Print Management On-Premises

Version 2.14.0

Configuration Guide

Contents

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 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 send your files to the server from the following securely 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.

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

Getting started

System requirements

For configuring Print Release with rf IDEAS

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 necessary document types

For configuring DNS servers

- Microsoft Windows Server (2012 or 2008 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.

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. In an enterprise environment, you can see the status of all application servers from all workgroup systems in the System Status page.

1 From Lexmark Management Console, click **System > System Status**.

2 Select a server.

3 Click **Set Online** or **Set Offline**.

Notes:

- 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.
- Setting the server offline still allows administrators to stay connected to the server.

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.

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
- Microsoft Exchange

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]
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 are 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 HelpDesk 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.
* Indicates the default value.			

Setting name	Setting for	Possible values	Notes
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	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.
Conversion Method	Lexmark Print and E-mail	• MS Office and Open Office • Open Office 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 8.	Specifies the method used to convert attachments. If **Open Office Only** is selected, then all file types are converted using Open Office or LibreOffice. If **MS Office and Open Office** 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 Open Office**.
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.
* Indicates the default value.			

Setting name	Setting for	Possible values	Notes
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, 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.
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.
* Indicates the default value.			

Setting name	Setting for	Possible values	Notes
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.
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.
* Indicates the default value.			

Setting name	Setting for	Possible values	Notes
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.			

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 8.

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 document conversion software

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

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 the **C:\Windows\SysWOW64\config\systemprofile** folder.
   - For 32-bit operating systems, navigate to the **C:\WINDOWS\system32\config\systemprofile** folder.

5 Create a directory, and then use the `Desktop` name.

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

7 To convert 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 user name 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

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 <u>"Adding Lexmark Print to a software client group" on page 15</u>.

1 From your mobile device, open Lexmark Print.

2 From the application home screen, tap **Settings** > **Manage Devices**.

3 Do either of the following:
- For devices running the iOS operating system software, tap **Add a Device**.
- For devices running the Android™ platform, tap ✚.

4 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 and software load balancer in front of several subsystems, then type the hardