mail.ReadWrite • ews.aad.prompt=login, consent, or select_account **Notes:** – Set to login to prompt the user to enter a username and password. – Set to consent to prompt the user to grant permission after login. – Set to select_account to allow choosing cached user accounts in the default browser. Default: select_account. • ews.socket.timeout=<time (in milliseconds) to wait for the user to input and validate their credentials for authentication. Default: 300000> • ews.afterLoginMessage.standard=<message to display after log in of service account for standard print functionality> • ews.afterLoginMessage.guest=<message to display after log in of service account for guest print functionality> • ews.auth.prompt.delay=<delay (in milliseconds) between authentication prompts when both standard and guest print features are enabled>

Parameters

Parameter	Email Watcher service	Behavior
<no parm>	Stopped	Prompts the user to log in, and then starts the service.
start	Stopped	Prompts the user to log in, and then starts the service.
stop	Stopped	Shows message that service is already stopped.
restart	Stopped	Shows message that service is already stopped. The user must log in and start the service.
<no parm>	Running	Shows message that service is already running. The options available are either to start or stop the service.
<no param> then 1. STOP is selected in #5	Running	Stops the service
<no param> then 2. RESTART is selected in #5	Running	Stops the service. The user must log in and start the service again.

Parameter	Email Watcher service	Behavior
start	Running	Shows message that service is already running.
stop	Running	Stops the service.
restart	Running	Stops the service. The user must log in and start the service again.

Sample `config_emailwatcher.properties` file for Microsoft Exchange Online modern authentication in `<LDD-install-path>\EmailWatcher\conf>`

```
#------------------------------------------------------------------------------
# GENERAL CONFIGURATION
#------------------------------------------------------------------------------
ldd.server=http://<LB Server/LB IP>:9780

#------------------------------------------------------------------------------
# STANDARD PRINT CONFIGURATION
# This is the existing email watcher feature and is enabled by default.
# Do not use the same email account with guest print.
# Do not change the value of "ldd.profile"
#------------------------------------------------------------------------------

standard.print.enable=1
ldd.profile=mobileprint

### Required only if not using Exchange Online.
### "mail.user" and "mail.pw" values will be replaced with encrypted text
### when EmailWatcher service is started. To change either of the values,
### simply replace the encrypted value with the new value. Please make sure
### that the values do not start with "ENC(" end with ")".
mail.user=
mail.pw=

#------------------------------------------------------------------------------
# GUEST PRINT CONFIGURATION
# Using the email service account specified below, EmailWatcher can monitor
# incoming print jobs from guest users. This feature is disabled by default.
# To enable, set "guest.print.enable" to 1.
#
# Do not use the same email account with standard print.
# Do not change the value of "ldd.profile.guest".
#------------------------------------------------------------------------------
guest.print.enable=1
ldd.profile.guest=guestrelease

### Required only if not using Exchange Online.
### Specify the values for # "mail.user.guest" and "mail.pwd.guest". Values will
### be replaced with encrypted text when EmailWatcher service is started.
### Make sure that the values do not start with "ENC(" and end with ")".
mail.user.guest=
mail.pw.guest=

#------------------------------------------------------------------------------
# MAIL SERVER CONFIGURATION
# Uncomment then provide values for the applicable properties.
# If not applicable, keep it being commented out.
#------------------------------------------------------------------------------
### Specify mail server address for IMAP, POP3, Exchange Premise mail types
### For Exchange Online, value is not required.
mail.server=
mail.type=ews
#mail.domain=<mail domain>
#mail.ssl=< 0 or 1 >
#mail.port=<mail server port>
mail.folder=INBOX
#mail.ignoreSSLCert=< 0 or 1 >
mail.poll=60
```

```
#mail.allowIdle=1  #If  Mail Server supports IMAP IDLE
mail.hideUserAndJobInfo=1
#--------------------------------------------------------------------------
# ADDITIONAL SERVER CONFIGURATION FOR MS EXCHANGE
# Uncomment then provide values for the applicable properties.
# If not applicable, keep it being commented out.
#--------------------------------------------------------------------------
### Authentication types:
###   basic     - For username/password authentication
###   oauth2    - Modern authentication (OAuth 2.0)
ews.auth.type=oauth2

### Authorization flows:
###   auth-code-with-client-id-secret     - OAuth 2.0 authorization code grant type, or auth
code flow
ews.auth.grantType=auth-code-with-client-id-secret

### The generated application (client) ID of your registered
### app in Azure Active Directory.
ews.aad.clientId=076c7620-10e8-4418-9592-1f7a1a80868b

### The generated application (client) secret of your registered
### app in Azure Active Directory.
ews.aad.clientSecret=KeX8Q~Xd~wo.49fFqE_a6S.lMn~Pu6tQHhmE-a2c

### Identity platform endpoint to acquire security tokens
### ### For tenant, valid values are common, organizations, consumers, and tenant
identifiers.
ews.aad.authority=https://login.microsoftonline.com/12709065-6e6c-41c9-9e4d-fb0a436969ce

### The redirect URI of your app, where authentication responses
### can be sent and received by your app. It must exactly match one
### of the redirect URIs you registered in the portal.
### You must specify a port in the URI. For example: https://localhost:5000/
ews.aad.redirectUri=http://localhost:9991/

### A space-separated list of scopes that you want the user to consent to.
### This value allows your app to get consent for multiple web APIs you want to call.
ews.aad.scopes=openid offline_access https://graph.microsoft.com/Mail.ReadWrite

### Indicates the type of user interaction that is required
### when authenticating the user.
### Valid values: login, consent, select_account
ews.aad.prompt=select_account

### The timeout (milliseconds) to wait for the user to input and validate their
### credentials for authentication.
ews.socket.timeout=300000

### Messages that will be printed in the oauth2 login tab of browser after acquiring the
auth code.
ews.afterLoginMessage.standard=Authorization code for Email Watcher Standard Print service
account has been successfully acquired. You can now close this tab.
ews.afterLoginMessage.guest=Authorization code for Email Watcher Guest Print service account
has been successfully acquired. You can now close this tab.

### The delay (milliseconds) between authentication prompts
### when both standard and guest print features are enabled.
ews.auth.prompt.delay=5000
```

Understanding e-mail print options

When you submit an e-mail, several options are available that can be sent with the printer address or nickname that manages the output. To use the print options, make sure that Device ID is set to **First Word of Subject**. For more information, see “Understanding the mobile and e-mail configuration data” on page 64.

The options are specified after the device ID.

Option	Value	Notes
Copies	**/c#**	The **#** symbol indicates the number of copies. If a value greater than the Print Max Copies solution setting is entered, then the maximum value is used.
Duplex	**/d**	This setting prints the document in duplex. **Note:** This option may not work on some non-Lexmark printers.
Hole Punch	**/h**	If the printer has a hole punch finisher, then this setting uses the hole punch feature. **Note:** This option does not work on non-Lexmark printers.
No Attachments	**/na**	Only the message body is printed and the attachments are ignored. This setting has no effect when the Print Attachments solution setting is set to **Always**.
No Body	**/nb**	Only the attachments are printed and the message body is ignored. This setting has no effect when the Print Body solution setting is set to **Always**.
No Duplex	**/nd**	The document is printed one-sided. This setting has no effect when the Print Duplex solution setting is set to **Always**.
Print Attachments	**/pa**	This setting lets you print attachments in the e-mail. This setting has no effect when the Print Attachments solution setting is set to **Never**.
Print Body	**/pb**	This setting lets you print the message body in the e-mail. This setting has no effect if the Print Body solution setting is set to **Never**.
Staple	**/s**	If the printer has a staple finisher, then this setting uses the staple feature. **Note:** This option does not work on non-Lexmark printers.
Mono	**/m**	The document is printed in monochrome.

See the following examples:

Subject	Result
printerid /c2 /d	Prints two duplexed copies
printerid /nb	Prints only the attachment
printerid /d /s	Staples and duplexes the message body and each attachment
printerid /na	Prints only the message body

Configuring printer nicknames

Printer nicknames map a user-friendly nickname and the IP address of a printer. When configured, printer nicknames let users use the nickname instead of the IP address when submitting jobs.

Note: Make sure that Printer Nicknames is enabled in Print Management Console. For more information, see "Show more features" on page 96.

1. Open a web browser, and then type **http://*IPaddress*:9780/printrelease/**, where ***IPaddress*** is the IP address of the load balancer.
2. Log in as an administrator.

   Notes:

   - The default user name and password is **admin**.
   - The default credentials are the same as those in Lexmark Management Console (LMC).

- If the Print Management Console is configured to connect to an LDAP server, then use your LDAP user name and password.

3 Depending on your configuration, from the Print Management Console, do either of the following:
- Click **Printer Nicknames**.
- Click **Device Functions** > **Printer Nicknames**.

4 Manage the printers.
- Filter the list by typing the keywords in the Filter field, and then clicking .

  Note: Do not use special characters or symbols.
- Refresh the list by clicking .
- Add, edit, or delete printers.

Configuring the server for AirPrint

When installing Lexmark Print Management, select the AirPrint component to enable the AirPrint feature.

Accessing AirPrint configuration

1 Open a web browser, and then type **`http://IPaddress:0001/#/settings/configAccess`**, where ***`IPaddress`*** is the IP address of the load balancer.

2 From the side navigation, click the **AirPrint** group.

Understanding AirPrint discovery

To perform AirPrint advertisement and service discovery for Lexmark Print Management, do either of the following:

Unicast

- Configure a Microsoft DNS server. For more information, see “Configuring DNS servers for AirPrint advertisement” on page 124.
- Configure BIND for Windows DNS Server. For more information, see “Configuring BIND for AirPrint advertisement” on page 133.

Multicast

1 Access the AirPrint configuration page. For more information, see “Accessing AirPrint configuration” on page 82.

2 From the General tab, select **Enable Bonjour discovery**.

Configuring Guest Print

Guest Print is a feature in LPM Premise that lets guests print documents without accessing or setting up an account in an organization’s network.

Notes:

- The guests must have an e-mail client to be able to print by simply sending the document to a prespecified e-mail address.
- An administrator or an organization's representative provides the e-mail address that the guest can send their documents to.

Unsupported devices for Guest Print

The following printers do not support Guest Print:

- MX421
- MX421ade
- MX521
- MX521ade
- MX521adte
- MX521de

Configuring the Email Watcher configuration file

The **config_EmailWatcher.properties** file must be configured for the Guest Print feature. For more information, see "Understanding the Lexmark Email Watcher configuration data" on page 71.

Notes:

- Using the e-mail service account, the Email Watcher can monitor incoming e-mails from guest users. By default, this feature is disabled.
- To enable, set **`guest.print.enable`** to **`1`**.
- Specify the values for **`mail.user.guest`** and **`mail.pwd.guest`**.
- Do not use the same e-mail account with standard printing.
- Do not change the value of **`ldd.profile.guest`**.

Configuring Lexmark Print Management Console for Guest Print

mobileprint solutions level

1. From Lexmark Management Console, click the **Solutions** > **mobileprint**.
2. In the Tasks section, click **Configuration** > **Confirmation Success Email** > **To All Users**.
3. In the Tasks section, click **Configuration** > **Confirmation Error Email** > **To All Users**.
4. In the Confirmation Email From Address field, type the e-mail address.
5. In the Confirmation Email Subject field, type the subject of the e-mail.
6. In the LDAP Server field, enter the server address.

   Note: This step is optional. The LDAP Server is required to prevent employees from sending a print job or an e-mail as guest.

7 In the Delete Guest PINs After Specified Hours field, specify how long you want the PIN to be valid.

Note: You must configure PIN deletion so that you can delete guest PINs at required intervals. For more information, see "Configuring PIN deletion" on page 85.

8 In the Select the Guest PIN length field, enter the value.

Note: The value ranges from 4 to 8. The default value is 6.

9 In the Number of Pages Allowed for Guest field, enter the maximum number of pages that you allow the guest to print.

Notes:

- If the total number of pages of the print job exceeds the value set in the Number of Pages Allowed for Guest field, then the user receives an e-mail indicating the error. This feature is available only if the Lexmark Email Watcher is enabled. For more information, see "Understanding the Lexmark Email Watcher configuration data" on page 71.
- You can only submit a maximum of 1,000 pages at a time.

10 In the Tasks section, click **Configuration** > **Guest Print Confirmation Email Language** > **<preferred language>**.

11 Click **Apply**.

PrintReleasev2 solutions level

1 From Lexmark Management Console, click the **Solutions** > **PrintReleasev2**.

2 In the Tasks section, click **Configuration** > **User Authentication** > **Custom**.

3 Click **Apply**.

Device Groups level

1 From Lexmark Management Console, click the **Device Groups** > **Print Release**.

2 In the Tasks section, click **eSF Configuration**.

3 In the eSF Applications: (Solution) section, click **guestlaunch(PrintReleasev2)**.

a Clear **Verify eSF application deployment and deploy these eSF settings**, and select **Deploy to**.

b Click **Save Settings**.

4 In the eSF Applications: (Solution) section, click **cardAuth(PrintReleasev2)**.

a Configure Custom Profile:

- In the Name or ID field, type **guestlaunch**.
- In the Icon Text field, type **Guest Print**.

Note: For more information on setting up CardAuth, see "Configuring BadgeAuth and CardAuth" on page 180.

b Click **Save Settings**.

5 In the eSF Applications: (Solution) section, click **badgeAuth(PrintReleasev2)**.

a Configure Custom Profile:

- In the Name or ID field, type **guestlaunch**.
- In the Icon Text field, type **Guest Print**.

Note: For more information on setting up BadgeAuth, see "Understanding the BadgeAuth version 2 configuration data for e-Task 4 and e-Task 3 printers" on page 186.

b Click **Save Settings**.

Services level

1 From Lexmark Management Console, click **Services** > **Email**.

2 Configure the e-mail parameters.

3 Click **Apply**.

Configuring PIN deletion

Configure PIN deletion at the System level.

1 From Lexmark Management Console, click **System** > **Schedule** > **Add**.

2 From the Choose task menu, select **Script**.

3 In the Choose a group type menu, select **None**, and click **Next**.

4 For solutions and scripts, do the following:

a In the Solutions menu, select **mobileprint**.

Note: In the Script menu, **DeleteGuestPinsTask** is automatically selected.

b Click **Next**.

c Configure the frequency of the task, and then click **Finish**.

Note: We recommend setting the frequency of DeleteGuestPinsTask to 1 hour.

Testing the solution

After changing the configuration or adding devices to the device group, configure a client workstation to make sure that print queueing is working properly.

1 Open the printer wizard.

In Windows 10 operating system

a From the control panel, navigate to the Devices and Printers window.

b Click **Add a printer**.

In Windows 8 operating system

From the Search charm, navigate to:

Apps list > **Run** > type **`control printers`** > **OK** > **Add devices and printers**

In Windows 7 and Vista operating system

a Click  > **Run**.

b In the Start Search dialog box, type **`control printers`**.

c Click **Add a printer** > **Add a network, wireless or Bluetooth printer**.

2. Select the option that lets you connect to your network printer, and then type the destination folder where your printer is located.
3. Set the printer as default, and then select the option that lets you print a page, if prompted.
4. From the printer home screen, touch **Print Release**.
5. Select the print job that contains the test page, and then touch **Print Selected**.

Deploying Lexmark Print Management

The eSF applications, card reader drivers, and UCF files required to use LPM are provided with the solution. Lexmark Management Console lets you configure and deploy the applications to the printers.

The required files can be found in the following folders:

- **Advancedprompt**—*<install-Dir>*\Lexmark\Solutions\apps\wf-ldss\firmware
- **eSF applications and drivers**—*<install-Dir>*\Lexmark\Solutions\apps\wf-ldss\solutions\PrintReleasev2-*release version*\firmware
- **UCF files**—*<install-Dir>*\Lexmark\Solutions\Apache2\htdocs\apachewebdav\ucf\PrintReleasev2

Where *<install-Dir>* is the installation folder of LDD.

Supported components

Note: For more information on e-Task printers, see “Supported printer models” on page 24.

Component		Description	Compatible eSF framework	Purpose
eSF applications	Badge Authentication (badgeauth)	Locks out the printer until a user authenticates with a badge or PIN	• e-Task 4 • e-Task 3	Used for badge or card authentication **Note:** After upgrading to LPM 2.5.2 or later, manually configure each Badge Authentication application to deploy to the target printer family.
	Card Authentication (cardAuth)	Locks out the printer until a user authenticates with a badge or PIN	e-Task 5	Used for badge or card authentication
	Device Usage (deviceusage)	Provides all usage data on the printer	• e-Task 5 • e-Task 4 • e-Task 3	Used when Device Usage tracking is enabled **Note:** After upgrading to LPM 2.5.2 or later, manually configure each Device Usage application to deploy to the target printer family.
	Guestlaunch	Provides authentication for the Guest Print feature	• e-Task 5 • e-Task 4 • e-Task 3	Used for PIN authentication when for Guest Print
	PrintCryption (printcryption2)	Enables secure printing of encrypted jobs sent from the user's workstation	• e-Task 5 • e-Task 4 • e-Task 3	Used to decrypt the encrypted print jobs
LDD application	advancedprompt	Provides basic prompts for the user at the printer control panel	• e-Task 5 • e-Task 4 • e-Task 3	Used for prompts
Card reader drivers	keyboardreader	The driver for the RFID card reader	• e-Task 5 • e-Task 4 • e-Task 3	Used for RFID card readers
	omnikey5427ckdriver	The driver for the Omnikey card reader	• e-Task 5 • e-Task 4	Used for Omnikey card readers
	omnikeydriver	The driver for the Omnikey card reader	e-Task 3	Used for Omnikey card readers
For more information on the eSF application versions, see *Release Notes*.				

Managing eSF configurations

1. From Lexmark Management Console, click the **Device Groups** tab.
2. From the Device Groups section, click **Print Release**.
3. From the Tasks section, click **eSF Configuration**.
4. Do any of the following:

Change the deployment order

From the eSF Applications: (Solution) section, select an application, and then click the up or down arrow button.

We recommend the following order of deployment:

- deviceusage
- Card reader drivers: keyboardreader, omnikey5427ckdriver, ominikeydriver
- advancedprompt
- IdleScreen
- badgeauth or cardAuth
- mobileAuth

Notes:

- IdleScreen is available only in LPM On-Premises version 2.5 or earlier.
- mobileAuth is available only in LPM On-Premises version 2.6 or earlier.
- By default, the compatible eSF level and the recommended deployment order are installed.

Exclude an eSF application from a policy update

a. From the eSF Applications: (Solution) section, select an application.
b. From the Settings section, in the Deploy to list, clear the settings.

Note: When Card Authentication for e-Task5 is excluded from application deployment or policy update, exclude the corresponding security setup files (CardAuth_e5.ucf) as well. For more information on how to exclude UCF file, see “Managing UCF settings” on page 90.

Configure the eSF application settings

a. From the eSF Applications: (Solution) section, select an application.
b. From the Settings section, configure the eSF application settings.

Note: To select an e-Task printer, make sure that **Deploy to** is selected.

5. Click **Save Settings**.

Note: To deploy multiple applications, make sure that you save the settings after configuring each application.

6. From the Tasks section, click **Policy Update** > **Update Policy**.

Note: The deployment can take from one to two minutes. For more information on how to improve the policy update performance, see “Improving device discovery and policy update speed” on page 92.

7. Click **Done**.

Understanding UCF files

You can deploy the following UCF files to the printers using Lexmark Management Console:

- **BadgeAuth2**—Similar to BadgeAuth except that it is compatible with e-Task 3 and e-Task 4 devices.
- **CardAuth_e5**—Secures access to e-Task 5 devices using a card reader. For LPM version 2.6, CardAuth_e5.ucf must be updated after installation.

  The following settings must be removed from the configuration file:

  ```
  <name>esf.IdleScreen.ChgBkgnd</name>
  <name>esf.IdleScreen.Idle</name>
  <name>esf.IdleScreen.showroomFAC</name>
  ```

  The following setting must be added:

  ```
  <name>use profiles</name>
  ```

- **MobileAuth_e5**—Secures access to e-Task 5 devices using a mobile device.

  Note: MobileAuth_e5 is available only in LPM On-Premises version 2.6 or earlier.

Managing UCF settings

Solutions level

The settings at the Solutions level serve as global values. During deployment, the system uses the global values unless local values defined at the Device Groups level are specified.

1. From Lexmark Management Console, click the **Solutions** tab.
2. From the Solutions section, click **PrintReleasev2**.
3. From the Tasks section, click **Security Setup Files**.
4. Exclude a UCF file from a policy update. In the Deploy to menu, clear the check boxes.
5. Click **Apply**.

Device Groups level

The settings at the Device Groups level serve as local values.

1. From Lexmark Management Console, click the **Device Groups** tab.
2. From the Device Groups section, click **Print Release**.
3. From the Tasks section, click **Security Setup Files**.
4. Exclude a UCF file from a policy update. In the Deploy to menu, clear the check boxes.
5. To let the policy update use the UCF settings at the Device Groups level, clear **Use Solution Configuration**.
6. Click **Apply**.

Note: If all devices will be configured with the same Security Setup File configuration, then we recommend managing the Security Setup Files on the Solutions tab.

Configuring UCF settings

1. From Lexmark Management Console, click the **Device Groups** tab.
2. From the Device Groups section, click **Print Release**.
3. From the Tasks section, click **Security Setup Files**.
4. Select a UCF file, and then configure the settings.

   ### BadgeAuth2.ucf

   Set the values for your environment, such as Active Directory.

   Set the values for the LDAP server settings: **`searchBase`**, **`serverAddress`**, and **`useridAttribute`**

   If your environment does not allow anonymous binding, then sent **`anonBind`** to **0**. Set the values for **`mfpDN`** and **`mfpPassword`**.

   The other settings can remain in their default values.

   ### CardAuth_e5.ucf

   Set the values for your environment, such as Active Directory.

   If your environment allows anonymous binding, then set the values for **`address`**, **`search_base`**, and **`userid_attr`**.

   If your environment does not allow anonymous binding, then set **`anon_bind`** to **0**. Set the values for **`machine_dn`** and **`machine_password`**.

   The other settings can remain in their default values.

5. Click **Apply**.

Managing Lexmark Print Management

Improving device discovery and policy update speed

When using three or more servers, the speed of device discovery and policy updates may slow down. Do the following to improve their speed:

1. From Lexmark Management Console, click the **Services** tab.
2. From the Services section, select **General**.
3. From the Tasks section, select **Parameters**.
4. In the ChunkSize field, enter a new value.

   Note: When using three or more servers, a value as low as 2 may be appropriate.
5. Click **Apply**.

Scheduling cleanup tasks

Lexmark Print Management can establish total or color user quotas on a monthly or yearly basis. It can also limit function access by user or group and manage temporary badges. Schedule tasks to run for each feature to update and clean up data periodically.

If you are using quotas, then reset the quotas to delete the data from the previous year automatically and let users start with refreshed quotas. Schedule this task to run once a year on a schedule that works best for your business processes. For example, many schools run this task at the beginning of each school year.

If you are using function access, then update the group information periodically to provide access to the functions granted to their user role. Set the frequency that this task runs by how frequently users move around within groups in your environment.

For temporary badges, make sure to reset the user information associated with the badges. When the badge is assigned to a new user, the new user must re-register and cannot gain access to the previous user's jobs. Set the frequency that this task runs by how long you assign temporary badges.

1. From Lexmark Management Console, click the **System** tab.
2. From the System section, select **Schedule**.
3. Click **Add** > **Script** > **Next** > **None** > **Next**.
4. Select a solution and the script associated with your task.
   - **ResetFAUserGroup**—The function access limit of the group is reset.
   - **PrintDelete**—The print jobs are deleted automatically after a time.

     Note: By default, the **PrintDelete** task is scheduled.
   - **DeleteOrphanFiles**—The print jobs that were not deleted on the file storage but were deleted on the database are deleted from the file storage.
   - **GenerateCSV**—The report is generated after a time.
   - **TempBadgeDelete**—The temporary badge data is deleted.
   - **ResetQuota**—The user quotas is reset annually.
   - **ResetUserGroup**—The users that are already defined in the database to their current group are updated.

5 Click **Next**.

6 From the “Choose the frequency” dialog box, specify the start date and time, and how often the cleanup occurs.

7 Click **Finish**.

Setting up multiple domain support in Lexmark Management Console

Multiple domain support lets the device accept multiple domain configurations, so that different users under different domains can use the device.

Note: The following instructions are apply only if your environment has multiple domains.

1 Enable multiple domain support in Lexmark Management Console.
   a From Lexmark Management Console, click the **Solutions** tab.
   b From the Solutions section, click **PrintReleasev2**.
   c From the Tasks section, click **Configuration**.
   d From the Configuration (PrintReleasev2) section, in the LDAP Multi-Domain Support menu, select **Enabled**.
   e Click **Apply**.

   Note: If Lexmark Print is installed, then also enable LDAP Multi-Domain Support for **mobileprint**.

2 Configure the following files:
   - idm-production-config.properties
   - ldap.properties

   Note: For default installation, you can find these files at ***<Install-Dir>*\Lexmark\Solutions\apps\idm\WEB-INF\classes** and ***<Install-Dir>*\Lexmark\Solutions\apps\printrelease\WEB-INF\classes**, respectively.

3 Restart Lexmark Solution Application Server in Windows Services.

Setting up multiple domain support for BadgeAuth or CardAuth

Multiple domain support lets the device accept multiple domain configurations, so that different users under different domains can use the device.

Note: Multiple domains are supported only when Card Auth is configured for web services through the LPM server. It is not supported when Card Auth is configured for LDAP.

The following instructions are optional and applicable only if your environment has multiple domains.

1 From Lexmark Management Console, click the **Device Groups** tab.

2 From the Device Groups section, select **Print Release**.

3 From the Tasks section, select **eSF Configuration**.

4 From the eSF Applications: (Solutions) section, select either of the following:

- **cardAuth(PrintReleasev2)**—Select this application to configure cardAuth(PrintReleasev2).
- **badgeauth(PrintReleasev2)**—Select this application to configure badgeauth(PrintReleasev2).

  Note: Make sure that you select the second **badgeauth(PrintReleasev2)** from the eSF Applications: (Solutions) section to deploy the application to e-Task2+, e-Task3, and e-Task4.

Note: Any application configuration changes require Policy Update. For more information on Policy Update, see "Managing eSF configurations" on page 89.

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

Note: By default, Use Selected Realm is not selected.

Notes:

- For more information on Use Selected Realm for cardAuth(PrintReleasev2), see **Advanced Settings** section in "Understanding the CardAuth version 5 configuration data for e-Task 5 printers" on page 180.
- For more information on Use Selected Realm for badgeauth(PrintReleasev2), see **Advanced Settings** section in "Understanding the BadgeAuth version 2 configuration data for e-Task 4 and e-Task 3 printers" on page 186.

Configuring Print Management Console

You need administrative rights to use the Print Management Console administrator portal.

Accessing Print Management Console

1 Open a web browser, and then type either of the following URLs:

- **http://*hostname*:9780/printrelease/**
- **https://*hostname*/printrelease/**

Where ***hostname*** is the host name or IP address of the Print Management server.

2 From the Domain menu, select **No Domain**.

3 Log in as an administrator.

Note: If the Print Management Console is configured to connect to an LDAP server, then use your LDAP user name and password.

Configuring Print Management Console

1 Click  on the upper-right corner of Print Management Console.

2 Do any of the following:

Restrict access to the configuration settings

a Click **Configuration Access**.

b In the Authentication menu, select one of the following:

- **None**—After users log in to Print Management Console, no further authentication is required.
- **Password**—Requires users to authenticate before accessing the System Configuration page. For more information on password management, see "Password Management" on page 98.
- **LDAP Group**—Restricts access to the System Configuration page to specific users in an LDAP group.

  Notes:

  - The LDAP group is case sensitive and must match the LDAP directory.
  - Make sure that the Print Management Console login is **LDAP Login**. For more information, see "Set the Print Management Console login" on page 95.

c Click **Save Changes**.

Set the Print Management Console login

Note: This feature authenticates administrators when logging in to Print Management Console.

a Click **Login**.

b In the Type menu, do either of the following:

- To use Lexmark Management Console authentication, select **LMC Login**.
- To use LDAP authentication, select **LDAP Login**, and then configure the settings.

  Notes:

  - Use a different LDAP server or a different search base for administrators.
  - To configure LDAP for users, see "Manage LDAP settings" on page 97.

c Click **Save Changes**.

Set the Disclaimer page

The Disclaimer page informs users about certain privacy policies or important messages.

Note: By default, the Disclaimer page option is disabled.

a Click **Disclaimer**.

b Select **Show a disclaimer dialog before login**.

c In the Title field, type the title of the disclaimer.

Note: The Title field is optional.

d In the Text field, type the disclaimer message.

e Click **Save Changes**.

Note: Click **Reset** to revert to the previous state.

Show more features

By default, the only visible features on the pages are Dashboard, Print Queue, Delegates, and Badges.

a Click **Feature Options** > **Settings**.

b Select the features to show.

Note: For more information on each feature, see "Using the Print Management Console features" on page 99.

c Click **Save Changes**.

Configure the user portal

a Click **Feature Options** > **User Portal Dashboard**.

Note: Data displayed in the chart or card is sample or for representation purpose only.

b Do any of the following:

- Add, edit, or delete cards.
- Organize cards.
- Customize the column layout.

c Click **Save Changes**.

Configure the print job settings

Note: This feature is applicable only to Print Management Console. For example, when the Print feature is disabled, only users using Print Management Console are unable to print..

a Click **Feature Options** > **Print Jobs**.

b From the Administrator section, configure the print job settings that administrators can perform.

c From the User section, configure the print job settings that users can perform.

d Click **Save Changes**.

Remove user information

Deleting a user deletes all information for that user. We recommend using this feature only when a user leaves the organization.

a Click **Erase User** > **Erase User**.

Notes:

- LPM uses the User Data Management Service to handle the deletion of user information from the LPM system.
- Some of the user information is deleted from the database while some is just replaced with **`'<deleted user>'`**. The replacement ensures data consistency.
- The user information replaced with **`'<deleted user>'`** includes print statistics and reports.

b Search for a user, and then click .

Note: Permanently deleted users cannot be recovered.

c Click **Yes**.

Note: To confirm whether the removal is successful, click **Refresh**.

Manage e-mail reports

Notes:

- The reports are based on the default dashboard.
- A maximum of only five reports are stored in the server.
- Depending on the size of the report, its delivery time may vary.
- The download file is a ZIP file that contains CSV files that are named after each card in the dashboard.
- Large data such as data that covers more than two years may cause an error to the e-mail reporting feature.

a Click **Feature Options** > **E-mail Reporting**, and then do any of the following:

- To send e-mail reports, select **Enable E-mail Reporting**.
- To specify the frequency of e-mail reports, configure the Reporting Schedule section.
- To specify the sender, recipient, and default language of the e-mail reports, configure the Email Defaults section.
- To configure the SMTP server, configure the E-mail Setup section.
- To specify the location of the reports, configure the Reports Storage Location section.

  Note: If the location is on a different server or in an enterprise environment with multiple servers, then share the reports with read and write access.

b Click **Save Changes**.

Manage AirPrint settings

a Click **AirPrint**, and then do any of the following:

- To change the server status, click **Server Status**.
- To configure server settings, click **General**.
- To configure print settings, click **Printing** or **Paper Options**.
- To view the DNS record, click **DNS Record**.

b Click **Save Changes**.

Manage LDAP settings

Note: Use a different LDAP server or a different search base for administrators.

a Click **LDAP**.

b Configure the settings.

Manage user information

Note: This setting is applicable only to new logs.

a Click **Log Information**.

b Configure the setting.

When enabled, user information such as the following are hidden in the log files:

- User name
- User ID
- E-mail address

- Workstation IP address
- Print job name

c Click **Save Changes**.

Log files that contain user information before LPM version 2.9 deployment are not hidden. If you want to hide or remove older user information, then clear the following log files from ***<install_Dir>*\Lexmark \Solutions**, where ***<install_Dir>*** is the installation folder of LDD:

- idm.log
- lpm.log
- mfpauth.log
- lsas.log

Password Management

When selecting **Password** as the Authentication method, enter the password in the Password field, and then reenter the same password in the Confirm Password field.

Notes:

- The password must be at least 8 characters, and must include at least one uppercase, one special, and one numeric character.
- It must also be different from the last number of passwords as set in the Prevent Reuse of Most Recently Used Passwords setting.

Password Management

1 Select **Allow password configuration**.

Note: Even after configuring the Password Management, you can clear the **Allow password configuration** to disable the password management and e-mail notification configuration.

2 Configure the settings:

- **Password Expiration**—Set the number of days after which the password expires. The applicable values range from 90 to 180 days.
- **Prevent Reuse of Most Recently Used Passwords**—Set the number of previous passwords that you want to prevent from being reused. The applicable values range from 3 to 10.

3 Click **Save Changes**.

E-mail Notification

1 Select **Send e-mail reminder before the password expires**.

Note: Even after configuring the E-mail Notification, you can clear **Send e-mail reminder before the password expires** to disable the e-mail notification configuration. This setting does not affect the password expiry even if it is disabled.

2 Configure the settings:

- **SMTP Server**—Enter the server address.
- **Port**—Enter the port number.

- **Use SSL/TLS**—Select the preferred security protocol. Select **Require Trusted Certificate** to enhance the security protocol.

  Note: The SMTP Server, Port and Use SSL/TLS settings are shared with Email Reporting settings. Any changes in these settings will be reflected on the E-mail Reporting settings as well.
- **Number of Days Before Expiration**—Set the number of days before expiration of a password when the notification begins. The applicable values range from 15 to 150 days.
- **Frequency**—Set the frequency for the e-mail notification.

  Note: You can set the exact time, day, and date of the frequency.
- **Default Language**—Select the preferred language.
- **Recipient's Email Address**—Type the e-mail address or addresses of the recipient.

3 Click **Save Changes**.

Using the Print Management Console features

By default, the only visible features on the page are Dashboard, Print Queue, Delegates, and Badge. To show more, see “Show more features” on page 96.

Dashboards

Notes:

- The setting configured from the Lexmark Reports Aggregator Service determines how frequently the data is refreshed. For more information, see “Configuring Reports Aggregator” on page 210.
- You can view the depicted total per category by hovering the mouse over any colored area of the chart. Clicking on the aforementioned area will show a detailed list encompassing that selected category. Clicking any area on the chart will update the data table accordingly. For example, clicking the "Deleted" section in the "Printed vs Deleted" card will update the data table to show only the deleted jobs. However, clicking on the refresh button located on the top right corner of the data table will show a combined list per category

1 From Print Management Console, click **Dashboards**.

2 Do any of the following:

Create a dashboard

a Click **Actions** > **Dashboard** > **Create**.

b Type a unique name.

Note: Dashboard names are case sensitive.

c Click **Create**.

Note: You can also copy or delete existing dashboards.

Create cards

a Select a dashboard, and then click **Actions** > **Add Card**.

b Type a unique name.

c Select a report type, and then configure its settings.

Note: For more information on report types, see "Understanding reports" on page 100.

d Click **Add Card** > **Done**.

Notes:

- For the top user report, the ID of the users who released the jobs appear.
- The environmental impact computations use the Paper Calculator from Environmental Paper Network. For more information, go to **https://www.papercalculator.org/**.

Change card layout

a Select a dashboard, and then click **Actions** > **Change View**.

b Select the number of columns.

Rename the dashboard

a Select a dashboard, and then click **Actions** > **Dashboard** > **Rename**.

b Type a unique name.

Note: Dashboard names are case sensitive.

c Click **Rename**.

Note: You can also change the dashboard name from the Edit page.

Setting a default dashboard

In the list of dashboards, the default dashboard has a ★ beside its name.

Select a dashboard, and then click **Actions** > **Dashboard** > **Set as Default**.

Manage e-mail reports

Click **Actions** > **Dashboard** > **Setup Reporting**.

Note: For more information, see "Manage e-mail reports" on page 97.

Understanding reports

Report type	Report items
Color versus Mono—Shows the total number of printed color and black-and-white jobs.	• **Card Name** • **Chart Type** • **Date Range**
Duplex versus Simplex—Shows the total number of printed two-sided and one-sided jobs.	
Job Type—Shows the total number of sent jobs per type.	
Printed versus Deleted—Shows the number of pages that are printed and the number of pages that are deleted, based on the number of submitted pages. Pages that are deleted are expired or were removed manually.	

Report type	Report items
Environmental Impact—Shows some analysis on the printer usage, such as potential savings and environmental impact.	• **Card Name** • **Unit of Measurement**—Lets you select either the English or metric system when viewing the reports. • **Date Range**
Pages Printed—Shows the total number of printed jobs.	• **Card Name** • **Chart Type** • **Date Range** • **Interval**—Lets you view the daily, weekly, monthly, or yearly data of the report.
Top Printers by Job Type—Shows the printers with the highest usage per job type. The graph is sorted based on the page count.	• **Card Name** • **Job Type** • **Number of Printers** • **Date Range**
Top Users by Job Type—Shows the users with the highest usage per job type. The graph is sorted based on the page count.	• **Card Name** • **Job Type** • **Number of Users** • **Date Range**

Print and Reprint Queues

Use the Print Queue feature to view all submitted jobs that are not yet printed or deleted.

Use the Reprint Queue feature to view all submitted jobs that are printed at least once but not yet deleted.

1. Depending on your configuration, from the Print Management Console, do either of the following:
   - Click **Print Queue** or **Reprint Queue**.
   - Click **Print Jobs** > **Print Queue** or **Reprint Queue**.
2. Manage the print jobs.
   - Filter the list by typing the keywords in the Filter field, and then clicking  .

     Note: Do not use special characters or symbols.
   - Show or hide columns by clicking  .
   - Refresh the list by clicking  .
   - Delegate, print, or delete print jobs.

     Note: When delegating to groups, only the group ID is shown on the Print Management Console user portal.

Delegates

View and manage user or group delegates.

A delegate is a user who is allowed to print another user's jobs. For example, an administrative assistant may print jobs submitted by an executive.

Notes:

- You can assign an individual as the delegate or as part of a delegate group for more than one user. However, you can assign only one delegate or delegate group to each user.
- When delegating to groups, only the group ID is shown on the Print Management Console user portal.

1. From Print Management Console, click **Delegates**.
2. Manage the delegates.
   - Filter the list by typing the keywords in the Filter field, and then clicking  .

     Note: Do not use special characters or symbols.
   - Refresh the list by clicking  .
   - Add, edit, or delete users or groups.

     Notes:

     - For groups, you can add only one member at a time.
     - If multiple domain support is enabled, then use the **`user@domain.com`** format.
     - If Update the delegate for existing print jobs is not selected, then the delegate can print only future jobs.

PIN

Increase security by adding a Print Release PIN (PIN only) or a Card Authentication PIN (user name and PIN) to a user account. Only one PIN type can be used at a time. For more information on Card Authentication, see the *Card Authentication Administrator's Guide*.

Notes:

- Administrators cannot manually add and edit guest users.
- Guest PINs cannot be exported.

1. Depending on your configuration, from the Print Management Console, do either of the following:
   - Click **PIN**.
   - Click **Security** > **PIN**.
2. Manage the PINs.
   - Filter the list by typing the keywords in the Filter field, and then clicking  .

     Note: Do not use special characters or symbols.
   - Refresh the list by clicking  .

- Add, edit, or delete PINs.

  Note: You can create a random PIN by clicking **Generate PIN**.
- Import or export PINs.

  Note: When importing, use a CSV file with the **`pin, userid`** format.

Configuring PIN settings

1. Click  on the upper-right corner of the Print Management Console.
2. Click **Feature Options** > **PIN**.
3. Configure the settings.

   Note: If Unique PIN is enabled, then make sure that there are no duplicate Print Release PINs in the Print Management Console. For more information, see “PIN” on page 102.
4. Click **Save Changes**.

Badge

Manage badges registered for the solution.

Note: Configure the solution to let users register their badges when using the solution for the first time. For more information, see the *Card Authentication Administrator’s Guide*.

1. Depending on your configuration, from the Print Management Console, do either of the following:
   - Click **Badge**.
   - Click **Security** > **Badge**.
2. Manage the badges.
   - Filter the list by typing the keywords in the Filter field, and then clicking  .

     Note: Do not use special characters or symbols.
   - Show or hide columns by clicking  .
   - Refresh the list by clicking  .
   - Add, edit, or delete badges.

     Notes:

     - Make sure that the badge ID is mapped to your operating system user ID to get the print jobs from the print queue.
     - You can only add one badge ID at a time.
     - You can also create a temporary badge ID for a user.
   - Import or export badges.

     Note: When importing, use a CSV file with the **`badgeid, userid`** format.

Configuring feature options for badges

1. Click on the upper-right corner of the Print Management Console.
2. Click **Feature Options** > **Badge**.
3. Configure the following:
   - **Registered Device**—The printer where the badge was registered
   - **Last Used Device**—The printer where the badge was last used
4. Click **Save Changes**.

Function Access

Manage user or group access to printer functions.

1. Depending on your configuration, from the Print Management Console, do either of the following:
   - Click **Function Access**.
   - Click **Security** > **Function Access**.
2. Manage the access to printer functions.
   - Filter the list by typing the keywords in the Filter field, and then clicking .

     Note: Do not use special characters or symbols.
   - Refresh the list by clicking .
   - Add, edit, or delete accesses.
   - Set the default access to printer functions.
     a. Depending on your configuration, do either of the following:
        - Click **Groups** > **Defaults**.
        - Click **Users** > **Defaults**.
     b. Select any of the following:
        - **Allow Copy**
        - **Allow Color Copies**
        - **Allow only Mono Copies on Color Devices**
        - **Allow Email**
        - **Allow Fax**
        - **Allow Scan to Network**
        - **Allow Print**
        - **Allow Color Print**
        - **Allow only Mono Print on Color Devices**

Allowing group access to printer functions

1. Click on the upper-right corner of the Print Management Console.
2. Click **Feature Options** > **Function Access**.

3 In the Groups menu, select **Yes**.

4 Click **Save Changes**.

Quotas

View and manage user and group print quotas.

1 From Print Management Console, click **Quotas**.

2 Manage quotas.

- Filter the list by selecting a quota type, typing the keywords in the Filter field, and then clicking  .

  Note: Do not use special characters or symbols.

- Show or hide columns by clicking  .
- Refresh the list by clicking  .
- Add, edit, or delete quotas.

  Notes:

  - Add the group associated with the Active Directory group manually. The group name must match the name in the Active Directory group.
  - A user quota is established depending on their Active Directory group.
  - The individual user quota supersedes the group quota.

Configuring quota settings

Manage user and group quotas on a monthly or annual basis. Depending on your configuration, the user receives a new allocation of pages on the first day of each month or year. Unused pages are not carried over from the previous time frame.

1 Click  on the upper-right corner of Print Management Console.

2 Click **Feature Options** > **Quota**.

3 Configure the following:

- **Type**—Lets you select when the running quota is refreshed
- **Groups**—Lets you select whether the quota is applied on a group
- **Allow Edit**

4 Click **Save Changes**.

Policies

Manage user or group restrictions when printing. Print policies are settings that are enabled when printing jobs. They override the print settings configured by a user.

Note: To enforce print policies during job submission, make sure that the Lexmark Print Management Client is installed on the user's computer.

1. From the Print Management Console, click **Policies**.
2. Manage the policies.
   - Filter the list by typing keywords such as the policy name in the Filter field, and then clicking .

     Note: Do not use special characters or symbols.
   - Refresh the list by clicking .
   - Add, edit, copy, or delete a policy.
   - Add, edit, or delete users or groups.
   - Assign policies to users or groups.

Allowing group policies

1. Click on the upper-right corner of the Print Management Console.
2. Click **Feature Options** > **Policies**.

   Note: If Policies is not available, then enable Policies from the Settings section.
3. In the Groups menu, select **Yes**.
4. Click **Save Changes**.

Notes:

- Policies are created using policy rules.
- Assign the policy to a group. The group name must match the AD/LDAP group. For more information on assigning policies, see "Assigning policies" on page 106
- If a user tries to release a job but is not a policy user, that user is looked up in the LDAP group. If the user exists in a group, then the user automatically inherits or is assigned the policy that is in place for that LDAP group. The user is also automatically added in the Users tab of the policy. If the user is a member of multiple groups, the first group in the lookup applies.

Assigning policies

You can assign policies to two types of groups: Custom and AD/LDAP.

For Custom groups:

1. Create a group.
2. Assign users to the group.
3. Assign policies to the group.

For AD/LDAP groups:

1. Create a group with the same name as the AD/LDAP group name.

   Note: Unlike a Custom group, there is no need to assign users to a newly created AD/LDAP group.
2. Assign policies to the group.

Adding policies

You can add, edit, delete policies.

1. From the Print Management Console, click **Policies** > **Add**.
2. In the Policy name field, type the name of the policy.
3. If you want to restrict jobs to black-and-white printing only, then select **Force color jobs to mono**.

   Note: You can specify a limit to the number of color pages that can be printed.
4. If you want to restrict jobs to two-sided printing only, then select **Force jobs to two-sided printing**.
   a. From the Edge menu, select the edge type.
   b. From the Applies to menu, select whether to apply the policy to color and mono jobs or to selected jobs.

   Notes:

   - You can specify a limit to the number of color pages that can be printed.
   - Force jobs to two-sided printing policy is not enforced or applied to secure print jobs.
5. If you want to restrict the printing to a certain time, then select **Set print schedule**.
6. Configure the print schedule by selecting the day, start time, and end time.
7. Click **Add Policy**.

Understanding policy rules

A policy contains the business rules of the organization based on the following:

- User
- Document attributes

Policy rules and actions

Original print job properties		Action
Color/Mono	Number of pages	
Color	All	Force to mono
Color	At least a specific number	Force to mono
Mono	All	N/A, since job is already mono

Original print job properties			Action
Simplex/Duplex	Color/Mono	Number of pages	
Simplex[1]	Color	All	Force to duplex
Simplex[1]	Color	At least a specific number	Force to duplex
Simplex[1]	Mono	All	Force to duplex
Simplex[1]	Mono	At least a specific number	Force to duplex
Simplex[1]	Color and Mono	All	Force to duplex

[1] Prints only on one side of the paper.

[2] Prints on both sides of the paper.

Original print job properties			Action
Simplex/Duplex	Color/Mono	Number of pages	
Simplex[1]	Color and Mono	At least a specific number	Force to duplex
Duplex[2]	Any	All	N/A, since job is already duplex

[1] Prints only on one side of the paper.

[2] Prints on both sides of the paper.

Alternate Locations

This feature lets you release print jobs on another printer. For example, when using a monochrome printer, you can select a color printer to release print jobs in color.

1. Depending on your configuration, from the Print Management Console, do either of the following:
   - Click **Alternate Locations**.
   - Click **Device Functions** > **Alternate Locations**.
2. Manage the printers.
   - Filter the list by typing the keywords in the Filter field, and then clicking .

     Note: Do not use special characters or symbols.
   - Refresh the list by clicking .
   - Add, edit, or delete the printers.
     - **Release IP**—The IP address of the printer where the print job is submitted
     - **Alternate IP**—The IP address of the printer where the print job is printed
     - **Alternate Display Name**
     - **Alternate Model Name**
     - **Alternate Device is Color**

PrintTrack Devices

Track print jobs on printers that do not support the Device Usage application.

You can still print jobs through a shared Windows operating system print queue, but directly to the printer instead of being held before printing. To store the information with the print job data, add the information using the PrintTrack Device feature. If the information is not added, then the model and the device type are not stored in the usage date.

1. Depending on your configuration, from the Print Management Console, do either of the following:
   - Click **PrintTrack Devices**.
   - Click **Device Functions** > **PrintTrack Devices**.
2. Manage the sites.
   - Filter the list by typing the keywords in the Filter field, and then clicking .

     Note: Do not use special characters or symbols.
   - Refresh the list by clicking .

- Add, edit, or delete sites.
  - **Site**—The location where the print job is printed
  - **Address**—The IP address of the printer where the print job is printed
  - **Model Name**—The printer model number or custom text such as the printer friendly name
  - **Model Type**
  - **Comment**

Printer Nicknames

Printer nicknames are friendly names that are associated with the IP address of printers. When printing directly to a printer, EmailWatcher lets users specify a printer nickname in the subject line of e-mails instead of the printer IP address.

1. Depending on your configuration, from the Print Management Console, do either of the following:
   - Click **Printer Nicknames**.
   - Click **Device Functions** > **Printer Nicknames**.
2. Manage the printers.
   - Filter the list by typing the keywords in the Filter field, and then clicking  .

     Note: Do not use special characters or symbols.
   - Refresh the list by clicking  .
   - Add, edit, or delete printers.

Auditing logs using the LPM portal

1. From the LPM portal, navigate to the audit log, and then configure the following:
   - **Enable/Disable audit logging**—Enabled by default.
   - **Email information**—The default value of the subject is Login Alert.
   - **The sender's email address**
   - **The recipient's email address**—Can be multiple.
2. Export the audit logs to a CSV file.

   The audit logs track the following events:
   - Logging in and logging out from the LPM admin and user portals
   - Logging in using LMC credentials
   - Logging in using LDAP credentials
   - Logging in to the system configuration access setting
   - Updating configuration access authentication settings and password management
   - Adding or updating LDAP settings

Managing and generating a report

Using Lexmark Management Console

Generating reports

Export the data from the usage tracking database to a CSV or a PDF file for data analysis.

1. From the Lexmark Management Console, click the **System** tab.
2. From the Systems section, select **Reports**.
3. From the Available Reports section, select **PR - Full Data Export**, and then specify the reporting period.
4. Select the output format.
5. Do either of the following:

   Save the report

   a. Select **Save To**, and then click **...** beside the text field.
   b. Specify the folder path.
   c. If the folder is password protected, then provide the necessary credentials.
   d. Click **OK**.

   E-mail the report

   a. Select **Email To**, and then click **...** beside the text field.
   b. Specify the e-mail settings.
   c. Click **OK**.

6. If necessary, add more parameters.
7. Click **Run Report**.

Adding a custom report

1. From the Available Reports section, click +.
2. Type a unique report name, and then configure the settings.
3. Click **Save**.

Scheduling reports

1. Access Lexmark Management Console from your Web browser, and then click the **System** tab.
2. From the System section, select **Schedule**, and then click **Add**.

   Note: If you want to modify the existing schedule, then select the scheduled task, and then click **Edit**.
3. From the “Choose task” dialog, select **Report**, and then click **Next**.
4. From the Available Reports section, select **PR - Full Data Export**, and then specify the reporting period.

5 Select the output format you want to generate.
   - **PDF**—This generates a report in PDF format.
   - **CSV**—This generates a report in Excel format.

6 If you want to save the exported file, then do the following:
   a Select the **Save To** check box, and then click the button next to the “Save to” field.
   b Specify the path of the folder where you want to save the file, and then click **OK**.

7 If you want to send the report to an e-mail address, then do the following:
   a Select the **Email To** check box, and then click the button next to the “Email to” field.
   b Specify the recipient of your e-mail and other information, and then click **OK**.

8 Click **Next**.

9 From the “Choose the frequency” dialog, specify the start date and time and how often the generated report runs, and then click **Finish**.

Using Print Management Console

Generating reports

1 From the Print Management Console, click **Dashboards**.

2 Select a dashboard, and then select a card.

Exporting reports

1 From the Print Management Console, generate a report.

2 Click  , and then click **Export**.

Securing Lexmark Print Management

Understanding Free and Open Source Software and vulnerability scanners

The LDD platform, where LPM resides, uses Free and Open Source Software (FOSS). We review the FOSS and monitor sites for publicly known cybersecurity vulnerabilities.

When a vulnerability is detected, the code is refactored and the components are replaced. Patches are prepared, and then released.

Numerous vulnerabilities are related to older versions of the web server software. Hotfixes and patches issued for Apache, Tomcat, or OpenSSL are included in the next version of LDD. We recommend updating to the latest version of LDD when available.

Various vulnerability scanners are used on LPM. These tools analyze the product and the source code to identify known vulnerabilities and weaknesses. The findings are categorized using the following rating system that varies for each printer:

- Critical
- Important
- Moderate
- Informational

The scanning software reports issues found in the server operating system and the software that are installed on it. Some of these issues are not directly LPM issues. We recommended applying the latest updates and patches from Windows Update and software vendors.

Configuring Secure Print

LPM Premise offers a more secure way of printing jobs by implementing the End-to-End Encryption of print jobs. Print jobs are encrypted during submission with the use of a specific print driver (Lexmark UPD 3.0). The print job stays encrypted while being stored in the file server and is decrypted only during printing with the use of PrintCryption 2.0 eSF application. Encrypted print jobs can be identified by the file extension .tar in the file name.

Note: Encrypted print jobs are not converted to duplex even if the user is assigned with Force jobs to two-sided printing policy.

Job Submission Methods

To submit secure print jobs, you can use either Job Router or Client Software.

For more information on installing the job router service, see the *Lexmark Document Distributor Administrator's Guide*.

For more information on installing Client Software, see "Installing the LDD Port monitor software" on page 49.

Note: Secure print is not supported on jobs submitted by mobile, e-mail, AirPrint, PrintTrack, and LPM.

Device Groups

1. From Lexmark Management Console, click **Device Groups** > **Print Release**.
2. In the Tasks section, click **eSF Configuration**.
3. In the eSF Applications: (Solution) section, click **printcryption2(PrintReleasev2)**.
   a. Enable **Deploy to**.
   b. Click **Save Settings**.

Securing access to Print Management Console

Enforcing HTTPS is the easiest way to ensure that users do not use plain text HTTP to send data. Before enforcing HTTPS, make sure that Apache is configured for HTTPS connection and that the necessary SSL certificates are installed.

For LDD version 5 or earlier

1. Open the **httpd.conf** file.
2. Add the **`Redirect permanent / https://y:9783/lmc/`** line, where ***y*** is the server address.

   Note: Any request made to the **http://*y*:9780/lmc** URL directs to the **https://*y*:9783/lmc** URL, where ***y*** is the server address.
3. Save the file.
4. Restart the Apache service.

For LPM

1. Open the **httpd.conf** file.
2. Remove **#** from the **`IncludeOptional conf/httpd-lpm-redirect.conf`** line.

3 Add**#** before the **IncludeOptional conf/httpd-lpm.conf** line.

4 Save the file.

5 Restart the Apache service.

Sample configuration

```
# Include lpm specific configuration file
#
IncludeOptional conf/httpd-lpm-redirect.conf

# Include lpm specific configuration file
#
# IncludeOptional conf/httpd-lpm.conf
```

To enhance security, do the following:

- Change the default administrator account user name and password.
- Set up a connection with an LDAP server to authenticate user names and passwords other than the administrator account.
- Restrict access to only administrators.

For more information, see the *Lexmark Document Distributor Administrator's Guide*.

Understanding digital certificates

LPM comes with self-signed certificates. Obtain a digital certificate signed by a trusted certificate authority, and then apply it in the following locations:

- Apache
- Httpd.conf file

Configuring Apache to use SSL certificate

When using HTTPS to connect to the Lexmark Management Console or Print Management Console, obtain a valid SSL certificate for the server. This process is necessary only for the LDD load balancer server.

Note: When using LDD version 4.8 or later, enter **https://*LBaddr*/lmc**, where ***LBaddr*** is the host name or IP address of the LDD load balancer server. This URL accesses the Lexmark Management Console or Print Management Console.

1 Log in to console of the server, hosting the LDD load balancer.

2 Open the command prompt as an administrator.

3 Navigate to the ***<install-Dir>*\lexmark\solutions\Apache2\bin** folder, where ***<install-Dir>*** is the installation folder of LDD.

4 In the command prompt, type the **set OPENSSL_CONF=*<install-Dir>*\lexmark\solutions\Apache2\conf\openssl_ldd.cnf** line, where ***<install-Dir>*** is the installation folder of LDD.

5 Type the following command:

```
openssl req -new -newkey rsa:2048 -nodes -out <lddserver.csr> -keyout <lddserver.key> -
subj "/C=US/ST=KY/L=Lexington/O=Lexmark/OU=NA/CN=lddserver.domain.com"
```

Note: Omitting the **-subj** and the path prompts the OpenSSL to require a value. You may consult with your certificate authority team for the appropriate values. The fully qualified name is built for this server, but the subject data is unique per customer.

6. Send the **lddserver.csr** file to your certificate authority team.
7. Save the signed certificate as a PEM file, for example, **lddserver.pem**.
8. Copy the following to the ***<install-Dir>*\lexmark\solutions\Apache2\conf** folder, where ***<install-Dir>*** is the installation folder of LDD:
   - **lddserver.key** file
   - **CA.pem** (root or intermediary CA) certificate file
   - **lddserver.pem** file
9. From the ***<install-Dir>*\lexmark\solutions\Apache2\conf\ldd-cert.conf** for LDD versions 5.1 and later or ***<install-Dir>*\lexmark\solutions\Apache2\conf\httpd-ssl.conf** file for LDD versions 5 and earlier, update the following:

Sample configuration

```
SSLCertificateFile "<install-Dir>/Lexmark/Solutions/Apache2/conf/lddserver.pem"

SSLCertificateKeyFile "<install-Dir>/Lexmark/Solutions/Apache2/conf/lddserver.key"

SSLCertificateChainFile "<install-Dir>/Lexmark/Solutions/Apache2/conf/ca.pem"
```

Where ***<install-Dir>*** is the installation folder of LDD.

10. Save the file.
11. Restart the Apache service.

Access the LDD load balancer server, and then verify whether your certificate authority has signed the certificate on the website.

Note: The CN value for the certificate signing request in lddserver.domain.com must be the same value for accessing the server when using Lexmark Management Console. Using only the IP address or host name generates an invalid certificate error when accessing the server when it does not match the certificate.

Authenticating Lexmark Print Management

We recommend applying security policies such as the following on LPM servers:

- Minimum passwords policies
- Service accounts
- Directory permissions
- Open ports

Note: Some restrictions may be in conflict with LPM. For example, virus scanning of certain directories can cause file contention issues. To ensure that new policies do not conflict with LPM, review each policy before applying them.

Antivirus policy requirements and recommendations

Required antivirus policies

- Exclude the following folders when performing real-time virus scanning:
  - Load balancer server or database server
    - ***<install-Dir>*\Lexmark\Solutions\Apache2\htdocs\auth** and all subfolders
    - ***<install-Dir>*\Lexmark\Solutions\Apache2\htdocs\printrelease** and all subfolders

    Where ***<install-Dir>*** is the installation folder of LDD.
  - Application servers
    - ***<install-Dir>*\Lexmark\Solutions\apps\idm** and all subfolders
    - ***<install-Dir>*\Lexmark\Solutions\apps\lpm** and all subfolders
    - ***<install-Dir>*\Lexmark\Solutions\apps\mfpauth** and all subfolders
    - ***<install-Dir>*\Lexmark\Solutions\apps\printrelease** and all subfolders

    Where ***<install-Dir>*** is the installation folder of LDD.
  - Directory for print jobs

    For example, **C:\lexmark\printrelease**.

    Note: The directory can be configured using the PrintReleasev2 solution setting.
  - Directory for installation and backup files for troubleshooting

    For example, **C:\ProgramData\Lexmark\PrintManagement** and all subfolders.

Recommended antivirus policy

Run the following on all Lexmark servers during off-peak hours:

- Full virus scans
- Virus definition updates

Configuring Apache using the httpd.conf file

1. From your computer, navigate to the ***<install-Dir>*\Solutions\Apache2\conf** folder, where ***<install-Dir>*** is the installation folder of Apache.
2. Using a text editor, configure any of the following:

   Notes:

   - Some directives are not present or inactive by default.
   - For more information, see the Apache website.

Vulnerability	Directive
The web server response header of an HTTP response may contain the following: • Web server type and version • Operating system and version • Associated ports • Compiled-in modules	Set the **`ServerTokens`** directive to **`Prod`**, and the **`ServerSignature`** directive to **`Off`**.

Vulnerability	Directive
Other files such as documentation, sample code and applications, and tutorials may be a threat.	**Note:** The list of sample files may change with the software versions. Remove the following sample code and documentation items: • ***<install-Dir>*/apache2/manual/*.*** • ***<install-Dir>*/apache2/conf/extra/*.*** • ***<install-Dir>*/apache2/cgi-bin/printenv** • ***<install-Dir>*/apache2/cgi-bin/test-cgi** Where ***<install-Dir>*** is the installation folder of Apache.
To help mitigate denial-of-service attacks, specify timeouts. **Note:** If necessary, adjust these settings for each server.	Do the following: • Set **`Timeout`** directives to **`300`** or less. • Set **`KeepAlive`** directives to **`On`**. • Set **`KeepAliveTimeout`** to **`15`** or less.
CGI scripts are one of the most exploited vulnerabilities on web servers. Run CGI scripts in Apache using the following methods: • **`ScriptAlias`**—Configures the server to read everything in a directory as a CGI script. • Combination of the **`Options`** and **`AddHandler`** or **`SetHandler`** directives—When a combination of the **`Options`** and **`Handler`** directives is used, the ability to manage scripts centrally is lost, creating a vulnerability on the web server. We recommend managing scripts using the **`ScriptAlias`** directive.	Search for the following uncommented directives: • **`SetHandler`** • **`AddHandler`** • **`Options`** For all instances of the **`SetHandler`** and **`AddHandler`** directives, query the web administrator to determine if the directives allow CGI scripts. If CGI scripts are used by the **`SetHandler`** or **`AddHandler`** directives, then it is a finding. For all instances of the **`Options`** directive that are using +ExecCGI or ExecCGI, it is a finding. If the **`Options`** directive is found with -ExecCGI, then it is not a finding. If the value does not exist, then it is a finding unless the **`Options`** statement is set to **`None`**. Locate the scripts in a **`ScriptAlias`** directory, and then add the appropriate symbol to disable ExecCGI, or set the **`Options`** directive to **`None`**.

Vulnerability	Directive
The **Options** directive configures the web server features that are available in specific directories. The **FollowSymLinks** feature lets you reference a file or directory using a symbolic name, raising a potential hazard when the symbol is linked to sensitive data. The **includesNoOEXEC** feature enables server-side includes but disables the **exec** command to help prevent the execution of malware. The **Multiviews** feature may respond with all available files in a directory that are not meant for browsing. If a URL maps to a directory without a **DirectoryIndex** (index.html), then a list of directories that are not meant for browsing may be returned.	Set all **Options** directives to the following, respectively: • **-FollowSymLinks** • **-includes**, **-includesNOEXEC**, or **+includesNOEXEC** • **-MultiViews** • **-indexes** **Note:** Setting the **Options** directive to **None** disables all extra features.
The following directives mitigate buffer overflow and denial-of-service attacks by limiting the amount of accepted data: • The **LimitRequestBody** directive lets you set a limit on the allowed size of an HTTP request message body. • The **LimitRequestFields** directive lets you limit the number of request header fields. • The **LimitRequestFieldSize** directive lets you set a limit on the allowed size of an HTTP request header field. • The **LimitRequestLine** directive lets you set a limit on the allowed size of a client's HTTP request-line. **Note:** If errors occur, then adjust these values for each server.	Do any of the following: • Set the **LimitRequestBody** directive to any number greater than **0**. • Set the **LimitRequestFields** directive to any number greater than **0**. • Set the **LimitRequestFieldSize** directive to **8190**. • Set the **LimitRequestLine** directive to **8190**. **Note:** Some of these values are the default values, but they must be explicitly set.
Web servers get their capabilities using modules. Minimizing the enabled modules to only the required modules reduces the number of vulnerable points. The Apache proxy modules let the server act as a forward or reverse proxy of HTTP and other protocols.	To show a list of loaded modules, do the following: **a** From your computer, open the command prompt. **b** Navigate to the ***<install-Dir>*/apache2/bin/** folder, where ***<install-Dir>*** is the installation folder of Apache. **c** Run the **httpd -M** command. The following modules are required core Apache modules: • core_module • win32_module • mpm_winnt_module • http_module • so_module

Vulnerability	Directive
Scanning for web servers that send proxy requests is a common attack. Proxy servers can anonymize attacks on other servers or send proxy requests to a protected network. The following modules are Apache proxy modules and are not required for LPM: • proxy_module • proxy_ajp_module • proxy_balancer_module • proxy_ftp_module • proxy_http_module • proxy_connect_module Disable the **UserDir** directive to prevent access to user home directories. userdir_module Content that is specific to the web server can be used to identify the type and version of the web server. Disable access to various content to help mitigate attacks. autoindex_module	To disable modules that are not required for LPM, in the httpd.conf file, add **#** before appropriate modules.
Access to the root of the web server must be secured. • The Apache **Directory** directive enables directory-specific configuration. Create a default deny policy that does not allow access to the root directory of the operating system. • Use the Apache **Options** directive to create a default minimal options policy for the root directory where permissions may be enabled. • Use the Apache **OverRide** directive to let a .htaccess file specify previous configuration directives that can be changed. **Note:** The authz_core_module uses the **Require all denied** directive.	Set the root **Directory** directive (**<Directory />**) to the following, respectively: • **Order deny,allow** • **Deny from all** • **Options None** • **AllowOverride None** If these root directory entries do not exist, then add them.
The TRACE method is not necessary and must be disabled.	Set the **TraceEnable** directive to **Off**. If this directive does not exist, then add it.
The Apache **Listen** directive specifies the IP addresses and port numbers that the Apache web server listens to for requests. Configure the server to listen only to expected addresses and port numbers.	Specify the IP address and the port number for each **Listen** directive.

Vulnerability	Directive
The **ScriptAlias** directive specifies which directories the Apache server recognizes as containing scripts. If the directive uses a URL-path name that is different than the actual file system path, then the script source code may be exposed.	Verify whether **URL-path** and **file-path/directy-path** of the **ScriptAlias** directive match. **Sample of a correct path** **ScriptAlias/cgi-bin/*<install-Dir>*/cgi-bin/**, where ***<install-Dir>*** is the installation folder of Apache. **Sample of an incorrect path** **ScriptAlias/script-cgi-bin/*<install-Dir>*/cgi-bin/**, where ***<install-Dir>*** is the installation folder of Apache.
HTTP Request Methods such as PUT and DELETE modify resources and are not required for LPM to function. Disable these methods.	For each **Directory** directive except **root**, set the following: **Order allow,deny** **<LimitExcept GET POST OPTIONS> Deny from all </LimitExcept>**

3 Save the file.

4 Restart the Apache service.

Note: Some common security-related configuration, such as WebDAV, and Apache mod_info and mod_status modules, may be in conflict with LPM or LDD.

Supported port numbers and protocols

Make sure that the firewall allows the following port numbers and protocols:

Component	Port number	Protocol	Configuration	Function
Database (Firebird)	3050	TCP	Application server to database	Database communications
	8001	TCP	Application server and load balancer to database server	Backup and Restore agent

[1] MFPAuth requires either 443 or 9783 depending on how the URL is defined within the CardAuth.

Note: The configuration between server and database or between server and load balancer is done on specific firewall rules based on source IPs.

Component	Port number	Protocol	Configuration	Function
Load balancer	443	TCP	Open	Load balancer HTTPS TLS communications, including Lexmark Management Console
	9700	TCP	Open	• Profile submission to e-Task printers • Web adapter (JMX)
	9705	TCP	Application server to load balancer	Apache agent
	9780	TCP	Open	Load balancer communications, including Lexmark Management Console
	9783	TCP	Open	Load balancer HTTPS TLS communications, including Lexmark Management Console
Server	4111	TCP	Application server to application server	JMX
	5111	TCP	Application server to application server	RMI
	8009	TCP	Load balancer to Tomcat	AJP and Tomcat connector (load balancer worker)
	9743	TCP	Open	HTTPS TLS profile job submission from printers or client software to a server, including Lexmark Management Console
	9788	TCP	Open	Profile job submission from printers or client software to a server, including Lexmark Management Console

[1] MFPAuth requires either 443 or 9783 depending on how the URL is defined within the CardAuth.

Note: The configuration between server and database or between server and load balancer is done on specific firewall rules based on source IPs.

Component	Port number	Protocol	Configuration	Function
Printer	79	TCP		Finger
	161	UDP		• SNMP • Printer discovery
	5000	TCP		• Policy updates • ObjectStore plain text communication
	5353	UDP		Multicast DNS
	6000	UDP		• Printer discovery • ObjectStore communication using XML protocol
	6100	UDP		• Printer discovery • Policy updates • Lexmark Secure Transport (LST) encrypted data
	6110	TCP		• Printer discovery • Policy updates • LST authentication and negotiation
	9100	TCP		• Printing • Policy updates
	9300	UDP		• Printer discovery • NPA protocol UDP communications
	9500	TCP		NPA protocol TCP communications
LPM	631	TCP	Open	IPP
	5672	TCP	Application Server to application server	ActiveMQ
	61613			
	61614			
	61616			

[1] MFPAuth requires either 443 or 9783 depending on how the URL is defined within the CardAuth.

Note: The configuration between server and database or between server and load balancer is done on specific firewall rules based on source IPs.

Standard port numbers for LDAP and LDAPS

Port number	Function
389	LDAP communications
636	LDAPS communications

Authenticating using LPM REST API

Note: The following instructions are applicable to the Print Management Console, mobile authentication, and Chrome extension authentication.

Authenticating using a token

To protect resources, the LPM REST API token uses JSON web token for verifying access claims. Depending on the credentials provided during authentication, the REST service may issue an administrator or user token.

Note: The user token has limited resource access.

By default, the token validity is 30 minutes. To update the expiration time, do the following:

1. From your computer, navigate to the ***<install-Dir>*\Lexmark\Solutions\apps\idm\WEB-INF\classes** folder, where ***<install-Dir>*** is the installation folder of LDD.
2. Using a text editor, open the **idm-production-config.properties** file.
3. Specify the value for **`idm.token.expirationInMinutes`**.
4. Save the file.

Authenticating using a hashid

To address the Insecure Direct Object Reference vulnerability, the LPM REST API service masks all resource IDs with hashids. This method prevents the interface from exposing dbid references to outside entities.

The hashid algorithm relies on key phrase or salt to calculate and generate a hashid value. Changing the salt value generates different hashid calculations.

To change the default salt value, do the following:

1. From your computer, navigate to the ***<install-Dir>*\Lexmark\Solutions\apps\lpm\WEB-INF\classes** folder, where ***<install-Dir>*** is the installation folder of LDD.
2. Using a text editor, open the **app-production-config.properties** file.
3. Specify the value for **`hashids.salt`**.
4. Save the file.

Note: When using an enterprise setup, make sure that all application servers have the same salt value.

Performing optional configurations

Configuring DNS servers

The following instructions are verified using BIND version 9.

You can manually configure a Microsoft DNS server or a BIND for Windows DNS server to do the following:

- AirPrint advertisement
- Service discovery for the Lexmark Print Management solution
- Reply to Unicast DNS queries from an AirPrint-capable device

This section provides information on how to add the DNS role, create a zone or domain, and add the required subdomains and appropriate resource records (TXT/PTR/SRV).

This section provides information on the most common configurations for an enterprise environment and is intended for network administrators. For information on other configurations, contact the Lexmark Professional Services team.

Configuring DNS servers for AirPrint advertisement

Adding a DNS role in Windows Server 2012

Note: Make sure that the server is configured with a static IP address.

1. From the Windows Administrative Tools window, click **Server Manager**.
2. Click **Manage** > **Add Roles and Features** > **Next**.
3. For the installation type, select **Role-based or feature-based installation**, and then click **Next**.
4. Click **Select a server from the server pool**, and then select the appropriate server.
5. Select **DNS Server** > **Add Features** > **Next**.
6. Click **Install**.

Adding a forward lookup zone

Note: Make sure that you have the domain name and IP address of your DNS server.

1. From the Windows Administrative Tools window, click **DNS**.
2. Expand the host name of your server, right-click **Forward Lookup Zones**, and then click **New Zone** > **Next**.
3. For the zone type, select **Primary zone**, and then click **Next**.
4. Specify the name of your domain, and then click **Next**.
5. Click **Create a new file with this file name**, and then click **Next**.

6 Select **Do not allow dynamic updates** > **Next**.

Note: Allow dynamic updates only when adding the new zone to a parent DNS server or when the new server installation is the only network DNS server. For more information on your environment, contact your system administrator.

7 Click **Finish**.

Adding a reverse lookup zone

Notes:

- Make sure that you have the domain name and IP address of your DNS server.
- This process is optional. Add a reverse lookup zone only when your network does not have a parent DNS server that manages the host records for clients on your network. You can also add a reverse lookup zone when your organization does not allow dynamic updates to occur on the parent DNS server.

1 From the primary DNS server, navigate to the Windows Administrative Tools window, and then click **DNS**.

Note: The primary DNS server is the parent DNS server of your organization or the new DNS server that you are installing.

2 Expand the host name of your server, right-click **Reverse Lookup Zones**, and then click **New Zone** > **Next**.

3 For the zone type, select **Primary zone**, and then click **Next**.

4 Select **IPv4 Reverse Lookup**, and then click **Next**.

5 Enter the first three octets of the IP address of your DNS server, and then click **Next**.

6 Click **Create a new file with this file name**, and then click **Next**.

7 Select **Do not allow dynamic updates** > **Next**.

Note: Allow dynamic updates only when adding the new zone to a parent DNS server or when the new server installation is the only network DNS server. For more information on your environment, contact your system administrator.

8 Click **Finish**.

Adding a host A record

Note: This process is optional. Add a host A record only when your network does not have a parent DNS server that manages the host records for clients on your network. You can also add a host A record when your organization does not allow dynamic updates to occur on the parent DNS server.

1 From the primary DNS server, navigate to the Windows Administrative Tools window, and then click **DNS**.

Note: The primary DNS server is the parent DNS server of your organization or the new DNS server that you are installing.

2 Expand the host name of your server, right-click the domain that is created in the forward lookup zone, and then click **New Host (A)** > **Next**.

3 Specify the host name and IP address of the LPM server.

Note: In an enterprise system, make sure that the LPM server is performing a load balancer role and that its IP address is static.

4 Select **Create associated pointer (PTR) record** > **Add Host**.

Other considerations

Host A records in the forward and reverse lookup zones are created automatically in the following scenarios:

- When joining Active Directory Domain
- When the DNS server is not a member of Active Directory Domain and Dynamic Updates are allowed

When creating host A records in a zone or subdomain, specify only the host name of the server, and not the fully qualified domain name.

Adding a Canonical Name (CNAME) record

Note: This process is optional. Add a CNAME record only when you have the DNS entries of an existing server and you want to use **`lpm-airprint`** as an alias for the server.

1 From the primary DNS server, navigate to the Windows Administrative Tools window, and then click **DNS**.

Note: The primary DNS server is the parent DNS server of your organization or the new DNS server that you are installing.

2 Expand the host name of your server, right-click the domain that is created in the forward lookup zone, and then click **New Alias (CNAME)** > **Next**.

3 Specify the alias name and the fully qualified domain name of the server.

4 Click **OK**.

Adding an _tcp subdomain

1 From the Windows Administrative Tools window, click **DNS**.

2 Expand the host name of your server, right-click the domain that is created in the forward lookup zone, and then click **New Domain**.

3 In the New DNS Domain dialog box, type **`_tcp`**.

4 Click **OK**.

Adding an _ipp subdomain

1 From the Windows Administrative Tools window, click **DNS**.

2 Expand the host name of your server, right-click the _tcp subdomain following the forward lookup zone, and then click **New Domain**.

3 In the New DNS Domain dialog box, type **`_ipp`**.

4 Click **OK**.

Adding an _sub subdomain

1. From the Windows Administrative Tools window, click **DNS**.
2. Expand the host name of your server, and then expand the _tcp subdomain following the forward lookup zone.
3. Right-click the _ipp subdomain, and then click **New Domain**.
4. In the New DNS Domain dialog box, type **_sub**.
5. Click **OK**.

Adding the _universal PTR record

1. From the Windows Administrative Tools window, click **DNS**.
2. Expand the host name of your server, and then expand the _tcp and _ipp subdomains following the forward lookup zone.
3. Right-click the _sub subdomain, and then click **Other New Records**.
4. In the Resource Record Type dialog box, select **Pointer (PTR)**, and then click **Create Record**.
5. In the Host IP Address field, type **_universal**.
6. In the Host name field, type the host name in the following format:

   ***hostname*._ipp._tcp.*domain*.com**

   Where:

   - ***hostname*** is the host name of the server used when creating the host A record.

     Note: Use the correct server host name in the PTR record for the _sub domain and the PTR, SRV, and TXT records for the _ipp domain.
   - ***domain*** is the domain name of your organization.
7. Click **OK**.

Adding the PTR, SRV, and TXT records

1. From the Windows Administrative Tools window, click **DNS**.
2. Expand the host name of your server, and then expand the _tcp subdomain following the forward lookup zone.
3. Right-click the _ipp subdomain, and then click **Other New Records**.
4. In the Resource Record Type dialog box, do any of the following:

   For PTR

   a. Select **Pointer (PTR)**, and then click **Create Record**

   b. Leave the Host IP Address field blank.

   c. In the Host name field, type the host name in the following format:

   ***hostname*._ipp._tcp.*domain*.com**

Where:

- ***hostname*** is the host name of the server used when creating the host A record.

  Note: Use the correct server host name in the PTR record for the _sub domain and the PTR, SRV, and TXT records for the _ipp domain.

- ***domain*** is the domain name of your organization.

For SRV

a Select **Service Location (SRV)**, and then click **Create Record**

b In the Service field, type the host name of the server.

c In the Protocol field, type **_ipp**.

d Make sure that the Priority and Weight fields are set to **0**.

e In the Port number field, enter **631**.

f In the Host offering this service field, type the fully qualified domain name of the LPM server.

For TXT

a Select **Text (TXT)**, and then click **Create Record**

b In the Record name field, type the host name of the server.

c In the Text section, specify the correct key and value pairs.

Sample key and value pairs (_ipp subdomain)

```
txtvers=1
qtotal=1
product=(Lexmark Print server version 1.0)
note=Physical location to advertise
pdl=image/urf,application/pdf,image/jpeg,application/octet-stream
adminurl=http://SERVERIPADDRESS:9780/lpm/config
priority=0
rp=lpm/ipp/print
URF=V1.4,CP1,PQ3-4-5,RS300-600,MT1-2-3-4-5-6-8-10-11-12-13,W8,ADOBERGB24,DEVRGB24,DEVW8,SRGB2
4,IS1,IFU0,OB10
Color=T
Duplex=T
Scan=F
Fax=F
Binary=T
Transparent=T
Copies=T
Collate=T
ty=Lexmark Print server version 1.0
UUID=b15525c7-8885-4279-a0a2-2ec669b9fbaa
TLS=1.2
kind=document
PaperMax=<legal-A4
air=none
```

Note: The key and value pairs from the DNS Record window on the configuration portal of your server (**http://*serverIPaddress*:9780/lpm/config**) apply to the _ipp and _ipps subdomains. However, the value for the **air=** key must be **none**, and the **printer-type=** key and value pair must be omitted from the _ipp TXT record.

5 Click **OK**.

Adding an _ipps subdomain

1. From the Windows Administrative Tools window, click **DNS**.
2. Expand the host name of your server, right-click the _tcp subdomain following the forward lookup zone, and then click **New Domain**.
3. In the New DNS Domain dialog box, type **_ipps**.
4. Click **OK**.

Adding an _sub subdomain for _ipps subdomain

1. From the Windows Administrative Tools window, click **DNS**.
2. Expand the host name of your server, and then expand the _tcp subdomain following the forward lookup zone.
3. Right-click the _ipps subdomain, and then click **New Domain**.
4. In the New DNS Domain dialog box, type **_sub**.
5. Click **OK**.

Adding the _universal PTR record for _sub subdomain

1. From the Windows Administrative Tools window, click **DNS**.
2. Expand the host name of your server, and then expand the _tcp and _ipps subdomains following the forward lookup zone.
3. Right-click the _sub subdomain, and then click **Other New Records**.
4. In the Resource Record Type dialog box, select **Pointer (PTR)**, and then click **Create Record**.
5. In the Host IP Address field, type **_universal**.
6. In the Host name field, type the host name in the following format:

   ***hostname*._ipps._tcp.*domain*.com**

   Where:

   - ***hostname*** is the host name of the server used when creating the host A record.

     Note: Use the correct server host name in the PTR record for the _sub domain and the PTR, SRV, and TXT records for the _ipps domain.
   - ***domain*** is the domain name of your organization.
7. Click **OK**.

Adding the PTR, SRV, and TXT records for _ipps subdomain

1. From the Windows Administrative Tools window, click **DNS**.
2. Expand the host name of your server, and then expand the _tcp subdomain following the forward lookup zone.
3. Right-click the _ipps subdomain, and then click **Other New Records**.

4 In the Resource Record Type dialog box, do any of the following:

For PTR

a Select **Pointer (PTR)**, and then click **Create Record**

b Leave the Host IP Address field blank.

c In the Host name field, type the host name in the following format:

***hostname*._ipps._tcp.*domain*.com**

Where:

- ***hostname*** is the host name of the server used when creating the host A record.

  Note: Use the correct server host name in the PTR record for the _sub domain and the PTR, SRV, and TXT records for the _ipps domain.

- ***domain*** is the domain name of your organization.

For SRV

a Select **Service Location (SRV)**, and then click **Create Record**

b In the Service field, type the host name of the server.

c In the Protocol field, type **_ipps**.

d Make sure that the Priority and Weight fields are set to **0**.

e In the Port number field, enter **443**.

f In the Host offering this service field, type the fully qualified domain name of the LPM server.

For TXT

a Select **Text (TXT)**, and then click **Create Record**

b In the Record name field, type the host name of the server.

c In the Text section, specify the correct key and value pairs.

Sample key and value pairs (_ipp subdomain)

```
txtvers=1
qtotal=1
product=(Lexmark Print server version 1.0)
note=Physical location to advertise
pdl=image/urf,application/pdf,image/jpeg,application/octet-stream
adminurl=http://SERVERIPADDRESS:9780/lpm/config
priority=0
rp=lpm/ipp/print
URF=V1.4,CP1,PQ3-4-5,RS300-600,MT1-2-3-4-5-6-8-10-11-12-13,W8,ADOBERGB24,DEVRGB24,DEVW8,SRGB2
4,IS1,IFU0,OB10
Color=T
Duplex=T
Scan=F
Fax=F
Binary=T
Transparent=T
Copies=T
Collate=T
ty=Lexmark Print server version 1.0
UUID=b15525c7-8885-4279-a0a2-2ec669b9fbaa
TLS=1.2
kind=document
PaperMax=<legal-A4
air=username,password
printer-type=0x4C0901C
```

Note: The key and value pairs from the DNS Record window on the configuration portal of your server (**http://*serverIPaddress*:9780/lpm/config**) apply to the _ipp and _ipps subdomains. However, the value for the **air=** key must be **username,password**, and the **printer-type=** key and value pair must be added in the _ipps TXT record.

5 Click **OK**.

Adding an _udp subdomain

1 From the Windows Administrative Tools window, click **DNS**.

2 Expand the host name of your server, right-click the domain that is created in the forward lookup zone, and then click **New Domain**.

3 In the New DNS Domain dialog box, type **_udp**.

4 Click **OK**.

Adding an _udp-sd subdomain

1 From the Windows Administrative Tools window, click **DNS**.

2 Expand the host name of your server, right-click the _udp subdomain following the forward lookup zone, and then click **New Domain**.

3 In the New DNS Domain dialog box, type **_dns-sd**.

4 Click **OK**.

Adding the _services, b, and lb PTR records for _dns-sd subdomain

1 From the Windows Administrative Tools window, click **DNS**.

2 Expand the host name of your server, and then expand the _udp subdomain following the forward lookup zone.

3 Right-click the _dns-sd subdomain, and then click **Other New Records**.

4 In the Resource Record Type dialog box, do any of the following:

For _ipp

a Select **Pointer (PTR)**, and then click **Create Record**

b In the Host IP Address field, type **_services**.

c In the Host name field, type **_ipp._tcp.*domain*.com**, where ***domain*** is the domain name of your organization.

For _ipps

a Select **Pointer (PTR)**, and then click **Create Record**

b In the Host IP Address field, type **_services**.

c In the Host name field, type **_ipps._tcp.*domain*.com**, where ***domain*** is the domain name of your organization.

For b and lb

a Select **Pointer (PTR)**, and then click **Create Record**

b In the Host IP Address field, type **b** or **1b**, respectively.

c In the Host name field, type the domain name of your organization.

5 Click **OK**.

Setting up a DNS forwarder

In network environments where primary or secondary DNS servers are installed, create a forwarder to the new DNS server. The new DNS server must be where the resource records for AirPrint advertisement and services discovery are maintained. The forwarder lets AirPrint devices locate the LPM server without adding the records required for AirPrint advertisement to the existing DNS servers. It is not necessary to update the IP address of the primary and secondary DNS servers on the client devices or computers.

Note: Setting up a DNS forwarder is not necessary when adding the resource records to a parent DNS server. It is also not necessary when the new server installation is the only network DNS server. For more information on your environment, contact your system administrator.

1 From the primary or secondary DNS server, navigate to the Windows Administrative Tools window, and then click **DNS**.

Note: The primary DNS server is the parent DNS server of your organization or the new DNS server that you are installing.

2 Right-click the host name of your server, and then click **Properties**.

3 From the Forwarders tab, click **Edit**.

4 In the Selected domain's forwarder IP address list field, specify the IP address of your new server installation.

5 Click **Add**.

Configuring BIND

1 From Windows Explorer, navigate to the BIND installation folder, and then open the **etc** folder.

2 Open the **named.conf** file, and then add the following line:

```
options { forwarders { DNSserver; }; forward only; };
```

Where ***DNSserver*** is the IP address of the DNS server that contains the appropriate AirPrint resource records.

3 Save the file.

Delegating a domain

In network environments where primary or secondary DNS servers are installed, create a delegation map for the new domain to the new DNS server. The new DNS server must be where the resource records for AirPrint advertisement and services discovery are maintained. Delegation mapping lets AirPrint devices locate the LPM server without adding the records required for AirPrint advertisement to the existing DNS servers. Make sure that the IP address of the new DNS server is added to the list of DNS servers on the client devices or computers.

Note: Setting up a delegation is not necessary when adding the resource records to a parent DNS server. It is also not necessary when the new server installation is the only network DNS server. For more information on your environment, contact your system administrator.

1. From the primary or secondary DNS server, navigate to the Windows Administrative Tools window, and then click **DNS**.

   Note: The primary DNS server is the parent DNS server of your organization or the new DNS server that you are installing.

2. Right-click the zone or domain where you want to create a delegation, and then click **New Delegation** > **Next**.
3. Specify the name of the subdomain to delegate, and then click **Next** > **Add**.
4. Specify the IP address of the DNS server that contains the appropriate AirPrint resource records for the subdomain, and then click **Ok**.
5. Click **Finish**.

Configuring BIND for AirPrint advertisement

Note: Make sure that the server is configured with a static IP address, and that you have installed BIND.

Creating key files

1. From the command prompt, navigate to the BIND installation folder. For example, **`cd C:\dns`**.
2. Switch to the bin directory. For example, **`cd bin`**.
3. Type **`rndc-confgen -a`**, and then press **Enter**.
4. Type **`rndc-confgen >..\etc\rndc.conf`**, and then press **Enter**.

Creating named.conf files

1. From the command prompt, navigate to the BIND installation folder. For example, **`cd C:\dns`**.
2. Switch to the etc directory. For example, **`cd etc`**.
3. Type **`start notepad named.conf`**, and then press **Enter**.
4. When prompted to create a file, click **Yes**.
5. At the top of the file, type **`options { directory dir-install; };`**, where ***`dir-install`*** is the BIND installation directory, and then press **Enter**.
6. From Windows Explorer, navigate to the BIND installation folder, and then open the **etc** folder.

7 Open the **rndc.conf** file, and then copy the text following the **`# Use with the following named.conf..`** line.

8 Open the **named.conf** file, and then paste the text after the **`options {directory...`** line.

9 Remove **#** from all lines except the **`Use with the following...`** and **`End of named.conf`** lines.

10 Click **File** > **Exit** > **Save**.

Creating forward lookup zone files

Note: Make sure that you have the domain name and IP address of your DNS server.

1 From the command prompt, navigate to the BIND installation folder. For example, **`cd C:\dns`**.

2 Switch to the etc directory. For example, **`cd etc`**.

3 Type **`start notepad db.domain`**, where ***`domain`*** is the domain name of your server, and then press **Enter**.

4 When prompted to create a file, click **Yes**.

5 In the new zone file, add the following in **bold**:

```
$TTL 3600
@ IN SOA lpm-airprint.domain.com. unused-email (1 10800 3600 604800 60)
@ IN NS lpm-airprint.domain.com.
lpm-airprint.domain.com. IN A 192.168.1.10
b._dns-sd._udp IN PTR @
lb._dns-sd._udp IN PTR @
_services.dns-sd._udp IN PTR _ipp._tcp.domain.com.
_services.dns-sd._udp IN PTR _ipps._tcp.domain.com.
_universal._sub._ipp._tcp IN PTR lpm-airprint._ipp._tcp.domain.com.
_universal._sub._ipps._tcp IN PTR lpm-airprint._ipps._tcp.domain.com.

_ipp._tcp IN PTR lpm-airprint._ipp._tcp.domain.com.
lpm-airprint._ipp._tcp IN SRV 0 0 631 lpm-airprint.domain.com.
lpm-airprint._ipp._tcp IN TXT "txtvers=1""qtotal=1""product=Lexmark Print server version
1.0""note=Physical location to
advertise""pdl=image/urf,application/pdf,image/jpeg,application/octet-
stream""adminurl=http://SERVERIPADDRESS:
9780/lpm/config""priority=0""rp=lpm/ipp/print""URF=V1.4,CP1,PQ3-4-5,RS300-600,MT1-2-3-4-5-
6-8-10-11-12-13,W8,ADOBERGB24,DEVRGB24,DEVW8,SRGB24,IS1,IFU0,OB10""Color=T""Duplex=T""Scan
=F""Fax=F""Binary=T""Transparent=T""Copies=T""Collate=T""ty=Lexmark Print server version
1.0""UUID=b15525c7-8885-4279-
a0a2-2ec669b9fbaa""TLS=1.2""kind=document""PaperMax=<legal-A4""air=none"

_ipps._tcp IN PTR lpm-airprint._ipps._tcp.domain.com.
lpm-airprint._ipps._tcp IN SRV 0 0 443 lpm-airprint.domain.com.
lpm-airprint._ipp._tcp IN TXT "txtvers=1""qtotal=1""product=Lexmark Print server version
1.0""note=Physical location to
advertise""pdl=image/urf,application/pdf,image/jpeg,application/octet-
stream""adminurl=http://SERVERIPADDRESS:
9780/lpm/config""priority=0""rp=lpm/ipp/print""URF=V1.4,CP1,PQ3-4-5,RS300-600,MT1-2-3-4-5-
6-8-10-11-12-13,W8,ADOBERGB24,DEVRGB24,DEVW8,SRGB24,IS1,IFU0,OB10""Color=T""Duplex=T""Scan
=F""Fax=F""Binary=T""Transparent=T""Copies=T""Collate=T""ty=Lexmark Print server version
1.0""UUID=b15525c7-8885-4279-
a0a2-2ec669b9fbaa""TLS=1.2""kind=document""PaperMax=<legal-A4""air=username,password""prin
ter-type=0x4C0901C"
```

Where:

- ***`lpm-airprint.domain.com`*** is the fully qualified domain name of your server.
- ***`192.168.1.10`*** is the IP address of your server.
- ***`lpm-airprint`*** is the host name of your server.

Note: The key and value pairs are listed in the DNS Record window on the configuration portal of your server (**http://*serverIPaddress*:9780/lpm/config**). Make sure that the extra parenthesis for the **product=** key and value pairs are removed.

6 Save the file.

Creating reverse lookup zone files

Note: Make sure that you have the domain name and IP address of your DNS server.

1 From the command prompt, navigate to the BIND installation folder. For example, **cd C:\dns**.

2 Switch to the etc directory. For example, **cd etc**.

3 Type **start notepad db.*domain*.in-addr.arpa**, where ***domain*** is the first three octets of the IP address of your server in reverse order, and then press **Enter**.

4 When prompted to create a file, click **Yes**.

5 In the new zone file, add the following:

```
$TTL 3600
@ IN SOA lpm-airprint.domain.com. unused-email (1 10800 3600 604800 60)
@ IN NS lpm-airprint.domain.com.
20 IN PTR lpm-airprint.domain.com.
```

Where:

- ***lpm-airprint.domain.com*** is the fully qualified domain name of your server.
- ***20*** is the last octet of the IP address of your server.

Notes:

- If there are duplicate AirPrint advertisements on the client devices when using BIND on Linux or Unix in the db.domain file, remove the **_universal._sub._ipp._tcp IN PTR lpm-airprint._ipp._tcp.domain.com** line.
- If character limitations occur when using GUI tools to add DNS records to a BIND server, reduce the key and value pairs to **air=**, **pdl=**, **qtotal=**, **rp=**, **tls=**, and **urf=**.
- If there are Mac OS X 10.10 or later client workstations on the network, then add the **Color=** and **Duplex=** key and value pairs. Starting with Mac OS X 10.10, depending on the value of **Color=** and **Duplex=**, the color and duplex print settings for an AirPrint printer are disabled.

6 Save the file.

Referencing zone files in the named.conf file

Note: The zone file may not be in the same folder as the named.conf file.

1 From Windows Explorer, navigate to the BIND installation folder, and then open the **etc** folder.

2 Open the **named.conf** file, and then add the following after the **options {directory...** line:

```
zone "domain.com." { type master; file "db.domain"; allow-update { any; }; };
zone "1.168.192.in-addr.arpa" { type master; file "db.1.168.192.in-addr.arpa"; allow-
update { any; }; };
```

Notes:

- The value after the **`file`** element is the relative path to the zone file. The path and file name must be correct based on the zone file that you have created. The **`allow-update`** key allows clients to add or update their DNS records, known as Dynamic Update.
- Allow dynamic updates only when adding the new zone to a parent DNS server or when the new server installation is the only network DNS server. For more information on your environment, contact your system administrator.

3 Save the file.

Starting the ISC BIND service

After the following are created, start the ISC BIND service:

- Key files
- Zone files
- named.conf file

Note: Make sure that the startup type for the service is set to **Automatic**.

1 From the Windows Administrative Tools window, click **Services**.

2 Right-click the ISC BIND service, and then click **Properties**.

3 From the Log On tab, set Log on as to **Local System Account**, and then click **OK**.

4 Right-click the ISC BIND service, and then click **Start**.

Other considerations for DNS server configuration

The zones, domains, and resource records for AirPrint advertisement can be added to the parent DNS server of your organization. These domains and resource records can also be added to an existing zone. Clients that are configured to use that DNS server can discover the server using AirPrint when the following are specified in the network properties:

- DNS server IP address
- Search domains

However, we recommend installing the DNS role on the LPM server, and then adding the appropriate zones, domains, and records to that server. Specify that server as a secondary DNS server or configure a forwarder on the parent DNS server using the IP address of the LPM server.

Zone transfers

Zone transfers can be considered a security risk. It must not occur between the parent DNS server and the LPM server. Setting up a forwarder or a delegation prevents zone transfers between the parent DNS server and the LPM server.

Note: For more information on your environment, contact your system administrator.

Client configuration

You can configure the following with the IP address of the DNS server that is configured with a forwarder to the DNS server. The DNS server must be where the resource records for AirPrint advertisement and services discovery are maintained. Make sure that the iOS mobile device contains the correct zone or domain name as a search domain. For example, **domain.com**. These settings can be configured on the mobile device using a DHCP server or by manually editing the settings of that particular network:

- Mobile devices
- Macintosh computers

Note: For more information on your environment, contact your system administrator.

Creating profiles using Apple Configurator

An AirPrint device or AirPrint server can be deployed to a mobile device using a profile.

Note: AirPrint profiles are applicable only on mobile devices running on iOS 7 or later.

1. From your Macintosh computer, launch the Apple Configurator tool.
2. Click **Supervise**.
3. Select **All Devices** > ✚ > **Create New Profile**.
4. Select **AirPrint**, and then click **Configure**.
5. From the AirPrint window, click ✚.
6. Do either of the following:

   ### Manual configuration

   a. From the Configure printer menu, select **Manually**, and then type the IP address of the load balancer.
   b. In the Resource path field, type **lpm/ipp/print**.

   ### LPM configuration

   Note: The following instructions are applicable only when your Macintosh computer is on the same subnet as the AirPrint server. You must also enable Bonjour discovery in the LPM web portal.

   a. From the Configure printer menu, select **Lexmark Print Management**, and then type the IPv4 or IPv6 address of the load balancer.
   b. In the Resource path field, make sure that **/lpm/ipp/print** is entered.

   Note: You can add multiple AirPrint devices to a profile.

7. From the Supervise window, select the profile, and then export it.
8. Type a unique name for the profile, and then specify the location.
9. Click **Save**.

To install the profile on a mobile device, do the following:

- Use the Apple Configurator tool
- E-mail the profile to the mobile device as an attachment
- Deploy the profile using a mobile device management tool

Understanding the command line tools for DNS server configuration

- **NSLookup**—Lets you resolve names in the forward and reverse lookup zones. From the command line of a Windows or Macintosh computer, do either of the following:
  - Type **nslookup *IPaddress***, where ***IPaddress*** is the IP address of the server, and then press **Enter**. Make sure that the correct host name is returned to indicate that the host (A) records have been created successfully.
  - Type **nslookup *HostName***, where ***HostName*** is the IP address of the server, and then press **Enter**. Make sure that the correct IP address is returned to indicate that the host (A) records have been created successfully.
- **DNS-SD**—Lets you view a list of AirPrint-advertised services and their associated domain names. You must be on the same network subnet as the server to view the mDNS advertisements of the server. This tool lets you check whether the records for AirPrint advertisement have been created correctly for the appropriate zone or domain name.

  With the Bonjour SDK installed on your Windows computer, from the command line, type **dns-sd -B _ipp._tcp**.

  To check the details of an advertised printer service, from the command line, type the following:

  dns-sd -L *HostName* _ipps._tcp *DomainName*

  Where:
  - ***HostName*** is the host name for your environment.
  - ***DomainName*** is the domain name for your environment.

  Note: To prevent conflicts with the Bonjour Service used for mDNS advertisements, do not install the Bonjour SDK (or Bonjour for Windows) on the LPM server.
- **DIG**—Lets you check whether the resource records are correct from a terminal session on a Macintosh computer. The following are sample DIG commands:
  - **dig -t PTR _ipps._tcp.domain.com**

    This command returns the host name for the PTR record in the **Answer** section of the response.
  - **dig -t SRV lpm-airprint._ipps._tcp.domain.com**

    This command returns the priority, weight, port, and host name information for the SRV record in the **Answer** section of the response.
  - **dig -t TXT lpm-airprint._ipps._tcp.domain.com**

    This command returns the key and value pairs for the TXT record in the **Answer** section of the response.
  - **dig -x *192.168.1.10***

    This command performs a forward lookup. It returns the host name in the **Answer** section as defined in the forward lookup zone for the sample IP address ***192.168.1.10***.
  - **dig *lpm-airprint.domain.com***

    This command performs a reverse lookup. It returns the IP address in the **Answer** section as defined in the reverse lookup zone for the sample host name ***lpm-airprint.domain.com***.

Configuring Print Release with rf IDEAS

1. Install the rf IDEAS Ethernet 241 adapters. For more information, see "Installing the rf IDEAS Ethernet 241 adapter" on page 139.
2. Configure the rf IDEAS Ethernet 241 adapters.
   - For more information on using the discovery tool, see "Configuring rf IDEAS Ethernet 241 using the rf IDEAS discovery tool" on page 139.
   - For more information on using the Lexmark Print Release Adapter Management tool, see "Configuring rf IDEAS Ethernet 241 using the Lexmark Print Release Adapter Management tool" on page 140.
3. If necessary, configure the rf IDEAS badge readers. For more information, see "Configuring rf IDEAS badge readers" on page 140.
4. Configure the client profiles. For more information, see "Configuring client profiles" on page 141.
5. Configure the user authentication. For more information, see "Configuring user authentication" on page 141.
6. Configure the Lexmark Print Management Console features. For more information, see "Configuring the Print Management Console features" on page 141.
7. Set the LDD server online. For more information, see "Changing the status of the server" on page 48.

Note: After the configuration, the rf IDEAS device reboots and may cause its IP address to change. We recommend performing a subnet search again after configuring it.

Installing the rf IDEAS Ethernet 241 adapter

1. From your computer, connect the rf IDEAS Ethernet 241 RJ-45 network port to your network.
2. Connect the rf IDEAS Ethernet 241 RJ-45 printer port to the network port of your printer.
3. Connect the badge reader to the rf IDEAS Ethernet 241 serial or USB card reader port.

Configuring rf IDEAS Ethernet 241 using the rf IDEAS discovery tool

Notes:

- rf IDEAS Discovery Tool requires firmware version 2.02 or later.
- We recommend using this tool when deploying to many printers.

1. From your computer, create a file containing the IP address of all rf IDEAS Ethernet 241 adapters.

Sample file

```
192.168.0.3
192.168.0.120
192.168.24.3
192.168.25.6
```

2. Run the discovery tool, and then load the file containing the IP address of all rf IDEAS Ethernet 241 adapters.
3. Create an HTML file for pointing rf IDEAS Ethernet 241 to the LPM server.

   Note: A sample file is provided by rf IDEAS.

4 Make sure that the following are added into the HTML file:

```
data_serv_addr=<LB IP Address>
data_serv_port=9780
data_str=/lmc/rws/jsapi/v1/rfideas?profile=RFIDeas&cardid=$1&mac=$2&luid=$3&seq=$4&ip=$5
data_retry_count=10
data_retry_sleep=2
data_long_beep=2
data_shrt_beep=5
```

5 Save the HTML file on a web share.

6 From the discovery tool, type the web share URL.

7 Select the printers, and then click **Configure 241 Devices**.

Note: The **data_serv_port** setting does not appear in the 241 Configuration Settings list.

Configuring rf IDEAS Ethernet 241 using the Lexmark Print Release Adapter Management tool

1 From your computer, create a file containing the IP address of all rf IDEAS Ethernet 241 adapters. From your LPM server, launch Print Release Adapter Management. Do either of the following:

- Navigate to the ***<install-Dir>*\ThirdPartyConfig** folder, where ***<install-Dir>*** is the installation folder of LPM.
- From the command line, type one of the following:
  - **..jre\bin\java.exe -jar lpm-third-party-config*.jar**
  - **run.bat**
  - **run**

2 Enter your credentials for the Print Management Console.

3 In the Address\Subnet of Adapters field, enter an IP address or subnet for printer discovery, and then click **Search**.

Note: When searching for a subnet, use the asterisk wildcard character (*****) at the end of the IP address to search for all printers in that subnet. For example, type **10.10.10.*** to search for all printers that have been discovered within the 10.10.10.1–10.10.10.255 range.

4 Select the adapters for use with the Lexmark Print Release application, and then click **Configure**.

Note: After the configuration, the rf IDEAS device reboots. This process may cause the IP address to change. If necessary, perform another printer discovery.

Configuring rf IDEAS badge readers

1 From your computer, run the rf IDEAS **PCProxConfig** application.

Note: You can also use the PCProxConfig application to configure the badge bit length. To connect to the rf IDEAS device, use its IP address, followed by the appropriate port number. Use port number 2000 for serial badge readers, or port number 2001 for USB badge readers.

2 Connect to the IP address of rf IDEAS Ethernet 241.

3 Click the **Data Format** tab.

4 Set the number of bits used for the badge.

Notes:

- To show the badge number, use a telnet protocol using the IP address of the rf IDEAS device, and then scan the badge.
- To check the configuration of the rf IDEAS device, use a telnet protocol using its IP address, followed by the default telnet port number 23. This process lets you check the values for the **`data_serv_addr`**, **`data_serv_port`**, and **`data_str`**. The format must match your load balancer URL and correct port (9780).

Configuring client profiles

1. From Lexmark Management Console, click the **Software Client Groups** tab.
2. From the Software Client Groups section, select **Print Release**.
3. From the Tasks section, select **Client Profiles**.
4. In the Address field, type the IP address of the printer and the LPM print server.
5. Click **Add** > **Save**.

Configuring user authentication

1. From Lexmark Management Console, click the **Solutions** tab.
2. From the Solutions section, select **PrintReleasev2**.
3. From the Tasks section, select **Configuration**.
4. In the User Authentication menu, select either **Badge with LDAP Lookup** or **Badge with Database Lookup**.
5. Click **Apply**.

If your environment uses different authentication methods such as Card Authentication and rf IDEAS Ethernet 241 devices at the same time, then configure a local authentication. This setting overrides the global authentication solution setting. For more information on configuring global or local solution settings, see the *Lexmark Document Distributor Administrator's Guide*.

The following are sample scenarios you can use for your mixed authentication environment:

- Set the global authentication solution setting to **Provided by Device**. Set the Software Client Group authentication setting to either **Badge with LDAP Lookup** or **Badge with Database Lookup**. You can also select the appropriate software client authentication method for your environment.
- Set the global authentication solution setting to **Badge with LDAP Lookup**. You can also select the appropriate software client authentication method for your environment, and then set the Software Client Group authentication setting to **Provided by Device**.

Configuring the Print Management Console features

Do any of the following:

- Configure the quotas. For more information, see "Quotas" on page 105.
- Configure the delegates list. For more information, see "Delegates" on page 102.
- Configure the policies. For more information, see "Policies" on page 105.

Using Print Release

Sending print jobs from your computer

1. Open a file or image.
2. Select the print option, and then select the print release queue.
3. Click **Print**.
4. If prompted, type your e-mail address and password.

Note: If there are any errors or exceptions that occur during the request, then JobSubmissionController enters the error into the lsas.log file. If necessary, change the logging level from **`info`** to **`debug`**.

Releasing print jobs using the printer

1. From the home screen, touch **Print Release**.
2. Select one or more print jobs.

   Note: To print the jobs that are delegated to you, touch ☰ if necessary, select a username, and then select the print jobs.

3. If necessary, change the print settings. Touch ⋮ beside the Print button, touch **Change Print Settings**, and then do either of the following:
   - Touch **Settings**, and then configure any of the following:
     - **Number of copies**
     - **Color**

       Note: You cannot change black-and-white print jobs to color at the printer for some file formats.
     - **Sides**—Specify whether to print on one side or two sides of the paper.
   - Touch **Finishing Options**, and then configure either of the following:
     - **Staple**—Staple the printed output.
     - **Hole punch**—Punch holes along the edge of the printed output.

     Note: The availability of these settings depends on the configuration of your Lexmark Print Management Client.
4. Touch **Print**.

Notes:

- The Lexmark Print Management Print Release server attempts to transmit the print jobs only to the printer that is attached with rf IDEAS Ethernet 241. The server does not check whether all jobs are printed successfully. If quotas are enabled, then they are updated with the assumption that all jobs are printed successfully.
- If the printer with the Ethernet 241 adapter is monochrome but the released job is in color, then the job is counted against the color quota.
- All queued print jobs are released for the user whose badge is swiped, assuming that the card authentication is successful. If quotas are enabled, then make sure that the quota of the user is adequate to print all the queued jobs.

- If quotas are enabled and the total number of queued pages exceeds the user's quotas, then the jobs are not printed. Increase the quota or delete one or more jobs to print the queued jobs. For example, if three pages remain in the quota but four one-page jobs are waiting in the print queue, then all queued jobs are not printed.

Releasing print jobs using rf IDEAS

1. From the printer, tap your badge on the card reader.

   To acknowledge the badge, the Ethernet 241 adapter beeps once. The following subsequent beeps indicate the status of the card authentication:

   - **Three short beeps**—The communication between the Ethernet 241 adapter and Lexmark Print Management Print Release is successful. A request is made to release your queued print jobs.

     Note: If the user account is not configured correctly, or if the queued jobs exceed the user's quotas, then the jobs are not printed. Make sure that the badge ID value in the Badge tab is configured correctly.
   - **Two long beeps**—The IP address of the printer is not determined. Make sure that the connection of the Ethernet 241 adapter to the printer is working properly.
   - **Five short beeps and two long beeps**—The communication between the Ethernet 241 adapter and Lexmark Print Management server is unsuccessful. Make sure that the Ethernet 241 adapter is configured properly and it is connected to the network.
   - **No beep**—The Lexmark Print Management server has received the request to release the queued print jobs but is unable to respond. Make sure that the system is configured correctly.
2. From the home screen, touch **Print Release**.
3. Select one or more print jobs.

   Note: To print the jobs that are delegated to you, touch ☰ if necessary, select a user name, and then select the print jobs.
4. Touch **Print**.

Configuring Local Printer Management Agent for LPM

The Print Tracker (PT) component of Local Printer Management Agent (LPMA) must know certain information to run properly. For example, it must know where to send a job report. This information is stored in a configuration file called **`PTConfiguration.ini`**. This file is in the directory where the service is installed.

Note: LPMA is installed in the client system and not in the server.

The following is a sample configuration file:

Sample configuration file

```
[CLIENT_VERSION]
VERSION=1.0.0.1

[SERVER]
BLACKOUT_DAYS=DISABLED
BLACKOUT_TIME=DISABLED
CS_COST_CENTER=<cost_center>
CS_CLIENT_ID=<clientID>
CS_CLIENT_SECRET=<clientSecret>
```

```
CS_REPORT_URI=/api/2.0/jobs/directPrint/batch
CS_TOKEN_URI=/idm/oauth/token
REPORT_SERVER_ADDRESS=
REPORT_SERVER_PORT=9780
REPORT_SERVER_SECURE_CONNECTION=DISABLED
TOKEN_SERVER_ADDRESS=
TOKEN_SERVER_PORT=9783
TOKEN_SERVER_SECURE_CONNECTION=ENABLED
TIMEOUT=30

[JOB_REPORT]
RUN=ENABLED
RUN_ON_STARTUP=ENABLED
TASK_RUN_TIME=INTERVAL:120
INCLUDE_LOCAL_PRINTERS=ENABLED
INCLUDE_NETWORK_PRINTERS=ENABLED

[SNMP]
INCLUDE_NETWORK_PRINTERS=ENABLED
```

Where:

- **<cost_center>** is the cost center of the company.
- The values for **<clientID>** and **<clientSecret>** can be taken from ***<install-dir>*\Lexmark\Solutions\apps\idm\WEB-INF\classes\idm-production-config.properties** file, where ***<install-dir>*** is the installation folder of LDD.

The general format of the configuration file is the following:

```
[SECTION_NAME]
key1=value1
key2=value2

...
```

Where:

- **[SECTION_NAME]** is a descriptive name for the section.
- **<key1>** and **<key2>** are names of configurable features that the LPMA service refers during its run.
- **<value1>** and **<value2>** are values to their respective keys.

Notes:

- If the value of a key is case-sensitive, then that key must be prefixed with **CS_**.
- If a key is not used, then its value must be **<DISABLED>**.

Settings and descriptions

The following tables describe features.

[SERVER]

Section key	Usage/values
CS_COST_CENTER	A cost center associated with the user sending the print job.
CS_CLIENT_ID	The client ID of the company sending the report. This user account must be created on IDM server during the server setup, and must not have an administrator right.

Section key	Usage/values
CS_CLIENT_SECRET	The case-sensitive password that is associated with the generic user account created at IDM server. It must never change.
TOKEN_SERVER_ADDRESS	The IP address or host name of the IDM server.
TOKEN_SERVER_PORT	IDM Token Server Port number to communicate to the server. IDM uses SSL port 9783 or 443.
TOKEN_SERVER_SECURE_CONNECTION	If set to **ENABLED**, server communication is secure. This key value pair is used with **[SERVER] TOKEN_SERVER_PORT**.
CS_TOKEN_URI	The URI for obtaining a security token from the IDM server and its value must be **/idm/oauth/token**.
REPORT_SERVER_ADDRESS	The IP address or host name of the LPM Premise server.
REPORT_SERVER_PORT	The LPM Premise Server Port number to communicate to the server. LPM Premise uses SSL port 9783 or 443, and Non-SSL port 9780.
REPORT_SERVER_SECURE_CONNECTION	If set to **ENABLED**, server communication is secure. This key-value pair is used with **[SERVER] REPORT_SERVER_PORT**.
CS_REPORT_URI	The URI for sending the reports to the LPM Premise server and its value must be **/api/2.0/jobs/directPrint/batch**.
TIMEOUT	A numerical value specifying communication timeout in seconds.
BLACKOUT_DAYS	The days of the week when communication with the Fleet Tracker servers is not allowed. This value can be used together with **[SERVER] BLACKOUT_TIME**. Use the numeric value that represents the day of the week, separated by commas. For example, if the value is **1**,**3**,**5**, and **7**, then the blackout days are Sunday, Tuesday, Thursday, and Saturday. You can also set the value to **DISABLED**.
BLACKOUT_TIME	The time of day when communication with the Fleet Tracker server is not allowed. This value is used together with **[SERVER] BLACKOUT_DAYS**. Use the format **HHMM-HHMM**, where **HHMM** is the 24-hour time format for the start and end of the blackout period. For example, **1200-1400** means that the blackout period starts at 12:00 p.m. and ends at 2:00 p.m.

[CLIENT_VERSION]

Section key	Usage/values
VERSION	The current version of the Print Tracker component installed in the system.

[JOB_REPORT]

Section key	Usage/values
RUN	If the value is **ENABLED**, then Print Tracker reports job metrics.
RUN_ON_STARTUP	If the value is **ENABLED**, then Print Tracker, on starting, sends stored job reports, in addition to scheduled job reporting.

Section key	Usage/values
TASK_RUN_TIME	The schedule for print job reporting. The default value is 2 hours. For more information on interval values, see "Valid interval values" on page 146
INCLUDE_LOCAL_PRINTERS	The user can enable or disable this key based on the document tracking requirement.
INCLUDE_NETWORK_PRINTERS	The user can enable or disable this key based on the document tracking requirement.

[SNMP]

Section key	Usage/values
INCLUDE_NETWORK_PRINTERS	Applies if the user wants to monitor Network Print Queue(INCLUDE_NETWORK_PRINTERS=ENABLED). If the network printer uses a different community name other than "public," then the user can provide a custom value in CS_COMMUNITY_NAME field.

Valid interval values

Values	Description
DISABLED	The task is disabled.
INTERVAL:mm	The task runs every time a specified number of minutes elapses. For example, if the key value is set to **INTERVAL:30**, then the task runs every 30 minutes.
HOURLY	The task runs every hour after the service starts. For example, if the service starts at 10:24, then the task runs at 11:24, 12:24, and so on.
DAILY:hhmm1,hhmm2,hhmm...	The task runs every day at specified times. For example, if the key value is **DAILY:0830,1245,2100**, then the task runs every day at 8:30 a.m., 12:45 p.m., and 9:00 p.m.
WEEKLY:dayofweek1,dayofweek2,dayofweek...:hhmm1,hhmm2,hhmm...	The task runs on one or more days of the week at specified times. For example, if the key value is set to **WEEKLY:Sunday,Tuesday,Thursday:0830,1245,2100**, then the task runs at 8:30 a.m., 12:45 p.m., and 9:00 p.m. on each of those days.
Note: Make sure to use the 24-hour time format. Use commas to separate the items.	

Troubleshooting

Lexmark Print Management troubleshooting

Cannot log in to the web portal

Try one or more of the following:

Make sure that the user credentials are correct

If the Print Management server is configured to connect to an LDAP server, then use your LDAP user name and password.

If the Print Management server is configured to support multiple domains, then select a domain, and then type your user name and password.

Contact your LDAP administrator

Cannot find users

Make sure that there are no duplicate Print Release PINs in the Print Management Console

For more information, see “PIN” on page 102.

Cannot remove user information

Check where the error occurred

From the Queued for Erasure table, mouse over the pause icon in the Status column.

Manually delete the user information

From the Queued for Erasure table, click **Verify** in the Status column to check whether the deletion is successful.

Firmware failure [9yy.xx]

The firmware on the device needs to be updated.

Contact Lexmark Help Desk for more information on the latest firmware update.

An application error about a missing bean on the home screen

Restart the Lexmark Solutions Application Server service on the LDD server.

LDAP connection test failed

Try one or more of the following:

Make sure that the user name and password are correct

Make sure that the LDAP settings are correct

Make sure that the LDAP server is working correctly

An error has occurred after IP address change in LDD

In an enterprise environment, an error may occur when the following are installed in three different computers and their IP addresses change:

- Database server (Firebird)
- Load balancer
- LDD application server

Try one or more of the following:

Make sure that the database server is configured correctly

1. From your computer, navigate to the **C:\ProgramFiles\Lexmark\Solutions\InstallHelper** folder.
2. Run **Update-addr.bat**, and then enter **`update-addr.bat –ip <DB_IPaddress>`**, where ***<DB_IPaddress>*** is the new database server IP address.
3. From the Framework DB section, make sure that the LOADBALANCER and SERVER tables are blank.

Make sure that the load balancer server is configured correctly

1. From your computer, navigate to the **C:\ProgramFiles\Lexmark\Solutions\InstallHelper** folder.
2. Run **lpm-update-address.bat**, and then enter **`lpm-update-addr.bat –ip <LB_IPaddress>`**, where ***<LB_IPaddress>*** is the new load balancer server IP address.
3. Stop all LDD services and Apache 3.
4. From the registry, do either of the following:
   - For Firebird, update **`HKLM\SOFTWARE\Wow6432Node\Apache Software Foundation \Procrun 2.0\ApacheAgent\Parameters\Start`** with **`Params [REG_MULTI_SZ] = "start <DB_IPaddress><LB_IPaddress> 9705 C:\Program Files\Lexmark \Solutions FIREBIRD"`**
   - For Microsoft SQL Server, update **`HKLM\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\ApacheAgent\Parameters\Start`** with **`Params [REG_MULTI_SZ] = "start <DB_IPaddress><LB_IPaddress> 9705 C:\Program Files\Lexmark\Solutions MSSQL"`**

   Where:
   - ***<DB_IPaddress>*** is the new database server IP address.
   - ***<LB_IPaddress>*** is the new load balancer server IP address.

5 Navigate to the **C:\ProgramFiles\Lexmark\Solutions\Apache2\conf** folder, and then configure the following files:

For httpd.conf

- **Listen *<LB_IPaddress>*:9780**
- **ServerAdmin admin@*<LB_IPaddress>***
- **ServerName *<LB_IPaddress>*:9780**
- **<VirtualHost *<LB_IPaddress>*:9780**

For httpd-lpm-airprint-config-extension.conf

- **Listen *<LB_IPaddress>*:631**
- **<VirtualHost *<LB_IPaddress>*:631**

For httpd-lpm-redirect.conf

- **RedirectMatch "^/printrelease/(.*)" https://*<LB_IPaddress>*/printrelease/$1**
- **RedirectMatch "^/lpm/(.*)" https://*<LB_IPaddress>*/lpm/$1**
- **RedirectMatch "^/idm/(.*)" https://*<LB_IPaddress>*/idm/$1**
- **RedirectMatch "^/mfpauth/(.*)" https://*<LB_IPaddress>*/mfpauth/$1**
- **RedirectMatch "^/email/(.*)" https://*<LB_IPaddress>*/email/$1**
- **RedirectMatch "^/mobile/(.*)" https://*<LB_IPaddress>*/mobile/$1**

For openssl_ldd.conf

update commonName_default = *<LB_Server>*

Where:

- ***<LB_IPaddress>*** is the new load balancer server IP address.
- ***<LB_Server>*** is the new load balancer server.

Make sure that the application server is configured correctly

1 From your computer, navigate to the **C:\ProgramFiles\Lexmark\Solutions\InstallHelper** folder.

2 Run **lpm-update-address.bat**, and then enter **lpm-update-addr.bat –ip *<LB_IPaddress>***, where ***<LB_IPaddress>*** is the new load balancer server IP address.

3 Navigate to the **C:/Program Files/Lexmark/Solutions/apps/wf-ldss/WEB-INF/classes/adaptor.properties** file, and then update the following:

- **adaptor.canonicalhostname=*<LB_IPaddress>***
- **adaptor.address=*<LB_IPaddress>***
- **centralwebdav.canonicalhostname=*<LB_IPaddress>***

Where ***<LB_IPaddress>*** is the new load balancer server IP address.

4 Navigate to the **C:/Program Files/Lexmark/Solutions/apps/wf-ldss/WEB-INF/classes/dbProduct.properties** file, and then update the following:

database.hostname=*<DB_IPaddress>*

Where ***<DB_IPaddress>*** is the new database server IP address.

5 Navigate to the **C:/Program Files/Lexmark/Solutions/apps/wf-ldss/lmc.url** file, and then update the following:

```
URL=http://<LB_IPaddress>:9780/lmc
```

Where ***<LB_IPaddress>*** is the new load balancer server IP address.

6 Navigate to the **C:/Program Files/Lexmark/Solutions/apps/printrelease/** folder, and then configure the following files:

database.properties

- **database.FRAMEWORK.connect=jdbc:firebirdsql:*<DB_IPaddress>*/3050:FRAMEWORK**
- **database.WEBAPP.connect=jdbc:firebirdsql:*<DB_IPaddress>*/3050:SOLUTIONINFO**
- **database.PRINTRELEASE.connect=jdbc:firebirdsql:*<DB_IPaddress>*/3050:SOLUTIONINFO**
- **database.PRINTRELEASE.driverUrl=jdbc:firebirdsql:*<DB_IPaddress>*/3050:**
- **database.PRINTTRACK.connect=jdbc:firebirdsql:*<DB_IPaddress>*/3050:SOLUTIONINFO**
- **database.PRINTTRACK.driverUrl=jdbc:firebirdsql:*<DB_IPaddress>*/3050:**
- **database.BADGE.connect=jdbc:firebirdsql:*<DB_IPaddress>*/3050:SOLUTIONINFO**
- **database.BADGE.driverUrl=jdbc:firebirdsql:*<DB_IPaddress>*/3050:**
- **database.PIN.connect=jdbc:firebirdsql:*<DB_IPaddress>*/3050:SOLUTIONINFO**
- **database.PIN.driverUrl=jdbc:firebirdsql:*<DB_IPaddress>*/3050:**
- **database.STATS.connect=jdbc:firebirdsql:*<DB_IPaddress>*/3050:SOLUTIONINFO**
- **database.STATS.driverUrl=jdbc:firebirdsql:*<DB_IPaddress>*/3050:update loadbalancer=http://*<LB_IPaddress>*:9780**

ldss.properties

```
loadbalancer=http://<LB_IPaddress>:9780
```

Where:

- ***<DB_IPaddress>*** is the new database server IP address.
- ***<LB_IPaddress>*** is the new load balancer server IP address.

7 Navigate to the **C:/Program Files/Lexmark/Solutions/apps/printrelease/idm** folder, and then configure the following files:

idm-production-config,properties

```
idm.lddLoadBalancer=<LB_IPaddress>
```

database-production-config.properties

- **dataSource.url=*<DB_IPaddress>***
- **dataSource_webapp.url=*<DB_IPaddress>***

Where:

- ***<DB_IPaddress>*** is the new database server IP address.
- ***<LB_IPaddress>*** is the new load balancer server IP address.

8 Navigate to the **C:/Program Files/Lexmark/Solutions/apps/printrelease/lpm** folder, and then configure the following files:

app-production-config.properties

- **lddMobile.lddLoadBalancer=*<LB_IPaddress>***
- **jms.broker.url=*<LB_IPaddress>***

database-production-config.properties

- **dataSource.url=*<DB_IPaddress>***
- **dataSource_secondary.url=*<DB_IPaddress>***

webdav-production-config.properties

webdav.baseUri=*<LB_IPaddress>*

Where:

- ***<DB_IPaddress>*** is the new database server IP address.
- ***<LB_IPaddress>*** is the new load balancer server IP address.

9 Navigate to the **C:/Program Files/Lexmark/Solutions/apps/printrelease/mfpauth** file, and then update the following:

jdbc.url=*<DB_IPaddress>*

Where ***<DB_IPaddress>*** is the new database server IP address.

10 Stop all LDD and LPM services.

Cannot connect to database

If the connection to the database is tested during installation, then try one or more of the following:

Make sure that the database configuration is correct

Check the following settings:

- Database name
- Server and instance names
- Database server IP address
- Port number
- User name and password

Make sure that the user name has permission to view role membership

Make sure that the Java Database Connectivity driver is installed

Make sure that the user name role has read and write access

Make sure that the user name in the Microsoft SQL Server is mapped to the database specified in the Database Name field

Make sure that the database server is working correctly

Profile server is not responding

Make sure that all required Lexmark services on the LDD load balancer are running

1. From the LDD load balancer, navigate to:
   Settings > **Control Panel** > **Administrative Tools** > **Services**
2. Make sure that the following services are in a Started state:
   - Firebird Server - Default Instance
   - Lexmark Solutions Backup and Restore Agent
   - Apache2
   - Lexmark Solutions Apache Agent
   - Lexmark Solutions Web (or Protocol)
   - Adaptor
   - Lexmark Solutions License Manager

Make sure that Lexmark Solutions Application Server is running

Restart the Lexmark Solutions Application Server service on the LDD server.

LDSS server is busy

Try one or more of the following:

Make sure that the LDD server is online

For more information, see “Changing the status of the server” on page 48.

Make sure that the printer is discovered in Lexmark Management Console

For more information, see “Adding printers to a device group” on page 54.

Make sure that the printer is licensed

Make sure that the policies are updated

Perform a policy update when the server or printer IP address has changed. For more information, see the *Lexmark Document Distributor Administrator’s Guide*.

Unable to add new devices using LMC

Make sure that your printer has sufficient licenses

1. From LMC, click the **System** tab, and then select **Licenses**.
2. Check if the licenses of your printer are added on the server and are not expired.

   Note: If you have not purchased licenses or if the licenses are expired, then contact your Lexmark Technical Program Manager.

“Out of Policy” error message still appears even after multiple tries to update the policy

The licenses may not be configured to allow the number of devices in the group. Contact your Lexmark Technical Program Manager to determine the number of printers for which licensing was purchased.

“Unsupported Device” error message appears when installing a badge reader to the printer

Make sure that the appropriate driver is installed on the printer

If you do not know the driver that is required, then check another working printer in the environment or contact Lexmark Help Desk.

“Unable to Read Badge Data” error message appears when swiping the badge

Make sure the badge reader has the correct configuration file

If you do not know the required configuration file, then check another working printer in your environment or contact Lexmark Help Desk.

An error has occurred when swiping the badge

Make sure that the badge ID is registered to the Print Management Console

For more information, see “Badge” on page 103.

Restart the printer

The card reader may be having issues that require the printer to be restarted.

Print jobs submitted by the users do not appear in the print queue

Try one or more of the following:

Make sure that the user credentials are correct

If the Print Management server is configured to connect to an LDAP server, then use your LDAP user name and password.

If the Print Management server is configured to support multiple domain, then select a domain, and then type your user name and password.

For Microsoft Windows operating system, make sure that the Lexmark Universal Print Driver of your shared printer is installed on your computer and that the port is configured to the Print Management server

For more information, contact Lexmark Help Desk.

For Mac OS operating system software, make sure that the generic print driver is installed on your computer

For more information, contact Lexmark Help Desk.

Make sure that the document name and the user ID are correct and that the user is not logged in using a different user ID when printing

For more information, see “Print and Reprint Queues” on page 101.

Make sure that the badge ID is registered to the correct user ID

For more information, see “Badge” on page 103.

Page count is inaccurate

Make sure that the print jobs are not sent until they are finished spooling

1. From the printer folder, right-click your printer, and then click **Printer properties** or **Properties**.
2. Click the **Advanced** tab, and then select the following check boxes:
   - **Spool print documents so program finishes printing faster.**
   - **Start printing after last page is spooled.**
3. Click **OK**.

Note: Print Management page count tracking is for trending purposes only and is not designed for billing.

Cannot send jobs using e-mail

Make sure that EmailWatcher is installed

When you upgrade from LPM version 2.3.15 or earlier, the LDD installer removes EmailWatcher. To install EmailWatcher, run the LPM installer, and then select the e-mail component. For more information on installing LPM using a backup, see "Installing LPM using a backup file" on page 30.

An error occurs when updating policies

An error may occur when updating the policy for printers with keyboard reader, OmniKey, BadgeAuth2, or AP Bundle installed.

Increase the Timeout per device value

1. From Lexmark Management Console, click the **Services** tab.
2. From the Services section, select **PolicyUpdate**.
3. In the Timeout per device field, enter **600**.
4. Click **Apply**.

An error occurs when deploying eSF applications

Increase the `Timeout` value

1. From the LDD server, navigate to the **C:\ProgramFiles\Lexmark\Solutions\apps\cdcl-rest-wrapper\WEB-INF\classes\META-INF** folder.
2. Using a text editor, open the **client_provided.properties** file.
3. Add the **`cdcl.ws.readTimeout=60000`** line.

Sample code

```
webservice.caesar2.clientId=LDDcdcl.ws.readTimeout=60000
millisecondshttp.timeout=30000
```

4. Save the file.
5. Restart the Lexmark Solutions Application Server service.
6. Update the policy.

An error occurs when saving long DBCS characters

Make sure that the characters do not exceed the maximum number

The following are the maximum number of characters for each database:

- Firebird—85
- Microsoft SQL Server—220

Reports are showing duplicate entries

Try one or more of the following:

Make sure that only one Lexmark Reports Aggregator Service is running

Stop other instances of the Reports Aggregator service in other load balancers.

Make sure that Device Usage and Print Release are configured correctly

Make sure that Device Usage and Print Release are not tracking simultaneously

If Device Usage is used to track print jobs, then from the Print Release application, in the Use Device Usage for Print Stats setting, select **Yes**.

An error occurs when validating a badge

If the **`Unable to connect to Web Server`** error message appears when attempting to validate a badge, do the following:

1. Verify that card validation settings have been migrated from Web Service to Identity Service or another validation method.
2. Configure the selected card validation method
3. Perform a policy update to apply the changes.

Note: Web services for MFPAuthService are no longer supported in LPM 2.14.2.0 and later.

Mobile device configuration troubleshooting

Job submission failed

Try one or more of the following:

Check the job status in the ActiveMQ queue

To access the ActiveMQ console, do the following:

1. Open a web browser, and then type **`http://`*`IPaddress`*`:8160/admin/`**, where ***`IPaddress`*** is the IP address of the load balancer.
2. Enter your credentials.

   Note: The default user name and password is **`admin`**.

Enable the ActiveMQ console

1. From your computer, navigate to the ***install-path*\ActiveMQ\conf** folder, where ***install-path*** is the installation path of ActiveMQ.
2. Using a text editor, open **activemq.xml**.

3 Toward the end of the file, uncomment the **`import resource`** line. For example, change it from **`<!--<import resource="jetty.xml"/>-->`** to **`<import resource="jetty.xml"/>`**.

3. Restart the ActiveMQ service.

4. Restart the lpm-portal web application using the Tomcat management console or restart the Tomcat service.

4 Save the file.

Check the log files

If an error occurs with mobile device submissions or e-mail job errors are encountered, check the log files. The files are saved on each of the document conversion servers except for the Email Watcher log file. The logging level is set to **`WARN`** by default. To change it to **`DEBUG`**, update the **log4j-config.groovy** file in the **apps\lpm\WEB-INF\classes** and **apps\idm\WEB-INF\classes** folders.

Log files from jobs submitted using AirPrint

- **\Lexmark\Solutions\tomcat\logs\idm.log** (Tomcat server)
- **\Lexmark\Solutions\tomcat\logs\lpm.log** (Tomcat server)
- **\Lexmark\Solutions\ActiveMQ\data\activemq.log** (Load balancer)

For jobs in pending status, navigate to the solutionInfo database, and then check the QUEUED_PRINT_JOB table for the Job_State_Reason column.

Tomcat server Lexmark solutions applications server service log file

The following log file contains processing information from the core Lexmark Print Management application and Tomcat service:

\Lexmark\Solutions\tomcat\logs\lsas.log

Load balancer Lexmark Email Watcher log file

The following log file contains processing information from the Lexmark Email Watcher service that runs in the Lexmark Print Management load balancer:

Note: For more information, see “Configuring Lexmark Email Watcher” on page 71.

\Lexmark\Solutions\EmailWatcher\logs*.log

Lexmark Management Console jobs and logs

1 From Lexmark Management Console, click the **System** tab.

2 From the System section, select **Jobs** or **Log**.

Do any of the following:

- To apply a filter, click **Filters**, and then configure the settings.
- To remove a previously applied filter, click **Reset Filter**.
- To filter the list view to only jobs in progress, in the Log State menu, select **Running**.
- To view all log entries that apply to a specific job, from the jobs list, click the task ID of a job.

  Note: The log is automatically filtered for the selected task ID.
- To stop a job, select the job, and then click **Stop Task**.

- To refresh the jobs list or logs, click **Refresh**.

  Note: To set the jobs list to refresh on a timed interval automatically, select the **Auto Refresh** option, and then select a time interval.
- To change the number of entries that appear, select a new value for the number of jobs or logs per page.
- To export the jobs list or logs in comma-separated values (CSV) format, click **Export Report**.
- To export the audit logs, click **Export Audit Log**. The following information is shown when exporting audit logs:
  - All attempts to log in to and log out from Lexmark Management Console
  - All attempts to change the active user name or password
  - Creation, modification, and deletion of user accounts, groups, and privileges
  - All attempts to modify the privileges of a user account
  - All attempts to modify the LDAP settings from Lexmark Management Console

Document conversion failed

Try one or more of the following:

Open the originally submitted document directly in the document conversion application, and then export it to type PDF-A

The supported document conversion applications do not convert some documents, or only partially convert some content of the original document into a PDF file. Documents with SmartArt, or external image or content references, may experience these issues. For mobile users who submit documents directly (not using e-mail) to Lexmark Print Management, no prompt appears that the document did not convert. The document does not appear in the user's mobile queue view or the Print Release Administrator Portal.

Adjust the number of documents that can be converted concurrently

By default, a document conversion server handles only three documents at a time because of a limitation in the third-party software that is used for conversions. Using a higher number of concurrent conversions may make conversions unstable. From each of the document conversion servers, do the following:

1. Navigate to the **%ProgramFiles%\Lexmark\Solutions\apps\wf-ldss\WEB-INF\classes** folder.

   Note: The path may be different for your installation.
2. Using a text editor, open the **OpenOfficeToPDFClass.properties** file with administrator privileges.
3. Set the **`officeToPDF.maxInstances`** value.

   Note: We recommend setting this value up to **5**. Specifying a higher number may cause errors when converting documents.
4. Save the file.
5. Restart Lexmark Solution Application Server in Windows Services.

Run Lexmark Solution Application Server as a user or as an interactive user

When you install a 32-bit version of Microsoft Office on a 64-bit version of Windows Server, the document conversion software may not respond. Do the following:

1. From your computer, run Component Services for 32-bit (**mmc comexp.msc /32**).
2. From Console Root, click **Component Services** > **Computers** > **My Computer** > **DCOM Config**.
3. Select the appropriate applications.
4. Right-click each of the applications, and then click **Properties**.
5. From the Identity tab, select **The interactive user** or **This user**.
6. Enter your credentials.

Submit a field escalation with the original document file and the log files

The files are saved on each of the document conversion servers except for the Email Watcher log file. The logging level is set to **WARN** by default. To change it to **DEBUG**, update the **log4j-config.groovy** file in the **apps\lpm\WEB-INF\classes** and **apps\idm\WEB-INF\classes** folders.

Log files from jobs submitted using AirPrint

- **\Lexmark\Solutions\tomcat\logs\idm.log** (Tomcat server)
- **\Lexmark\Solutions\tomcat\logs\lpm.log** (Tomcat server)
- **\Lexmark\Solutions\ActiveMQ\data\activemq.log** (Load balancer)

For jobs in pending status, navigate to the solutionInfo database, and then check the QUEUED_PRINT_JOB table for the Job_State_Reason column.

Tomcat server Lexmark solutions applications server service log file

The following log file contains processing information from the core Lexmark Print Management application and Tomcat service:

\Lexmark\Solutions\tomcat\logs\lsas.log

Load balancer Lexmark Email Watcher log file

The following log file contains processing information from the Lexmark Email Watcher service that runs in the Lexmark Print Management load balancer:

Note: For more information, see “Configuring Lexmark Email Watcher” on page 71.

\Lexmark\Solutions\EmailWatcher\logs*.log

Lexmark Management Console jobs and logs

1. From Lexmark Management Console, click the **System** tab.
2. From the System section, select **Jobs** or **Log**.

   Do any of the following:
   - To apply a filter, click **Filters**, and then configure the settings.
   - To remove a previously applied filter, click **Reset Filter**.
   - To filter the list view to only jobs in progress, in the Log State menu, select **Running**.

- To view all log entries that apply to a specific job, from the jobs list, click the task ID of a job.

  Note: The log is automatically filtered for the selected task ID.
- To stop a job, select the job, and then click **Stop Task**.
- To refresh the jobs list or logs, click **Refresh**.

  Note: To set the jobs list to refresh on a timed interval automatically, select the **Auto Refresh** option, and then select a time interval.
- To change the number of entries that appear, select a new value for the number of jobs or logs per page.
- To export the jobs list or logs in comma-separated values (CSV) format, click **Export Report**.
- To export the audit logs, click **Export Audit Log**. The following information is shown when exporting audit logs:
  - All attempts to log in to and log out from Lexmark Management Console
  - All attempts to change the active user name or password
  - Creation, modification, and deletion of user accounts, groups, and privileges
  - All attempts to modify the privileges of a user account
  - All attempts to modify the LDAP settings from Lexmark Management Console

An error occurs when submitting e-mail using mobile devices

Configure the properties files manually

If the document conversion software is added after installing Lexmark Print, then the **`Exception In Openofficetppdfclass. Openoffice Manager Is Not Initialized`** error may occur.

For more information on configuring the properties files for your document conversion software, see “Configuring document conversion software” on page 68.

Cannot add Lexmark Print Management to Lexmark Print

Try one or more of the following:

Make sure that the URL format of the Lexmark Print Management server is correct

For more information, see “Adding Lexmark Print Management to Lexmark Print” on page 70.

Make sure that the Lexmark Print Management server is online

1. From Lexmark Management Console, click **System** > **System Status**.
2. Select a server.
3. Click **Set Online**.

   Note: Before setting the server online, make sure that your printer has sufficient licenses. For more information on purchasing licenses, contact your Lexmark Technical Program Manager.

Make sure that you have installed the Lexmark Print .solution file

For more information, see “Configuring Lexmark Print” on page 63.

Make sure that all IP addresses and subnets are added to the Mobile Print software client group

For more information, see “Adding Lexmark Print to a software client group” on page 68.

Cannot authenticate from Lexmark Print

Try one or more of the following:

Make sure that the mobile solution is selected in Lexmark Management Console

Lexmark Print Management version 2.4 or later uses the LDAP information from Lexmark Print. For more information, see “Configuring Lexmark Print” on page 63.

Note: To maintain performance, solution settings are cached so that changes to the settings may not be available immediately. Settings may be cached every two to five minutes, and cannot be configured during that time.

Make sure that the LDAP settings are configured correctly

Note: For Lexmark Print Management version 2.4 or earlier, the LDAP information is in a property file.

Cannot print from mobile devices

Try one or more of the following:

Note: To maintain performance, solution settings are cached so changes to the settings may not be available immediately. Caching intervals may be from two to five minutes and cannot be configured.

Make sure that the Print Release directory is configured the same way as the PrintReleasev2 solution settings

1. From Lexmark Management Console, click the **Solutions** tab.
2. From the Solutions section, select **PrintReleasev2**.
3. From the Tasks section, select **Configuration**.
4. Check the following settings:
   - Directory for Print Jobs
   - Username for Print Job Directory
   - Password for Print Job Directory
5. Click **Apply**.

For more information on the settings, see “Solutions setting index” on page 171.

Make sure that the Print Release directory is configured the same way as the mobileprint solution settings

1. From Lexmark Management Console, click the **Solutions** tab.
2. From the Solutions section, select **mobileprint**.
3. From the Tasks section, select **Configuration**.

4 Check the following settings:
   - Print Release Directory
   - Print Release Username
   - Print Release Password

5 Click **Apply**.

For more information on the settings, see “Understanding the mobile and e-mail configuration data” on page 64.

Cannot start the ActiveMQ service

Make sure that the ActiveMQ port numbers are not used by other applications

The ActiveMQ service may not start or remain started if another application on the load balancer server also uses its port numbers. Identify the application that is using the ActiveMQ port numbers, and then either remove it or change the port number assigned to the application. The following port numbers are used by ActiveMQ:

- 8161 (web portal)
- 61616 (queue port number and the port number that JMS broker listens on)

An error message starting with `SLF4J` appears

Ignore the message

This message appears while starting the application with the batch file. This message has no impact on the application functionality.

An error occurred while acquiring the authentication code

Make sure that the configuration values are correct

1 Review the configuration values in the **`config_EmailWatcher.properties`** file.

2 Check if correct values are specified in the following:
   - Client ID
   - Client secret
   - Tenant ID
   - Redirect URI
   - Scopes

An error appears in the log file related to `GraphServiceException` in Email Watcher

Check the error message and the exception to identify the cause

The error can be caused by a connection problem, a lack of permissions for the service account to read or delete the mailbox, or other issues.

Sender did not receive confirmation mail

Make sure that the mobileprint parameters are correct

1. From Lexmark Management Console, click **Solutions** > **mobileprint**.
2. Make sure that the Confirmation Email from Address field has a valid email address.

Make sure that the email service parameters are correct

1. From Lexmark Management Console, click **Services** > **Email**.
2. Check if the information is valid in the following settings:
   - Email server host name / ip address
   - Password to log onto email server
   - User id to log onto email server

An error message on print job conversion occurred in LMC logs

Make sure that the parameters are correct

1. From Lexmark Management Console, click **Solutions** > **mobileprint** > **Configuration**.
2. iIn the Conversion Method field, select **MS Office and Open Office** or **Open Office Only**.

   Note: Make sure that MS Office and Open Office or Open Office Only is already installed in the LDD LPM server where the print job is located.

Lexmark Serverless Print Management 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** > **Log File**.
3. Analyze the log, and then resolve the problem.

Check the Lexmark Print Management Client log

To enable logging of the Lexmark Print Management Client events, modify the **Logger** element in the Lexmark Print Management Client configuration file.

For Windows operating system

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

For Mac OS operating system software

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

- 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.

Make sure to restrict public access to the application

1. From the Embedded Web Server, click **Settings** > **Security** > **Login Methods**.
2. From the Public section, click **Manage Permissions**.
3. Expand **Apps**, and then clear **Print Release**.
4. Click **Save**.

Make sure that Print Release is granted access control

When using either Cloud Authentication or Card Authentication, do the following:

1. From the Embedded Web Server, click **Settings** > **Security** > **Login Methods**.
2. From the Additional Login Methods section, click **Manage Permissions** beside the application.
3. Select a group, expand **Apps**, and then select **Print Release**.
4. Click **Save**.

Contact your Lexmark representative

Print Release prompts the user to log in

Make sure that the session access control is set to BadgeAuth

Jobs appear to be printing but no output are printed

Try one or more of the following:

Make sure that the B/W Print and Color Print settings are enabled

When using either Cloud Authentication or Card Authentication, do the following:

1. From the Embedded Web Server, click **Settings** > **Security** > **Login Methods**.
2. From the Additional Login Methods section, click **Manage Permissions** beside the application.
3. Select a group, and then expand **Function Access**.
4. Select **B/W Print** and **Color Print**.
5. Click **Save**.

Contact your Lexmark representative

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 Lexmark Serverless Print Management 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 Lexmark Print Management Client port number

A firewall may be blocking the communication between the printer and the workstation. Check the following:

- A non-Windows firewall is installed on workstations using the Windows operating system.
- A non-Mac OS firewall is installed on workstations using the Mac OS operating system software.

The default port number for the Lexmark Print Management Client is **9443**. For more information, contact your system administrator.

Make sure that the user is granted access to the computer where the Lexmark Print Management Client is installed

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

1. From the computer where the Lexmark Print Management Client 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**.

Make sure that Kerberos is configured in your printer

Contact your Lexmark representative

Jobs do not appear in document accounting

Make sure that Device Usage is configured correctly

Cannot retrieve jobs

Try one or more of the following:

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

For more information, contact your system administrator.

Remove the proxy settings used for your printer

For more information, contact your system administrator.

Make sure that the Lexmark Print Management Client and the printer are connected to the same network

For more information, contact your system administrator.

Make sure that the Lexmark Print Management Client 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 the Lexmark Print Management Client

For more information, contact your system administrator.

Make sure that Lexmark Print Capture Service and Lexmark Print Release Service are running when you access Print Release on the printer

When using a card to log in, make sure to use the user account with administrator privilege in Active Directory and the Lexmark Print Management Client

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. Click **Apply**.

Make sure that the time on the printer matches the time on the Kerberos KDC

Make sure that the password created for Certificate Authority is correct

For more information, contact your system administrator.

Make sure that the service account user name in Card Authentication and Print Release matches the user name in the Lexmark Print Management Client configuration file

For more information on configuring Card Authentication, see the *Card Authentication Administrator's Guide*.

Make sure that the HTTP or SSL port number in Print Release matches the port number in the Lexmark Print Management Client configuration file

Make sure that the user is granted access to the computer where the Lexmark Print Management Client is installed

1. From the computer where the Lexmark Print Management Client 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 domain group policy settings manage the 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**.

Contact your Lexmark representative

Loading the print jobs takes a long time

Try one or more of the following:

Make sure that the network switch is not set to half duplex

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 it stops communicating to a workstation.

Contact your Lexmark representative

Printing takes a long time

Try one or more of the following:

Make sure that the network switch is not set to half duplex

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 the Lexmark Print Management Client when using Mac computers

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 the Lexmark Print Management Client.

Contact your Lexmark representative

License error

Contact your Lexmark representative

Appendix

LPM function comparison by deployment options

Function	Lexmark Print Management On-Premises	Lexmark Cloud Print Management	Lexmark Cloud Print Management Serverless
Print Release			
Automatic user registration	✓	✓	✓
Submit jobs from the print driver (File > Print)	✓	✓	✓
Submit jobs from Lexmark Print	✓	✓	✓
Submit jobs from e-mail	✓	✓	✓
Submit jobs from Print Management Console	X	✓	X
Submit jobs using AirPrint	✓	X	X
Print and keep	✓	✓	X
Delete and Delete all	✓	✓	✓
Print job delegation	✓	✓	X
Color and monochrome print job identifier	✓	✓	✓
Automatic purge	✓	✓	✓
Set duplex default	✓	✓	✓
View jobs in print queue from Print Management Console	✓	✓	X
Add print jobs by drag-and-drop, and change the order of jobs in queue from Print Management Console	X	✓	X
Document accounting			
Browser-based	✓	✓	✓
Implement user quotas	✓	✓	X
Track print, copy, and scan activities, including embedded applications	✓	✓	✓
View reports	✓	✓	✓
Export data	✓	✓	✓
Graphical summary report	✓	✓	X

Files and services index

The following are the LPM files and services installed by each component:

Component	Load balancer	Application server	Database
Print Release	ActiveMQ	Print Release Solution	PR_tables[1,2,3,4,]
	Apache Config – httpd-lpm-pr-virtualhost-extension.conf	Print Release (web application)	MP_Printer table[2,3]
	Apache Config – httpd-lpm-portal-virtualhost-extension.con	MFPAuth (web application)	IDM tables[4]
	Apache Config - httpd-lpm-portal-config-extension.conf	ThirdPartyConfigTool	Admin portal tables[4]
	N/A	Liquibase	Queue Job tables[4]
	N/A	TIS files	Quartz tables[4]
	N/A	Document Conversion	N/A
	N/A	Mobile Solution	N/A
	N/A	.Net	N/A
	N/A	IDM (grails application)	N/A
	NA	Lpm-portal (grails application)	N/A
	N/A	Aggregator Report Service (springboot application)	N/A
	N/A	User Data Management Service	N/A
Email	EmailWatcher Service	Mobile Solution	N/A
	N/A	Document Conversion	N/A
	N/A	.Net	N/A
Mobile App	ActiveMQ	Mobile Solution	N/A
	Apache Config – httpd-lpm-mobile-virtualhost-extension.conf	Document Conversion	N/A
	Apache Config – httpd-lpm-portal-virtualhost-extension.conf	.Net	N/A
	Apache Config - httpd-lpm-portal-config-extension.conf	N/A	N/A
	N/A	IDM (grails application)	N/A
	N/A	Lpm-portal (grails application)	N/A

[1] Used for Print Release

[2] Used for e-mail

[3] Used for Lexmark Print application

[4] Used for AirPrint

Component	Load balancer	Application server	Database
AirPrint	ActiveMQ	Bonjour Service	N/A
	Apache Config– httpd-lpm-airprint-virtualhost-extension.conf	File Conversion	N/A
	Apache Config– httpd-lpm-airprint.conf	Lpm-portal (grails application)	N/A
	webdav\printer_icons	IDM (grails application)	N/A
	Apache Config – httpd-lpm-portal-virtualhost-extension.conf	Print Release Solution	N/A
	Apache Config - httpd-lpm-portal-config-extension.conf	N/A	N/A

[1] Used for Print Release

[2] Used for e-mail

[3] Used for Lexmark Print application

[4] Used for AirPrint

Solutions setting index

Setting	Can be local	Values	Description
Site	✓	<Any text string>	The descriptor for the name of the site tracked in a print job. Use this item only when the solution is used across customer locations.
User Authentication	✓	Provided by Device* Badge Badge with Database Lookup Badge with LDAP Lookup PIN with Database Lookup PIN with LDAP Lookup Userid Only Userid/Password Custom	The method used for authenticating user IDs. **Notes:** • If the BadgeAuth eSF or PKI/CAC application is installed and used, then set it to **Provided by Device**. • If the badges or PIN values are stored in the database tables, then the Database Lookup setting is used. • Use Active Directory or LDAP for LDAP options. • Userid/Password and Userid Only require users to enter their credentials on the printer control panel. • Custom refers to a custom authentication script.

* The default value of a setting.

Setting	Can be local	Values	Description
Alternate Badge Login	✓	Disabled Userid/Password* PIN with Database Lookup PIN with LDAP Lookup	An authentication method where the badges are the primary login and the users can enter their credentials manually. **Note:** If BadgeAuth eSF is installed, then this setting is not applicable.
Register New Badge Users	X	Disabled* Enabled	Lets users enter their LDAP credentials, if prompted, to register their badges for the first time. **Note:** If BadgeAuth eSF is installed, then this setting is not applicable.
Badge Prompt	X	<Any text string> Please Swipe Your Badge*	The message on the screen before the users enter their credentials. **Note:** If BadgeAuth eSF is installed, then this setting is not applicable.
Touchscreen - Job Release	✓	User selects from list* Print all jobs	Determines whether a user can browse and select a print job or print all jobs after authenticating. For more information on Touchscreen - Job Release, see “Automatic Print Release” on page 179.
Touchscreen - Print All	✓	Disabled* Enabled	Lets users select the Print All option. **Note:** This setting is applicable only to touch-screen printers.
Keypad Only - Job Release	✓	User selects from list* Print all jobs	Determines whether a user can browse and select a print job or print all jobs after authenticating.
Keypad Only - User Options*	✓	Print Only* Print and Delete	Lets users delete specific print jobs. **Note:** This setting is applicable only to non-touch-screen printers.
Keypad Only - Print All	✓	Disabled* Enabled	Lets users select all print jobs. **Note:** This setting is applicable only to non-touch-screen printers and when Keypad Only - Job Release is set to **User selects from the list**.
Job Display Order	X	Date Printed (Descending)* Date Printed (Ascending)	The order of print jobs.
Job Print Order	X	Date Printed (Descending)* Date Printed (Ascending)	The order of released print jobs.
Directory for Print Jobs	X	<Any network or local path> c:\lexmark\printrelease*	The location where print jobs are held or saved.
* The default value of a setting.			

Setting	Can be local	Values	Description
Username for Print Job Directory	**X**	<Any text string>	The name of the user with read and write privileges to the directory specified in Directory for Print Jobs. **Note:** If a domain account is used, then the user name format is **<domain; user name>**.
Password for Print Job Directory	**X**	<Any text string>	The password of the user with read and write privileges to the directory specified in Directory for Print Jobs.
Directory for Encrypted Print Jobs	**X**	<Any network or local path> c:\lexmark\printrelease*	The location where encrypted print jobs are saved. The administrator uses PrintCryption™ or smart cards to encrypt the print jobs.
Job Encryption Method	**X**	Device Certificate* User Certificate	The certificate used to decrypt encrypted print jobs before the jobs are released. • If PrintCryption is used, then select **Device Certificate**. • If smart cards are used, then select **User Certificate**.
Delete Unprinted Jobs After Specified Hours	**X**	1–336 10*	The number of hours before a print job is deleted.
Delete Printed Jobs After Specified Hours	**X**	1–24 0*	The number of hours before a released and kept job for reprinting are deleted. **Notes:** • Any value from **1** to **24** enables reprinting. • Specifying **0** disables reprinting.
Function Access	**X**	Disabled* By Userid By Group	Determines whether a user or a group can access certain printer functions.
User Quotas	**X**	Disabled* By Userid By Group	The number of jobs a user or group is allowed to print and copy.
Quota Duration	**X**	Monthly* Yearly	Determines whether quotas are measured on a monthly or yearly basis.
Default User Total Quota	**X**	<Any positive integer> 0*	The initial number of pages a user is allowed to print or copy.
Default User Color Quota	**X**	<Any positive integer> 0*	The initial number of pages a user is allowed to print or copy in color.
Default User Allow Color	**X**	Yes* No	Lets users print in color.

* The default value of a setting.

Setting	Can be local	Values	Description
Quota for Group Members	X	By Group* By User	Determines whether an administrator can override the quotas for individual users or all users in a group. **Note:** This setting is applicable only when User Quotas is set to **By Group**.
Show Copy Quota Remaining	X	Never* Before Copy Job After Copy Job	Notifies users of their remaining number of times to copy.
Reset Quotas	X	Reset All Totals* Remove All Users	Determines whether the quotas are reset or the users are removed from the quota table. **Note:** This setting is applicable only when the ResetQuotas script is configured.
Quota Overage	X	Disabled* Enabled	Lets users exceed their allotted print and copy quota.
Alternate Release Locations	X	Disabled* Enabled	Lets users release a job from another printer.
Enable Printing from Unix/Novell	X	Yes No*	Lets users perform advanced processing of the incoming jobs released from a print queue in a UNIX, Linux, OS X, or Micro Focus (formerly known as Novell) software environment.
LDAP Multi-Domain Support	X	Disabled* Enabled	Lets the printer accept multiple domain configurations, so that users in different domains can use the printer.
LDAP Server	X	<Any text string>	The LDAP server used for authentication.
LDAP Port	X	389* 636 3268 3269	The port number used by the LDAP server. • 389 is the standard LDAP port. • 636 is the standard LDAP port with SSL. • 3268 is the Global Catalog. • 3269 is the Global Catalog with SSL.
LDAP Use SSL	X	Yes No*	Lets LPM use SSL when querying LDAP.
LDAP Login Username	X	<Any text string>	The user ID used to log in to the LDAP server.
LDAP Login Password	X	<Any text string>	The password used to log in to the LDAP server.
LDAP Userid Type	X	Principal Name* Distinguished Name	The user ID format used for LDAP login credentials.

* The default value of a setting.

Setting	Can be local	Values	Description
LDAP Principal Domain	X	<Any text string>	The domain name used in LDAP. **Note:** The domain name is used when LDAP Userid Type is set to **Principal Name**.
LDAP Search Base	✓	<Any text string>	The LDAP search base used with LDAP queries.
LDAP Use Advanced Config File	X	Yes No*	The LDAP system requires LDD to use an advanced configuration file.
LDAP Userid Attribute	X	<Any text string>	The name of the LDAP field containing the user IDs.
LDAP Badgeid Attribute	X	<Any text string>	The name of the LDAP field containing the badge numbers. **Note:** This setting is required when User Authentication is set to **Badge with LDAP Lookup**.
LDAP PinID Attribute	X	<Any text string>	The name of the LDAP field containing the PIN numbers. **Note:** This setting is required when User Authentication is set to **PIN with LDAP Lookup**.
LDAP Email Attribute	X	<Any text string> mail*	The name of the LDAP field containing the users' e-mail addresses. **Note:** This setting is required when any of the advanced e-mail features is used.
LDAP Home Directory Attribute	X	<Any text string> homeDirectory*	The name of the LDAP field containing the users' home directories. **Note:** This setting is required when the Scan to Network profile and destination settings are configured in User's Home Directory.
LDAP Custom Attribute 1	X	<Any text string>	Lets you specify more LDAP attributes in tracked usage data.
LDAP Custom Attribute 2			
LDAP Custom Attribute 3			
Copy - Return to Copy Screen	X	Yes No*	Returns users to the copy home screen after completing a copy job.
Copy - Warning Threshold	X	0–999 999*	The number of copies that a user is required to confirm before the copy job is released. **Note:** Specifying **0** disables this setting.

* The default value of a setting.

Setting	Can be local	Values	Description
Copy - Copy Center Threshold	X	<Any integer> 0*	The number of pages allowed on a single copy job. **Note:** If the number of pages exceeds the maximum, then a prompt appears informing users to use Copy Center. Users cannot proceed with the copy job.
Copy Center Error Message	X	<Any text string> This job is too large to be processed on this device. It must be sent to the Copy Center.*	The message shown when the number of pages exceeds the maximum number of pages set in Copy - Copy Center Threshold.
Email - From Source	X	LDAP* Database Device	The source of e-mail addresses to use when sending an e-mail from a printer. **Notes:** • LDAP and Database use the user's e-mail address. • The printer uses the e-mail address configured in the printer e-mail settings.
Email - User can only send to self	X	Yes No*	Lets users send e-mail only to themselves.
Email - Send User a copy	X	Yes* No	Lets users receive a copy of released e-mail jobs.
Email - Track Destination	X	Yes No*	Tracks recipient e-mail addresses after completing an e-mail job.
Email - Send Thru	X	MFP* Server	Determines whether e-mail jobs are sent from the printer or an LDD server.
Email - Return to Email Screen	X	Yes No*	Returns users to the e-mail home screen after completing an e-mail job.
Email - Maximum Attachment Size	X	<Any integer> 0*	The maximum size of the file (in megabytes) a user can attach to an e-mail. **Notes:** • Specifying **0** disables this setting. • If the size of the file exceeds the maximum, then the user cannot proceed with the e-mail job.
Email - Maximum Size Error Message	X	<Any text string> The attachment exceeds the maximum allowed size set by your e-mail system; the e-mail cannot be sent.*	The message shown when the size of the file exceeds the maximum size set in Email - Maximum Attachment Size.

* The default value of a setting.

Setting	Can be local	Values	Description
Fax - Track Destination	X	Yes No*	Tracks fax destination numbers after completing a fax job.
Use Database Table for Fax	X	Yes No*	Uses the newly added database named PR_FAX table. This setting is used for the Fax feature of the printer. The Database lookup initiates only if the Use Database Table for Fax setting is set to **Yes**. In Fax Server, it first looks up in the Database for the sender's reply address. If it cannot be found, then the server initiates an LDAP lookup. If the user is not found during LDAP lookup as well, then there is no reply address. In Fax Analog, it first looks up in the Database for the sender's fax number. If it cannot be found, then the server initiates an LDAP lookup. Unlike Fax Server, Fax Analog involves an Embedded Web Server lookup in the printer if the user is not found during LDAP lookup. If it still cannot be found, then there is no reply address. For more information on setting up Embedded Web Server in printer for Fax Analog, see "Setting up Embedded Web Server for Fax Analog" on page 179. **Note:** The administrator manually populates the PR_FAX table using Firebird or Microsoft SQL Server.
Scan to Network - Destination	X	User's Home Directory* File Share File Share + Userid File Share + LDAP Attribute Database Lookup	The type of destination path when scanning to a network.
Scan to Network - File Share	✓	<Any network or local path>	The destination path of the file share options set in Scan to Network - Destination.
Scan to Network - Subfolder	X	<Any text string>	The subfolder of the network destination.
Scan to Network - Create Directory	X	No* Yes - Create Only Yes - Create and Set Permissions	Creates a directory automatically when the destination path specified by the user does not exist.
Scan to Network - Authentication	X	User Service Account* Prompt User for Password	The printer authentication type when scanning to a network.
Scan to Network - Domain	X	<Any text string>	The network domain used when scanning to a network.

* The default value of a setting.

Setting	Can be local	Values	Description
Scan to Network - Userid	**X**	<Any text string>	The name of the user who sends the job to a network. **Note:** This setting is applicable only when Scan to Network - Authentication is set to **Use Service Account**.
Scan to Network - Password	**X**	<Any text string>	The password of the user who sends the job to a network. **Note:** This setting is applicable only when Scan to Network - Authentication is set to **Use Service Account**.
Scan to Network - Default Filename	**X**	<Any text string> scan*	The name of the document sent to a network.
Scan to Network - Append Timestamp	**X**	Yes* No	Appends the date and time to a document when sent to a network.
Scan to Network - Prompt to Scan More	**X**	Yes No*	Prompts users to scan more documents after completing the Scan to Network job. **Note:** To let users return to the Scan to Network home screen, select **No**. If **Yes** is selected, the SCAN ANOTHER FILE? option appears.
Track Device Hostname	**X**	Yes* No	Records the printer host name or IP address with the usage data.
Print - Duplex Check for Page Counts	**X**	Disabled Enabled*	Checks print jobs to make sure that duplex jobs are accounted for correctly.
Print File Operations	**X**	Use Standard Method* Use Alternate Method	The method for saving files. **Notes:** • If the standard method is used, then specify FileClass (jcifs). • If the alternate method is used, then specify TISFile.
Use Device Usage for Print Stats	**X**	Yes No*	Uses the printer to track print jobs. **Note:** To prevent LDD from recording print jobs to the usage data, select **Yes**.
User Server Time for Device Usage	**X**	Yes No*	Uses the printer time for usage data. **Note:** To use the LDD server time for usage data, select **Yes**.
Job Separator	√	Disabled* Enabled	Places a sheet of paper between pages.
Show Print Status	**X**	Disabled Enabled*	Shows a status message on the printer display when printing a job.

* The default value of a setting.

Setting	Can be local	Values	Description
PJL User Info Key	✓	<Blank> @PJL LJOBINFO USERID <Other PJL strings for user ID>	The alternate method for assigning the user ID for a print job. **Note:** If not specified, then the user ID is taken from the JOB_INFO_2 structure of the port monitor.
Log Information	X	Disabled* Enabled	Shows detailed logging in the Lexmark Management Console log.
* The default value of a setting.			

Automatic Print Release

Automatic print release is an organizational setting that lets users release their print jobs automatically after logging in. This setting prevents users from interacting directly with the printer when releasing print jobs. If enabled, then this setting controls all print jobs in the queue from various sources.

1. From Lexmark Management Console, click the **Solutions** tab.
2. From the Solutions section, select **PrintReleasev2**.
3. From the Tasks section, select **Configuration**.
4. From the Configuration (PrintReleasev2) section, in the Touchscreen - Job Release menu, select **Print all jobs**.
5. Click **Apply**.

   Note: After completing these steps, launch Print Release in the printer panel to print all jobs automatically.

Note: Use automatic print release for Card Authentication by configuring the application to set Login Profile to **Print Release**. For more information on configuring eSF application, see "Configuring BadgeAuth and CardAuth" on page 180.

Setting up Embedded Web Server for Fax Analog

1. From the Embedded Web Server, click **Settings** > **Fax**.
2. In the Fax Defaults section, set Fax Mode to **Analog**.
3. Click **Analog Fax Setup**.
4. In the Fax Cover Page section, type the fax number of the sender in the From field.
5. Click **Save**.

Configuring eSF applications settings for Print Release

The following eSF applications are frequently used with the LDD Print Release solution. For more information on the supported eSF application versions, see “Supported Embedded Solutions Framework (eSF) applications” on page 9.

Note: When configuring the badge reader driver, we recommend using the default values.

Configuring BadgeAuth and CardAuth

Configuring BadgeAuth and CardAuth

Depending on the printer model, the BadgeAuth and CardAuth eSF applications require different versions. The installation and configuration of the applications also vary by printer model.

eSF application and version	Supported printers
CardAuth version	e-Task 5
BadgeAuth version	e-Task 4 and e-Task 3
BadgeAuth version	e-Task 2 (Not supported)

Note: For more information on the supported printer models, see “Supported printer models” on page 24.

Understanding the CardAuth version 5 configuration data for e-Task 5 printers

To prevent errors during deployment, do the following:

- Make sure that the existing CardAuth application is running during the upgrade.
- When applicable, configure the following:
  - User authentication settings
  - Web Service settings
  - Identity Service Provider settings
  - PIN settings
  - LDAP settings
  - LDAP Server Setup
  - LDAP Attributes
  - Login Screen settings
  - Lock Screen settings
  - Custom Profile
  - Advanced Settings

User authentication settings

Setting	Description
Card Validation	This setting determines how cards are validated. **Possible values** • Printer-based • Web Service (for LPM On-Premises) • LDAP • Identity Service
Card Registration	The login method for registering using cards. If this setting is not specified, or if the text does not match the printer security settings, then this setting is set to Disabled.
Manual Login	The login method for logging in manually. If this setting is not specified, or if the text does not match the printer security settings, then this setting is set to Disabled.
Realm	The location of the user account. Configure this setting when using Active Directory, Kerberos, or LDAP+GSSAPI.
Admin Login	The login method for the administrator login. 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, some functions, and administrative and device management menus are permitted for this group. However, this setting is disabled by default.
Authorized Group	The group that can use the administrator login feature. This feature is applicable only to user name, and user name and password accounts.
Show on Screen Saver	Shows the Admin Login button on the screen saver.

Web Service settings

If Card Validation is set to Web Service, then the following are used to communicate to the web server:

Note: These settings also determine the Web Service call version for user authentication.

Setting	Description
Server URL	The web service address used to register and to validate the badge ID. **Notes:** • From LPM 2.14.2.0 onwards, MFPAuthService is no longer supported. Web Service can still be used with a custom web server for badge validation and registration. • Identity Service is the recommended card validation method.
Timeout (seconds)	The timeout in seconds used for connecting to the web service. The default value is **15** seconds. To disable the timeout, set the value to **0**.

Setting	Description
Registration Interface	**Possible values** • Version 2 • Version 1 The default value is Version 1. Version 2 adds tracking to the IP address and host name of the printer used to register the badge. **Note:** Version 2 is applicable only to Print Release version 2.3 or later.
Lookup Interface	**Possible values** • Version 2 • Version 1 The default value is Version 1. Version 2 adds tracking to the last time the badge is used and from what printer. **Note:** Version 2 is applicable only to Print Release version 2.3 or later.

Configuring the Identity Service settings

1. From the Embedded Web Server, navigate to the configuration page for the application.
2. From the User Authentication section, set Card Validation to **Identity Service**.
3. From the Identity Service Settings section, set the identity service provider address to **`https://serverIP/idm`**, where ***`serverIP`*** is the IP address of the LPM server.
4. If the LPM server is configured with SSL, then set the badge service provider address to either of the following:
   - **`https://serverIP/lpm`**
   - **`https://serverIP:9780/lpm`**

   Where ***`serverIP`*** is the IP address of the LPM server.
5. Set Client ID to **`esf-cardauth-app`**.

   Note: You can update the client ID.
6. Set Client Secret with the value from ***<install-Dir>*****\Lexmark\Solutions\apps\idm\WEB-INF\classes\idm-production-config.properties** file, where ***<install-Dir>*** is the installation folder of LDD.

   Note: You can update the client secret.
7. Set Card Registration to **Identity Service**.
8. Set Manual Login to **Identity Service**.
9. Click **Save**.

PIN settings

Setting	Description
PIN Validation	Triggers PIN validation using LDAP or a web service. **Note:** LDAP validation is applicable only when Required Credentials is set to PIN Only.
Required Credentials	Determines whether the following are required when a user logs in to the printer: • Userid and PIN • PIN Only
PIN Registration/Update	Authenticates the user account before registering or updating the PIN. When disabled, this setting does not allow PIN registration or PIN update. If this setting is not specified, or if the text does not match the printer security settings, then this setting is set to Disabled.
Web Server Address	The server address where PIN is stored. Use the following format for its value: **`https://LBaddr/api/1.0`** Where ***`LBaddr`*** is the host name or IP address of the LDD load balancer server. **Note: `1.0`** is used for the LPM server to determine whether the Card Authentication PIN feature is used.
PIN Login Text	The custom message in the PIN Login screen. The minimum number of characters is 0, and the maximum number of characters is 100.
Minimum PIN Length	The minimum required PIN length for registration or update. The default value is **`4`**, but the supported range of value is from **`4`** to **`16`**. Make sure that the value is consistent with the LPM administrator portal PIN settings.
Invalid PIN Length Error Message	The custom error message that appears when the PIN entered does not meet the PIN length requirement during PIN registration or update. The minimum number of characters is 0, and the maximum number of characters is 256.
Invalid PIN Error Message	The custom error message that appears when an invalid PIN is entered. The minimum number of characters is 0, and the maximum number of characters is 256.
Network Timeout	The length of time before connection with the server is established. The default value is **`15`**, but the supported range of value is from **`0`** to **`30`**. To disable the timeout, set the value to **`0`**.
Socket Timeout	The length of time before response data from the server is received. The default value is **`15`**, but the supported range of value is from **`0`** to **`30`**. To disable the timeout, set the value to **`0`**.
PIN Notification	When a user registers, this setting lets you show the PIN on the printer display, e-mail it to the user, or both.

LDAP settings

Setting	Description
Use Address Book	Uses the LDAP settings configured in Address Book. For printers running on eSF version 5 or later, the LDAP settings in Network Accounts are used. If there are multiple network accounts, then the first in alphabetical order is selected. **Notes:** • To access Network Accounts, access the Embedded Web Server, and then click **Settings** > **Security** > **Network Accounts**. • This setting is used only when Card Validation is set to LDAP, or when other user information attributes are necessary.

LDAP Server Setup

Setting	Description
Server Address	The host name or IP address of the LDAP server.
Server Port	The port number used to communicate with the LDAP server. **Common possible values** • 389 (non-SSL) • 636 (SSL) • 3268 (non-SSL Global Catalog) • 3269 (SSL Global Catalog)
Use SSL	Uses SSL for communication.
Search Base	The directory where the LDAP search begins.
Login Username	The service account name used for logging in to the LDAP server. If this setting is not specified, then anonymous bind is performed.
Login Password	The service account password used for logging in to the LDAP server.

LDAP Attributes

The following LDAP attributes must be specified:

Setting	Description
User ID	The user's Windows user ID. For Active Directory, this setting corresponds to **samaccountname**.
Badge ID	The user's badge ID. This setting is used only when Card Validation is set to LDAP.
User Information	A comma-separated list of user attributes. This list is queried after the user has authenticated.
Group Membership Attribute	The groups where the user is a member of.
Group List	The groups shown in Manage Permission where the administrator can define permissions at a group level. If multiple groups are used, then the group names must be comma-separated.
User PIN	The LDAP attribute where the PIN validation is looked up against.

Login Screen settings

The following settings determine how the login screen is shown to the user:

Setting	Description
Use Custom Login Text	Shows the custom login text. To avoid redundancy, disable this setting when the text is included in the login screen image.
Custom Login Text	The text shown on the login screen. If this setting is not specified, then the default text is used.
Text Color	The color of the custom login text. **Possible values** • White • Black To maximize usability, select a color that contrasts with the color of the login screen image.
Use Custom Image for Login Screen	Uses the custom image background on the login screen.
Login Screen Image	The image shown on the login screen. The image can be in a GIF, PNG, or JPG format that is 800 x 480 pixels and does not exceed 100KB. If this setting is not specified, then the default image is used.
Manual Login Text	The text shown on the login screen for manual login. If this setting is not specified, then the default text is used. The minimum number of characters is 0, and the maximum number of characters is 100.
Allow Copy Without Login	Lets users perform a copy job without authenticating. **Note:** This setting is applicable only to printers that support the copy function.
Allow Fax Without Login	Lets users perform a fax job without authenticating. **Note:** This setting is applicable only to printers that support the fax function.

Lock Screen settings

The following settings determine how the lock screen is shown to the user:

Setting	Description
Text Location	The location of the login text on the lock screen. **Possible values** • Top • Middle • Bottom
Login Profile	The profile that is launched automatically after a successful login. **Possible value** Print Release

Custom Profile settings

Setting	Description
Name or ID	The application or printer function that users can access from the lock screen. The application name is case sensitive.
Icon Text	The custom name for the icon that is shown on the lock screen.
Use Custom Icon	Shows the custom icon.
Icon upload field	The custom icon image that is shown on the lock screen for Custom Profile. The image can be in a GIF, PNG, or JPG format that is 140 x 140 pixels and does not exceed 40KB.

Advanced Settings

Setting	Description
Badge Logout Delay (seconds)	The length of time before the printer registers a succeeding tap as a logout. The default value is **2**. To disable the timeout, set the value to **0**. The minimum time in seconds is **0**, and the maximum time in seconds is **10**.
Use Selected Realm	Adds the selected realm during registration and when users log in manually. For example, userid@realm. The feature is applicable only if the login methods for card registration and manual login are Kerberos, Active Directory, or LDAP+GSSAPI. 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. **Note:** This setting is not applicable when logging in or registering using a PIN.
Enable Beep for Successful Login	Enables a sound when the badge reader reads a badge successfully.
Beep Frequency	The sound frequency of the printer beep when a badge is read successfully. The default value is **2000**. The minimum frequency in Hertz is **0**, and the maximum frequency in Hertz is **65535**.

Understanding the BadgeAuth version 2 configuration data for e-Task 4 and e-Task 3 printers

Login Screen settings

The following settings determine how the login screen is shown to the user:

Setting	Description
Background Transparency	Determines the transparency of the banner background.
Display Login Text	Shows the custom login text. To avoid redundancy, disable this setting if the text is included in the login screen image.
Login Screen Text	The text shown on the login screen. If this setting is not specified, then the default text is used.
Login Screen Image	The image shown on the login screen. The image must be in GIF format that is 800 x 320 pixels and does not exceed 40KB. If this setting is not specified, then the default image is used.

Setting	Description
Login Method	Determines how users can log in to the printer. **Possible values** • Card Only • Card or Manual Login • Manual Login Only • PIN Only • Card or PIN Login • PIN or Manual Login • Card, PIN or Manual Login **Note:** If a badge is not available, then Manual Login lets users enter their credentials.
Allow Copy without Login	Lets users perform a copy job without authenticating. **Note:** This setting is applicable only to printers that support the copy function.
Allow Fax without Login	Lets users perform a fax job without authenticating. **Note:** This setting is applicable only to printers that support the fax function.
Custom Profile	The application or printer function that users can access from the lock screen. The application name is case-sensitive.
Icon Text	The custom name for the image on the lock screen.
Icon	The image shown on the lock screen. The image must be in GIF that is 120 x 75 pixels.
Icon when Pressed	The image shown while the icon on the lock screen is pressed. The image must be in GIF that is 120 x 75 pixels.
Login Text Placement	The location of the login text. **Possible values** • Above the Icon • Below the Icon
Icon or Text Placement	The location of the text or icon. **Possible values** • Top • Middle • Bottom

User authentication settings

Setting	Description
Card Validation	Determines how cards are validated. **Possible values** • None • LDAP • Web Service • Identity Service **Note:** Selecting **None** lets all users with valid card use the printer.

Setting	Description
Card Registration Access Control	Determines the access control that is used for card registration. **Note:** Select **None** to restrict all users from registering their badge at the specific printer. To configure access controls, do the following: **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**. • Click **Security** > **Edit Security Setups** > **Access Controls**. **3** Click **Device Apps** or **Device Solutions**, and then set the functions to the appropriate LDAP building block and security template. **4** Click **Submit**. For more information on configuring access controls, see the *Card Authentication Administrator's Guide*.
Manual Login Access Control	Determines the access control that is used for manual login. The access control configuration for this method is the same as Card Registration Access Control. **Note:** Selecting **None** allows users to log in without a badge.
Session Access Control	Determines the access control that is used for a user's session data. Another printer function, such as Copy, may be set to the same access control, and then get the user information. Select the solution or application number that corresponds to the BadgeAuth or CardAuth security template that is defined when creating an access control.
Admin Login Access Control	Determines the access control that is used to authenticate administrators. **Note:** Selecting **Disabled** prevents the Admin Login button from appearing on the lock screen.

Advanced Settings

Setting	Description
Show Registration Intro Message	Prompts users to register their badge before prompting them to enter their user ID. If disabled, then this setting prompts users to enter their user ID automatically.
Show Registration Finished Message	Informs users whether the badge registration is successful before redirecting them to the printer home screen. If disabled, then this setting redirects users to the home screen automatically.
Enable Beep for Successful Login	Enables a sound when the badge reader reads a badge successfully.
Beep Frequency	The sound frequency of the printer beep when a badge is read successfully.
Login Profile	The profile that is launched automatically after a successful login.
Use Selected Realm	Adds the selected realm during registration and when users log in manually. For example, userid@realm. The feature is applicable only if the login methods for card registration and manual login are Kerberos, Active Directory, or LDAP+GSSAPI. 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 username shown in the printer control panel is in username@realm format. **Note:** This setting is not applicable when logging in or registering using a PIN.

Web Service settings

If Card Validation is set to Web Service, then the following are used to communicate to the web server:

Note: These settings also determine the Web Service call version to use for user authentication.

Setting	Description
Server URL	The web service address used to register and to validate the badge ID. **Notes:** • From LPM 2.14.2.0 onwards, MFPAuthService is no longer supported. Web Service can still be used with a custom web server for badge validation and registration. • Identity Service is the recommended card validation method.
Registration Interface	Determines the Web Service call version to use for badge registration. **Possible values** • Version 2 • Version 1 The default value is Version 1. Version 2 adds tracking to the IP address and host name of the printer used to register the badge. **Note:** Version 2 is applicable only to Print Release version 2.3 and later.
Lookup Interface	Determines the Web Service call version to use for badge lookup. **Possible values** • Version 2 • Version 1 The default value is Version 1. Version 2 adds tracking to the last time that the badge is used and from what printer. **Note:** Version 2 is applicable only to Print Release version 2.3 and later.

Configuring the Identity Service settings

1. From the Embedded Web Server, navigate to the configuration page for the application.
2. From the User Authentication section, set Card Validation to **Identity Service**.
3. From the Identity Service Settings section, set the identity service provider address to **`https://serverIP/idm`**, where ***`serverIP`*** is the IP address of the LPM server.

4 If the LPM server is configured with SSL, then set the badge service provider address to either of the following:

- **`https://serverIP/lpm`**
- **`https://serverIP:9780/lpm`**

Where ***`serverIP`*** is the IP address of the LPM server.

5 Set Client ID to **`esf-cardauth-app`**.

Note: You can update the client ID.

6 Set Client Secret with the value from ***<install-Dir>*****\Lexmark\Solutions\apps\idm\WEB-INF\classes\idm-production-config.properties** file, where ***<install-Dir>*** is the installation folder of LDD.

Note: You can update the client secret.

7 Set Card Registration to **Identity Service**.

8 Set Manual Login to **Identity Service**.

9 Click **Save**.

PIN settings

Setting	Description
Web Server Address	The server address where the PIN is stored. Use the following format for its value: **`https://LBaddr/api/1.0`** Where ***`LBaddr`*** is the host name or IP address of the LDD load balancer server. **Note: `1.0`** is used for the LPM server to determine whether the Card Authentication PIN feature is used.
Minimum PIN Length	The minimum required PIN length for registration or update. The default value is **`4`**, but the supported range of values is from **`4`** to **`16`**. Make sure that the value is consistent with the LPM administrator portal PIN settings.
Invalid PIN Length Error Message	The custom error message that appears when the PIN is entered does not meet the PIN length requirement during PIN registration or update. The minimum number of characters is 0, and the maximum number of characters is 256.
Invalid PIN Error Message	The custom error message that appears when an invalid PIN is entered. The minimum number of characters is 0, and the maximum number of characters is 256.

LDAP settings and LDAP Server Setup

Setting	Description
Use Address Book	Uses the LDAP settings configured in Address Book. The LDAP settings must be specified for single-function printers.
Server Address	The host name or IP address of the LDAP server.

Setting	Description
Server Port	The port number used to communicate with the LDAP server. **Common possible values** • 389 (non-SSL) • 636 (SSL) • 3268 (non-SSL Global Catalog) • 3269 (SSL Global Catalog)
Use SSL	Uses SSL for communication.
Search Base	The directory where the LDAP search begins.
Login username	The service account name used for logging in to the LDAP server. If this setting is not specified, then anonymous bind is performed.
Login Password	The service account password used for logging in to the LDAP server.

LDAP Attributes

The following LDAP attributes must be specified:

Setting	Description
User ID	The user's Windows user ID. For Active Directory, this setting corresponds to **samaccountname**.
Badge ID	The user's badge ID. This setting is used only when Card Validation is set to LDAP.
User Information	A comma-separated list of user attributes. This list is queried after the user has authenticated.

Home Screen settings

The following settings determine how BadgeAuth interacts with the printer home screen after a user has logged in:

Setting	Description
Display username	The format of the username. **Possible values** • None—The username is not shown. • Userid—The user ID that is associated with the badge is shown. • cn—The cn LDAP attribute for the user is looked up, and then shown. • givenName + sn—The givenName and sn LDAP attributes for the user are looked up, and then shown. These attributes are usually the first and last names of the user. **Note:** The User ID LDAP attribute must match the results of the badge lookup.
Username Format	If Display username is set to **None**, then this setting determines how the format of the username is shown in the status window. Type **%u** for the username.
Use Home Screen Logout	Shows an icon for logging out on the printer home screen.
Badge Logout Delay	The length of time in seconds before the printer registers a succeeding tap as a logout. The default value is **2** seconds.

Configuring Device Usage

The Device Usage eSF application does not require a license. The following shows the configuration data for Device Usage for use with the LDD Print Release.

Notes:

- To avoid duplicate entries in the database for a single transaction, make sure that Device Usage and Print Release are not tracking simultaneously.
- The IP addresses of devices need to be added to the software client groupDevice Usage to be able to report information to LPM.

eSF application and version	Supported printers
Device Usage version 1.10	e-Task 5, e-Task 4, and e-Task 3
Device Usage version 1.6	• e-Task 2 • (Not supported)

Note: For more information on the supported printer models, see "Supported printer models" on page 24.

Understanding the Device Usage version 1.10 configuration data for e-Task 5, e-Task 4 and e-Task 3 printers

Setting	Description
Site ID	The site ID that the printer uses for reports. If this setting is not specified, then the default site code in LDD is used.
Server Type	Determines the server type that the usage data is being reported to. **Possible values** • **Web Service**—A generic web service that implements the Device Usage Web Service specification • **LDD**—An LDD server that is configured to receive device usage statistics
Server URL	The text shown on the login screen. If this setting is not specified, then the default text is used. This setting is the URL used to send data to the server. Use the following format for the LDD Server Type value: • **`http://LBaddr:9780`** • **`https://LBaddr`** Where ***`LBaddr`*** is the host name or IP address of the LDD load balancer server.
Track Copy	When enabled, copy jobs on the printer are tracked. We recommend this method for tracking copies when Print Release quotas are not used. If quotas are enabled, then LDD tracks copy jobs and the Track Copy setting must not be enabled. **Note:** During the Copy or Copy Cancel workflow, the Track Copy and Track Copy Cancel settings must not be enabled at the same time on a printer. Enabling these settings together causes duplicate entries in the PR_STATS report.

Setting	Description
Track Copy Cancel	When enabled, canceled copy jobs on the printer are tracked. We recommend this method to track regular copies and when quotas are enabled when using LDD. Only the actual pages printed are tracked when using this setting. Canceled copy jobs are sent immediately to the server for a real-time user quota update. **Note:** During the Copy or Copy Cancel workflow, the Track Copy and Track Copy Cancel settings must not be enabled at the same time on a printer. Enabling these settings together causes duplicate entries in the PR_STATS report.
Track Email	When enabled, emails sent from the printer are tracked. If LDD Print Release is used, then the From field shows the email address of the logged in user, and the Track Email setting must not be enabled.
Track Fax Send	When enabled, faxes sent from the printer are tracked. We recommend this method for tracking fax jobs. If Print Release (Fax + Profile) is used, then the Track Fax Send setting must not be enabled.
Track Fax Receive	When enabled, faxes sent to the printer are tracked.
Track FTP	When enabled, FTP scans sent from the printer are tracked.
Track Print	When enabled, print jobs from the printer are tracked. When you use LDD Print Release, we recommend this method to track only print jobs that are not sent using Print Release. Make sure that the Ignore Print Jobs From setting is enabled.
Ignore Print Jobs From	A comma-separated list of IP addresses that does not generate print tracking data. When using LDD Print Release, we recommend this method to avoid duplicate tracking entries when sending jobs using Print Release. If Track Print is enabled, then this list must include all the LDD application server addresses. Including LDD servers to this list results in duplicate tracking entries.
Track Internal Print	When enabled, print jobs such as fax confirmations, email confirmations, and menu settings are tracked. The report does not include user-initiated print jobs.
Track Other Scans	When enabled, jobs that generate a scan job are tracked. The report includes any other eSF application or LDD profile that is not part of the Print Release package.
Include Profile Name in Data	When enabled, the profile name that initiated the workflow or scan job is tracked. **Note:** We recommend enabling this setting only when necessary.

Job submission options for LDD

Setting	Description
Client ID	The client credentials that are obtained from the identity service provider used with the client ID.
Client Secret	The client credentials that are obtained from the identity service provider used with the client secret.
SSL Certificate	The certificate used for secure connection.
Job Submission Interface	Determines the Web Service call version to use for sending job reports. The default value is Version 1.

Setting	Description
Report Sending Mode	Determines how the application sends reports. **Possible values** • Send Immediately • Send by Batch • Send by Schedule The default value is Send Immediately.
Send by Batch: Maximum Records for Every Batch	Determines the number of tracked records the application collects before sending the reports by batch. The default value is **100**, but the supported range of value is from **1** to **1000**.
Maximum Wait Time to Form a Batch (in Minutes)	The length of time before the application sends the report by batch. The default value is **15**, but the supported range of value is from **0** to **35,790**. **Note:** Specifying **0** disables this setting.
Send By Batch: Resend Delay (in seconds)	The length of time before the application sends the report by batch. The default values are **600,1200,1800**.
Send By Schedule: Maximum Records for Every Batch	Determines the number of tracked records the application collects before sending the reports by schedule. The default value is **100**, but the supported range of value is from **1** to **1000**.
Send by Schedule: Resend Delay (in Seconds)	The length of time before the application sends the report by schedule. The default values are **600,1200,1800**.
Report Sending Interval	The interval for sending tracked jobs by batch. **Possible values** • Minutes • Daily • Weekly The default value is Minutes.
Minutes	Determines when to send reports in minutes. The default value is **10**, but the supported range of value is from **5** to **1440**.
Daily	Determines when to send reports within the day. Use the (HH:MM) time format. To add separate times, use commas.
Day of the Week	Determines when to send reports by selecting a day of the week. The default value is Sunday.
Time of Day (in 24-hour format)	Determines when to send reports during the selected day of the week. Use the (HH:MM) time format. To add separate times, use commas.

Using Microsoft SQL Server for Print Release database

The Print Release database tables in Microsoft SQL Server are automatically created during installation. During installation, specify the Microsoft SQL Server database server information on the database screen. This process populates the **database.properties** file with the correct information automatically. In the same directory as the database.properties file, a backup copy of the database_mssql.properties file is stored. The **database_mssql.properties** file contains variable names that can be used as a template when formatting the database.properties file for Microsoft SQL Server. If you edit the database_mssql.properties for use, then rename it to **`database.properties`**.

Notes:

- Only the database.properties file is used with the solution.
- Before saving the database.properties file, stop the Lexmark Solutions Application Server service.

When switching from Firebird to Microsoft SQL Server after installation, create the Print Release database in Microsoft SQL Server manually. Delete all the backup files, and then run the LPM installer. Specify the Microsoft SQL Server database information on the database screen.

Note: The LPM data is not migrated to the new Microsoft SQL Server database.

Microsoft SQL Server supported versions

- Microsoft SQL Server 2022
- Microsoft SQL Server 2019
- Microsoft SQL Server 2017
- Microsoft SQL Server 2016
- Microsoft SQL Server 2014

Before installing Microsoft SQL Server 2014 or 2012, from the Server Manager, add the following:

- .NET Framework 3.5 features for Microsoft Server 2012
- .NET Framework 3.5.1 features for Microsoft Server 2008

Creating Print Release database for Microsoft SQL Server

Note: The installer for LPM version 2.4 or later creates the Print Release tables during installation automatically.

1. From Management Studio, connect to the database server as a database owner.
2. Right-click on the database node, and then click **New Database**.
3. Type a descriptive name for the database.
4. Click **OK**.

Adding Unicode to Print Release tables

1. From your computer, update the Print Release tables. For example, **%ProgramFiles%\Lexmark\Solutions\lpm\ms-sql-script\migrate-ascii-column-data-to-unicode.sql**.

Notes:

- Errors for the MP_PRINTERS table may occur when the table does not exist. If you are not using Email Watcher with Printer Nicknames, then comment out its lines in the script.
- When you use Print Release version 2.3.15 or later, errors for the dbo.SCHEMA_ELEMENTS table may occur when running the script on Print Release version 2.3.14. If you are using Print Release version 2.3.14, then comment out its lines in the script.

2. From Management Studio, connect to the database server as a database owner.
3. Right-click the Print Release database, and then click **New Query**.
4. In the new query window, paste the contents of the **migrate-ascii-column-data-to-unicode.sql** file.
5. Make sure that the Print Release database is selected, and then click **Execute**.

The **`varchar`** datatype is now updated to **`nvarchar`** in all Print Release tables, such as PR_JOBS.

Updating the database.properties file for Microsoft SQL Server default instances

During installation, LPM version 2.4 or later creates connection strings in the properties files. Create the Print Release database in Microsoft SQL Server manually, and then run the LPM standalone installer. This process populates the database.properties file with the correct information, and then creates the Print Release tables in Microsoft SQL Server automatically.

1. From Lexmark Management Console, set the application server offline.
2. From the application server, browse to the ***<install_path>*\apps\printrelease\WEB-INF\classes** folder, where ***<install_path>*** is the installation path of LPM.
3. Rename **`database.properties`** to **`database_backup.properties`**.
4. Using a text editor, open the **database_mssql.properties** file.
5. Do the following:
   a. Search for **`${SQLSERVER}`**, and then replace all instances with the network address of Microsoft SQL Server.
   b. Search for **`${SQLDB}`**, and then replace all instances with the Microsoft SQL Server database name that contains the Print Release database tables.
   c. Search for **`${SQLUSER}`**, and then replace all instances with the Microsoft SQL Server named user that has read-write-delete access to the Print Release database tables.
   d. Search for **`${SQLPW}`**, and then replace all instances with the password for the Microsoft SQL Server named user.
6. Name the file as **`database.properties`**.
7. Save the file.
8. Restart the Lexmark Solutions Application Server service.
9. After the Lexmark Solutions Application Server process (tomcat7.exe) has fully initialized, set the server online.
10. Repeat this process for all application servers.

Note: When only subsets of the Print Release tables are stored in Microsoft SQL Server, copy sections from the database_mssql.properties file to the database.properties file. For example, if only the Print Release statistics data in Microsoft SQL Server is necessary, then from the database_mssql.properties file, copy the database.STATS section. From the database.properties file, overwrite the same information.

Updating datasources for multiple databases

Changes in the database.properties file require updates in the LPM portal application server. By default, the LPM portal is configured with datasources that are called the default and secondary datasources. Database information in the datasource varies on the LPM setup. For example, LPM installed in a non-serverless setup points the default and secondary datasources to the same database. In a serverless setup, the default datasource points to the LPM Microsoft SQL Server database, and the secondary datasource points to the LDD Firebird database.

1. From Lexmark Management Console, set the application server offline.
2. From the application server, browse to the ***<install_path>*\apps\lpm\WEB-INF\classes** folder, where ***<install_path>*** is the installation path of LPM.
3. Using a text editor, open the **database-production-config.properties** file.
4. Update the database information pointed by the default or secondary datasource.

Sample code

```
dataSource.url = jdbc:sqlserver://<ip address>;databasename=LPMPremise;?lc_ctype=UTF-8
dataSource.driverClassName = com.microsoft.sqlserver.jdbc.SQLServerDriver
dataSource.dialect = org.hibernate.dialect.SQLServer2008Dialect
dataSource.username = lpmadmin
dataSource.password = tiger123
dataSource.properties.validationQuery = select 1
dataSource.pooled = true
dataSource.properties.maxActive = 15
dataSource.properties.maxIdle = 1
dataSource.properties.minIdle = 1
dataSource.properties.minEvictableIdleTimeMillis=5000
dataSource.properties.timeBetweenEvictionRunsMillis=60000
dataSource.properties.testOnBorrow=true
dataSource.properties.testWhileIdle=true
dataSource.properties.testOnReturn=true
dataSource.removeAbandoned=true
dataSource.removeAbandonedTimeout=180000

dataSource_secondary.url = jdbc:firebirdsql://<ip address>/3050:SOLUTIONINFO?lc_ctype=UTF-8
dataSource_secondary.driverClassName = org.firebirdsql.jdbc.FBDriver
dataSource_secondary.dialect = org.hibernate.dialect.FirebirdDialect
dataSource_secondary.username = framework
dataSource_secondary.password = ENC (mna6C4NkloGNVSx4ry08RA==)
dataSource_secondary.properties.validationQuery = select 1 from RDB$DATABASE
dataSource_secondary.pooled = true
dataSource_secondary.properties.maxActive = 15
dataSource_secondary.properties.maxIdle = 1
dataSource_secondary.properties.minIdle = 1
dataSource_secondary.properties.minEvictableIdleTimeMillis=5000
dataSource_secondary.properties.timeBetweenEvictionRunsMillis=60000
dataSource_secondary.properties.testOnBorrow=true
dataSource_secondary.properties.testWhileIdle=true
dataSource_secondary.properties.testOnReturn=true
dataSource_secondary.removeAbandoned=true
dataSource_secondary.removeAbandonedTimeout=180000
```

5 To add another datasource, do the following:

   a Copy the secondary datasource.

   b Replace **secondary** with **tertiary** or any suffix that is appropriate and unique.

   c Update the database information for the added datasource.

   d Add the password encryption codec for the added datasource.

Sample code

```
dataSource_tertiary.url = jdbc:firebirdsql://<ip address>/3050:SOLUTIONINFO?lc_ctype=UTF-8
dataSource_tertiary.driverClassName = org.firebirdsql.jdbc.FBDriver
dataSource_tertiary.dialect = org.hibernate.dialect.FirebirdDialect
dataSource_tertiary.username = framework
dataSource_tertiary.password = ENC (mna6C4NkloGNVSx4ry08RA==)
dataSource_tertiary.properties.validationQuery = select 1 from RDB$DATABASE
dataSource_tertiary.pooled = true
dataSource_tertiary.properties.maxActive = 15
dataSource_tertiary.properties.maxIdle = 1
dataSource_tertiary.properties.minIdle = 1
dataSource_tertiary.properties.minEvictableIdleTimeMillis=5000
dataSource_tertiary.properties.timeBetweenEvictionRunsMillis=60000
dataSource_tertiary.properties.testOnBorrow=true
dataSource_tertiary.properties.testWhileIdle=true
dataSource_tertiary.properties.testOnReturn=true
dataSource_tertiary.removeAbandoned=true
dataSource_tertiary.removeAbandonedTimeout=180000
dataSource_tertiary.passwordEncryptionCodec=com.lexmark.utils.PBEWithMD5AndDESCodec
```

6 If a new datasource is added, then from the application server, browse to the ***<install_path>*\apps\lpm\WEB-INF\classes** folder, where ***<install_path>*** is the installation path of LPM.

7 Using a text editor, open the **app-production-config.properties** file.

8 Update the database information that must point to the tertiary datasource.

Sample code

```
datasource.webapp = secondary
datasource.badge = DEFAULT
datasource.pin = tertiary
datasource.stats = DEFAULT
datasource.printernicknames = secondary
datasource.printtrackdevices = DEFAULT
```

9 Make sure that the updates in the LPM portal are the same as the values in the database.properties file.

10 Save the file.

11 Restart the Lexmark Solutions Application Server service.

Using Microsoft SQL Server named instances

When using a named instance of Microsoft SQL Server for the Print Release database, add the **instanceName** parameter to the following properties:

- **connect**
- **dataSource**

For example, the STATS section must be updated to the following:

```
database.STATS.connect=jdbc:sqlserver://network.address.of.mssqlserver;databaseName=CustomerP
rDatabaseName;instanceName=nameOfCustomerMSSQLInstance;
```

```
database.STATS.dataSource=network.address.of.mssqlserver;databaseName=
CustomerPrDatabaseName;instanceName= nameOfCustomerMSSQLInstance;
```

Using Microsoft SQL Server for Print Release Badge table

To use Microsoft SQL Server for the Print Release Badge table, update the mfpauth database.properties file to point to Microsoft SQL Server.

1. Create the Print Release database in Microsoft SQL Server manually. For more information, see "Creating Print Release database for Microsoft SQL Server" on page 195.
2. Run the LPM standalone installer.
3. Using a text editor, open the **database.properties** file.
4. Do the following:
   a. If a custom name is used instead of the default column name, USERID, then set **`database.BADGE.colUserId`** to the name of the user ID column.
   b. If a custom name is used instead of the default column name, BADGEID, then set **`database.BADGE.colBadgeId`** to the name of the badge ID column.
5. Save the file.
6. Restart the Lexmark Solutions Application Server service.
7. After the Lexmark Solutions Application Server process (tomcat7.exe) has fully initialized, set the server online.
8. Repeat this process for all application servers.

Configuring the print queue on a clustered print server

Note: Before you begin, make sure that the print spooler cluster resource is installed.

1. From your computer, log the passive node of the cluster, and then install the LDD Port monitor software.

   Note: For more information on installing the LDD Port monitor software, see "Installing the LDD Port monitor software" on page 49.
2. Add LDD Client Service to the print spooler cluster group.

   Note: For more information on adding LDD Client Service, see "Adding LDD Client Service" on page 52.
3. From the Windows Administrative Tools window, open the Print Management console.
4. Right-click the node for print servers, and then select **Add/Remove Servers**.
5. Enter the network address of the print spooler cluster group.
6. Click **Add to List** > **OK**.
7. Configure the print queue. For more information, see "Configuring the print queue" on page 49.

Installing Print Release reports

If necessary, LPM has some predefined Jasper reports that can be installed. The report files to install vary based on whether the customer data is stored on Firebird or Microsoft SQL Server.

Configuring Microsoft SQL Server for database support

If you are using Microsoft SQL Server to store the Print Release usage data, then before installing the reports, do the following:

1. From Lexmark Management Console, click the **Services** tab.
2. From the Services section, select **Reports**.
3. Specify the following:
   - **Database driver**—When using Microsoft SQL Server, type **`com.microsoft.sqlserver.jdbc.SQLServerDriver`**.
   - **Database URL**—Enter **`jdbc:sqlserver://<IPAddress>:1433;databaseName=PRINTRELEASE;encrypt=false`**, where ***`IPAddress`*** is the IP address of Microsoft SQL Server.

     Note: If Integrated Security is used, then add **`;integratedSecurity=true;`** in the URL.
   - **Username for external database**—The LDD service account user name with read and write access to Microsoft SQL Server.

     Note: If Integrated Security is used, then this setting is optional.
   - **Password for external database**—The LDD service account password with read and write access to Microsoft SQL Server.

     Note: If Integrated Security is used, then this setting is optional.
4. Click **Apply**.

Configuring available reports

1. From Lexmark Management Console, click the **System** tab.
2. From the System section, select **Reports**.
3. Select a report, and then click  .
4. When using a Microsoft SQL Server database, set Datasource to **EXTERNAL**.
5. Specify the database information.
6. Click **Save**.

Installing reports

1. Extract the contents of the Print Release Reports install package to the LDD server.
2. From Lexmark Management Console, click the **System** tab.
3. From the System section, select **Reports**.

4 Click **Upload Report Files**.

5 Browse to the extracted reports, and then select the necessary files.

6 Click **Upload**.

7 From the System section, make sure that **Reports** is selected, and then click ✚.

8 Do either of the following:
- When using a Microsoft SQL Server database, set Datasource to **[EXTERNAL]**.
- When using the default database, set Datasource to **SOLUTIONINFO**.

9 Select a **PR_** jasper file.

10 Enter a descriptive report name.

11 Click **Save**.

12 If necessary, repeat step 8 through step 11 for all other **PR_** jasper files.

Submitting jobs from a Mac computer

Before you begin, make sure that an LDD server with the Print Release solution is installed and working properly. There must be a shared printer connected to the LDD Print Release solution.

You can submit jobs using either LPD printer share or Samba share.

Configuring LPD printer share

This method shares a printer on the server, and then the client Mac computer prints to it using the Line Printer Daemon (LPD) protocol.

Server configuration

1 From your computer, share a printer.

Note: We recommend creating a share name with only one word, such as **PrintRelease**.

2 From the Windows Administrative Tools window, open the Server Manager console, and then click **Roles** > **Add Roles** > **Print and Document Services**.

3 From the Add Roles window, click **Role Services** > **LPD Service Role**.

LDD configuration

1 From Lexmark Management Console, click the **Solutions** tab.

2 From the Solutions section, select **PrintReleasev2**.

3 From the Tasks section, select **Configuration**.

4 In the Enable Printing From Unix/Novell menu, select **Yes**.

Client configuration

1. From the client Mac computer, open the System Preferences window, and then click **Print & Scan**.
2. Click ✚.
3. Click **IP**, and then enter the server IP address.
4. In the Protocol menu, select **Line Printer Daemon – LPD**.
5. In the Queue field, enter the printer share name.
6. In the Use menu, select **Select Printer Software**.
7. In the Filter field, type **Lexmark**, and then select either of the following:
   - **Lexmark Generic Laser Printer Color**
   - **Lexmark Generic Laser Printer Mono**
8. Click **Add** > **OK**.

Configuring Samba share

This method shares a printer on the server, and then the client Mac computer connects to the shared printer as a Samba share.

1. From the Windows server, share a printer.

   Note: We recommend creating a share name with only one word, such as **PrintRelease**.
2. If the LPM print share is not in a domain, then do the following:
   - Enable Guest access. Navigate to Control Panel, and then click **Add or Remove user accounts** > **Guest** > **Turn on Guest Account**.
   - Add a standard user account with a password.

     Note: Make sure that the user name matches the user name for the Mac computer.
3. From the client Mac computer, open the System Preferences window, and then click **Print & Scan**.
4. Click ✚.
5. Press the control key, click the window toolbar, and then click **Customize Toolbar**.
6. Drag ⚙ to the toolbar, and then click **Done**.
7. Click ⚙ > **Type** > **Windows Printer via spools**.
8. Enter the smb:// URL with an IP address or server name and the printer share name. For example, **smb://10.1.2.3/PrintReleaseShareName**.
9. In the Use menu, select **Select Printer Software**.
10. In the Filter field, type **Lexmark**, and then select either of the following:
    - **Lexmark Generic Laser Printer Color**
    - **Lexmark Generic Laser Printer Mono**
11. Click **Add** > **OK**.

Note: When printing from a Mac computer, select the created printer, and then enter your credentials when prompted.

Configuring Serverless Print Release

Installing Lexmark Serverless Print Release

Note: Before you begin, make sure that Lexmark Print Management version 2.7 or later is installed.

1. From Lexmark Management Console, click the **Solutions** tab.
2. From the Solutions section, click **All Solutions**.
3. Click **Install/Upgrade**.
4. Browse to the Serverless Print Release application.
5. Click **Upload**.

Configuring Serverless client registration

Understanding the serverless configuration settings

Notes:

- The configuration file is case-sensitive.
- Modify only the elements that are applicable to your configuration.

Delete Job Tracker Settings

This setting tracks the unprinted print jobs that are deleted.

Delete Job Tracker Settings

Setting	Description
<TrackDeletedJob>	Enables tracking of deleted print jobs. The default value is **false**.
<SendImmediately>	Enables submitting the data after every data collection. Otherwise, the data is submitted in intervals. The default value is **true**.
<IntervalMode>	The default value is **Minutes**. The other modes are **Hourly**, **Daily**, and **Weekly**. The **Hourly** mode automatically sets the interval to 60 minutes.

Setting	Description
<Minutes>	The value must be equal or greater than 1.
<Daily>	The value must be in hours in HHMM format. The interval is daily, based on the set hour.
<Weekly>	The values must be in days and hours. The values in **<Day>** indicate the numeric representation of the days of the week, where *1* is Sunday and *7* is Saturday. The value in **<Hour>** must be in HHMM format.

Setting	Description
<ServerIP>	The IP address of the Lexmark Print Management (LPM) server.
<ServerPort>	The port number of the LPM server. The default port number is 9743.
<ServerSSL>	Enables communication with the server using an SSL or non-SSL connection. The default value is **true**. If the **<ServerPort>** is set to **9780**, then the value of **<ServerSSL>** must be set to **false**.

Setting	Description
<SiteName>	The name of the site where the print job was submitted from.

Configuring Lexmark Print Management Client

Serverless Print Release

1. From your computer, navigate to the **C:\ProgramData\LPMC** folder.
2. Using a text editor, open the **configuration.xml** file.
3. If necessary, set **LoggingEnabled** to **true**.
4. From the **ServerSettings** section, do the following:
   - Set **ServerIP** to the IP address of the LPM server.
   - Set **ServerPort** to **443** for SSL connections or **9780** for non-SSL connections.
   - Set **ServerSSL** to **true** for SSL connections or **false** for non-SSL connections.
5. From the **IDPServerSettings** section, do the following:
   - Set **ServerIP** to the IP address of the Identity Provider (IDP) server, and then add **/idm**.
   - Set **ServerPort** to **443** for SSL connections or **9780** for non-SSL connections.
   - Set **ServerSSL** to **true** for SSL connections or **false** for non-SSL connections.

Server Print Release

1. From your computer, navigate to the **C:\ProgramData\LPMC** folder.
2. Using a text editor, open the **configuration.xml** file.
3. If necessary, set **LoggingEnabled** to **true**.
4. From the **ServerSettings** section, do the following:
   - Set **ServerIP** to the IP address of the Print Release server. The default value is **lsp.lexmark.com/Lexmark**.
   - Set **ServerPort** to **443** for SSL connections or **80** for non-SSL connections.
   - Set **ServerSSL** to **true** for SSL connections or **false** for non-SSL connections.
5. From the **IDPServerSettings** section, do the following:
   - Set **ServerIP** to the IP address of the Print Release server. The default value is **idp.iss.lexmark.com**.
   - Set **ServerPort** to **443** for SSL connections or **80** for non-SSL connections.

- Set **ServerSSL** to **true** for SSL connections or **false** for non-SSL connections.

6 From the **IDPServerSettings** section, set **ServerPort** to **443**.

Note: Make sure that the user has administrative rights before connecting to the LDD print queue or submitting print jobs.

Configuring the Card Authentication application

The Card Authentication application must be configured for serverless print release to function.

Note: For more information on the card authentication configuration, see "Understanding the CardAuth version 5 configuration data for e-Task 5 printers" on page 180.

Configuring the Print Release application

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

2 From the Serverless Web Server Settings section, set Server Address to **https://*serverIP*/lpm/api/2.0**, where ***serverIP*** is the IP address of the LPM server.

3 Set the SSL port number to **9443**.

4 Set the HTTP port number to **9780**.

5 Set the security mode to **Auto**.

6 Click **Save**.

Configuring eSF applications settings for Print Release

Understanding the CardAuth configuration data for e-Task 5 printers

User authentication settings

Setting	Description
Card Validation	Determines how cards are validated. **Required value** Identity Service
Card Registration	The login method for registering using cards. **Required value** Identity Service **Note:** Selecting **Disabled** restricts all users from registering their badge at the specific printer.
Manual Login	The login method for logging in manually. **Required value** Identity Service **Note:** Selecting **Disabled** restricts all users from logging in without a badge.

Identity Service settings

Setting	Description
Identity Service Provider Address	The URL of the identity service provider. Use the following format for its value: • **http://*IPaddress*:9780/idm** • **https://*IPaddress*/idm** Where ***IPaddress*** is the IP address of the identity service provider.
Badge Service Provider Address	The URL of the badge service provider. Use the following format for its value: • **http://*IPaddress*:9780/lpm** • **https://*IPaddress*/lpm** Where ***IPaddress*** is the IP address of the badge service provider.
Client ID	The client credentials from the identity service provider used with the client secret. **Required value** esf-cardauth-app
Client Secret	The client credentials from the identity service provider used with the client ID. Set Client Secret with the value from ***<install-Dir>*\Lexmark\Solutions\apps\idm\WEB-INF\classes\idm-production-config.properties** file, where ***<install-Dir>*** is the installation folder of LDD. To increase security, update the client secret. Make sure that the values match the entries set in the idm-production-config.properties file.

Understanding the BadgeAuth configuration data for e-Task 4 and e-Task 3 printers

Note: To make sure that print jobs appear in the print queue, type the user ID in lowercase when registering a user.

User authentication settings

Setting	Description
Card Validation	Determines how cards are validated. **Required value** Identity Service

Setting	Description
Card Registration Access Control	Determines the access control that is used for card registration. **Required value** Identity Service **Note:** Selecting **None** restricts all users from registering their badge at the specific printer. To configure access controls, do the following: 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**. • Click **Security** > **Edit Security Setups** > **Access Controls**. 3 Click **Device Apps** or **Device Solutions**, and then set functions to the appropriate LDAP building block and security template. 4 Click **Submit**. For more information on configuring access controls, see the *Card Authentication Administrator's Guide*.
Manual Login Access Control	Determines the access control that is used for manual login. The access control configuration for this method is the same as Card Registration Access Control. **Required value** Identity Service **Note:** Selecting **None** restricts all users from logging in without a badge.
Session Access Control	Determines the access control that is used for a user's session data. Another printer function, such as Copy, may be set to the same access control, and then get the user information. Select the solution or application number that corresponds to the BadgeAuth or CardAuth security template that is defined when creating an access control. **Required value** Identity Service

Identity Service settings

Setting	Description
Identity Service Provider Address	The URL of the identity service provider. Use the following format for its value: • **http://*IPaddress*:9780/idm** • **http://*IPaddress*/idm** Where ***IPaddress*** is the IP address of the identity service provider.
Badge Service Provider Address	The URL of the badge service provider. Use the following format for its value: • **http://*IPaddress*:9780/lpm** • **http://*IPaddress*/lpm** Where ***IPaddress*** is the IP address of the badge service provider.
Client ID	The client credentials from the identity service provider used with the client secret. **Required value** esf-cardauth-app

Setting	Description
Client Secret	The client credentials from the identity service provider used with the client ID. Set Client Secret with the value from ***<install-Dir>*\Lexmark\Solutions\apps\idm\WEB-INF\classes\idm-production-config.properties** file, where ***<install-Dir>*** is the installation folder of LDD. To increase security, update the client secret. Make sure that the values match the entries set in the idm-production-config.properties file.

Understanding the LexDas configuration data for e-Task 4 and e-Task 3 printers

Web Server settings

Setting	Description
Web Server	Lets the application communicate with Lexmark Print Management Client via Lexmark Print Management as an Active Directory. **Required value** Enabled
Server Address	The URL of the web server. Use the following format for its value: • **http://*IPaddress*:9780/lpm/api/2.0** • **http://*IPaddress*/lpm/api/2.0** Where ***IPaddress*** is the IP address of the web server.
Security Mode	Handles the used HTTP connections. **Required value** Auto
SSL Port	The SSL port number used by the server. **Required value** 9443
HTTP Port	The HTTP port number used by the server. **Required value** 9780

Understanding the PrintRelease configuration data for e-Task 5 printers

Serverless Web Server settings

Setting	Description
Serverless (Web)	Lets the application communicate with Lexmark Print Management Client via Lexmark Print Management as an Active Directory. **Required value** Enabled

Setting	Description
Server Address	The URL of the web server. Use the following format for its value: • **http://*IPaddress*:9780/lpm/api/2.0** • **http://*IPaddress*/lpm/api/2.0** Where ***IPaddress*** is the IP address of the web server.
SSL Port	The SSL port number used by the server. **Required value** 9443
HTTP Port	The HTTP port number used by the server. **Required value** 9780
Security Mode	Handles the used HTTP connections. **Required value** Auto

Customizing the home screen for a serverless environment

1. From Lexmark Management Console, click the **Device Groups** tab.
2. From the Device Groups section, select **Serverless Print Release**.
3. From the Tasks section, select **Home Screen**.
4. Click the tab for each device class that you want to customize.
5. Select **Use this home screen as part of the device groups policy**.
6. In the Action menu, select **App Reservation**.
7. In the Profile menu, select either of the following:
   - For e-Task 5 printers, select **printRelease**.
   - For e-Task 4 and e-Task 3 printers, select **LPRP4**.
8. Click **Apply** on each tab.

Configuring Reports Aggregator

Lexmark Reports Aggregator Service generates report data that is shown on the Print Management Console Dashboard. The Reports Aggregator service is added to generate report data in the background at a specified time.

Note: The data shown in the administrator dashboard is based on the last data that is generated by the service.

For the Reports Aggregator service to work, database information is requested during installation on an Enterprise install (load balancer) environment. The service runs only on Java version 1.8 or later and requires LDD version 5 or later.

Configuring the scheduler

1. From your computer, access the load balancer server.
2. Navigate to the ***<install-Dir>*\Lexmark\Solutions\services\lpm-reports-service** folder, where ***<install-Dir>*** is the installation folder of LPM.
3. Using a text editor, open the **application.properties** file.
4. Set **`app.aggregation.service.schedule.cron`** to change interval.
5. Save the file.
6. Restart the Lexmark Solutions Application Server service.

Configuring e-mail reporting refresh frequency

1. From your computer, access the load balancer server.
2. Navigate to the ***<install-Dir>*\Lexmark\Solutions\services\lpm-reports-service** folder, where ***<install-Dir>*** is the installation folder of LPM.
3. Using a text editor, open the **application.properties** file.
4. Set **`app.reporting.email.checker.service.schedule.cron`** to change the interval.
5. Save the file.
6. Restart the Lexmark Solutions Application Server service.

Contacting Lexmark Help Desk

When contacting Lexmark Help Desk, make sure that you have the following information to expedite handling of issues:

- The PIN of your company, if provided.
- The version of LDD your printer is currently connected to.

  To obtain the version, do the following:

  1. Access Lexmark Management Console from your Web browser.
  2. From the top section of the page, click **About**.
- The version of the Print Management solution you are currently using.

To obtain the version, do the following:

1. Access Lexmark Management Console from your Web browser.
2. Click the **Solutions** tab, and then select **PrintReleasev2** in the Solutions section.
3. From the Tasks section, select **Summary**, and then find the version section.

Understanding standard reports

Usage by device (PR_DeviceUsageReport.jasper)

Report field	Description
Device IP	The IP address of the printer where you printed the job
Serial Number	The serial number of the printer where you printed the job
Output Volume (Total)	The total number of print and copy jobs printed
Print (Total)	The total number of print jobs printed
Print (Color)	The total number of jobs printed in color
Print (Mono)	The total number of jobs printed in black and white
Print (Duplex)	The total number of jobs printed on both sides of the paper
Copy	The total number of copy jobs printed
Email	The total number of e-mail jobs printed
Fax	The total number of fax jobs printed
Scan	The total number of jobs sent to a network
FTP	The total number of jobs sent to an FTP address

Usage by device host name (PR_DeviceUsageReport_Hostname.Jasper)

Note: The host name is obtained through DNS query. If the host name is not configured in DNS, then the IP address will be used as substitute.

Report field	Description
Device Name	The name of the printer where you released the job
Output Volume (Total)	The total number of print and copy jobs released
Print (Total)	The total number of jobs printed
Print (Color)	The total number of jobs printed in color
Print (Mono)	The total number of jobs printed in black and white
Print (Duplex)	The total number of jobs printed on both sides of the paper
Copy	The total number of copy jobs released
Email	The total number of e-mail jobs released
Fax	The total number of fax jobs released

Report field	Description
Scan	The total number of jobs sent to a network
FTP	The total number of jobs sent to an FTP address

Usage by device IP address and model name (PR_DeviceUsageReport_IPModel.jasper)

Report field	Description
Device IP	The IP address of the printer where you printed the job
Serial Number	The serial number of the printer where you printed the job
Model	The model name of the printer where you printed the job
Output Volume (Total)	The total number of print and copy jobs printed
Print (Total)	The total number of print jobs printed
Print (Color)	The total number of jobs printed in color
Print (Mono)	The total number of jobs printed in black and white
Print (Duplex)	The total number of jobs printed on both sides of the paper
Copy	The total number of copy jobs printed
Email	The total number of e-mail jobs printed
Fax	The total number of fax jobs printed
Scan	The total number of jobs sent to a network
FTP	The total number of jobs sent to an FTP address

Usage by device IP address, model name, and model type (PR_DeviceUsageReport_IPModelType.jasper)

Report field	Description
Device IP	The IP address of the printer where you printed the job
Serial Number	The serial number of the printer where you printed the job
Model	The model name of the printer where you printed the job
Output Volume (Total)	The total number of print and copy jobs printed
Print (Total)	The total number of print jobs printed
Print (Color)	The total number of jobs printed in color
Print (Mono)	The total number of jobs printed in black and white
Print (Duplex)	The total number of jobs printed on both sides of the paper
Copy	The total number of copy jobs printed
Email	The total number of e-mail jobs printed
Fax	The total number of fax jobs printed

Report field	Description
Scan	The total number of jobs sent to a network
FTP	The total number of jobs sent to an FTP address

Detail print report by device (PR_detailPrintReportByDevice.jasper)

Group header	
User	The name of the user who printed the print job
Total Print	The total number of pages printed

Report field	Description
Device IP	The IP address of the printer where you printed the print job
Serial Number	The serial number of the printer where you printed the job
Print Job Name	The name of the print job defined by the submitting system and extracted from the print job header
Print (Total)	The total number of print jobs printed
Color	Determines whether a job is printed in color
Duplex	Determines whether a job is printed on both sides of the paper
Paper Size	The size of the paper selected at the time the print job was printed

Detailed print report by user (PR_DetailPrintReportByUser.jasper)

Group header	
User	The name of the user who released the print job
Total Print	The total number of pages printed

Report field	Description
Device Address	The IP address of the printer where you released the print job
Print Job Name	The name of the print job defined by the submitting system and extracted from the print job header
Print (Total)	The total number of print jobs released
Color	Determines whether a job is printed in color
Duplex	Determines whether a job is printed on both sides of the paper
Paper Size	The size of the paper selected at the time the print job was released

Detailed print report by host name (PR_detailPrintReportByUser_Hostname.jasper)

Group header	
User	The name of the user who released the job
Total Print	The total number of pages printed

Report field	Description
Hostname	The host name of the printer where you released the job
Print Job Name	The name of the print job defined by the submitting system and extracted from the print job header
Print (Total)	The total number of print jobs released
Color	Whether a job is printed in color
Duplex	Whether a job is printed on both sides of the paper
Paper Size	The size of the paper selected at the time the job was released

Detailed print report by printer IP address, model name, and model type (PR_detailPrintReportByUser_ IPMMT.jasper)

Group header	
User	The name of the user who printed the print job
Total Print	The total number of pages printed

Report field	Description
Device IP	The IP address of the printer where you printed the print job
Serial Number	The serial number of the printer where you printed the print job
Model	The model name of the printer where you printed the print job
Model Type	The model type of the printer where you printed the print job
Print Job Name	The name of the print job defined by the submitting system and extracted from the print job header
Print (Total)	The total number of print jobs printed
Color	Determines whether a job is printed in color
Duplex	Determines whether a job is printed on both sides of the paper
Paper Size	The size of the paper selected at the time the print job was printed

Detailed print report by printer IP address and model type (PR_detailPrintReportByUser_ IPModelType.jasper)

Group header	
User	The name of the user who printed the print job
Total Print	The total number of pages printed

Report field	Description
Device IP	The IP address of the printer where you printed the print job
Serial Number	The serial number of the printer where you printed the print job
Model Type	The model type of the printer where you printed the print job
Print Job Name	The name of the print job defined by the submitting system and extracted from the print job header
Print (Total)	The total number of print jobs printed
Color	Determines whether a job is printed in color
Duplex	Determines whether a job is printed on both sides of the paper
Paper Size	The size of the paper selected at the time the print job was printed

Color or mono printing report by user (PR_ColorMonoByUser.jasper)

Report field	Description
User	The name of the user who released the print job
Print (Total)	The total number of print jobs released
Print (Mono)	The total number of jobs printed in black and white
Print (Color)	The total number of jobs printed in color

Usage report defined in Custom1 field (PR_[custom1]UsageReport.jasper)

Group header	
Custom1	The variable name defined as attribute for grouping users in LDAP database

Report field	Description
User	The name of the user who released the job
Copy	The total number of copy jobs released
Email	The total number of e-mail jobs released
Fax	The total number of fax jobs released
Print (Total)	The total number of print jobs released
Print (Mono)	The total number of jobs printed in black and white
Print (Color)	The total number of jobs printed in color

Report field	Description
Print (Duplex)	The total number of jobs printed on both sides of the paper

Single-sided or two-sided printing report by user (PR_simplexDuplexByUser.jasper)

Report field	Description
User	The name of the user who released the job
Print (Total)	The total number of print jobs released
Print (Simplex)	The total number of jobs printed on one side of the paper
Print (Duplex)	The total number of jobs printed on both sides of the paper

Top or bottom 20 users report by print count (PR_top20PRINTUser.jasper or PR_bottom20PRINTUser.jasper)

Report field	Description
User	The name of the user who owns the print job
Print (Total)	The total number of print jobs released
% of Total	The percentage of print jobs the user released against the total number of print jobs all users released

Top or bottom 20 users report by copy count (PR_top20COPYUser.jasper or PR_ bottom20COPYUser.jasper)

Report field	Description
User	The name of the user who released the copy job
Page Count (Total)	The total number of copy job the user released
% of Total	The percentage of copy job a user released against the total number of copy job all users released

Top or bottom 20 users report by e-mail count (PR_top20EMAILUser.jasper or PR_bottom20EMAILUser.jasper)

Report field	Description
User	The name of the user who released the e-mail job
Page Count (Total)	The total number of e-mail job a user released
% of Total	The percentage of e-mail job a user released against the total number of e-mail job all users released

Top or bottom 20 users report by scan to network count (PR_top20SCANUser.jasper or PR_ bottom20SCANUser.jasper)

Report field	Description
User	The name of the user who sent the scan job to a network
Page Count (Total)	The total number of scan job the user sent to a network
% of Total	The percentage of scan job a user sent to a network against the total number of scan job all users sent to a network

Top or bottom 20 users report by fax count (PR_top20FAXUser.jasper or PR_ bottom20FAXUser.jasper)

Report field	Description
User	The name of the user who released the fax job
Page Count (Total)	The total number of fax job the user released
% of Total	The percentage of fax job a user released against the total number of fax job all users released

Deleted pages report by user (PR_pageDeletedByUser.jasper)

Report field	Description
User	The name of the user who deleted the jobs
Page Count (Total)	The total number of all deleted jobs
Deleted User	The total number of jobs the user deleted
Deleted System	The total number of jobs the system automatically deleted
% of Total	The percentage of jobs the user and the system deleted against the total number of all deleted jobs

Notices

Edition notice

December 2024

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

Mac, Mac OS, AirPrint, and Safari are trademarks of Apple Inc., registered in the U.S. and other countries. App Store is a service mark of Apple Inc., registered in the U.S. and other countries.

Microsoft, Active Directory Excel, Internet Explorer, Microsoft Edge, PowerPoint, SQL Server, Vista, Windows, and Windows Server are trademarks of the Microsoft group of companies.

PCL® is a registered trademark of the Hewlett-Packard Company. PCL is Hewlett-Packard Company's designation of a set of printer commands (language) and functions included in its printer products. This printer is intended to be compatible with the PCL language. This means the printer recognizes PCL commands used in various application programs, and that the printer emulates the functions corresponding to the commands.

PostScript is either a registered trademark or trademark of Adobe Systems Incorporated in the United States and/or other countries.

Firebird is a registered trademark of the Firebird Foundation.

Google Chrome, Google Play, and Android are trademarks of Google LLC.

Java is a registered trademark of Oracle and/or its affiliates.

All other trademarks are the property of their respective owners.

Index

Symbols

A

B

C

D

E

F

G

H

I

J

S

T

U

V

W

Z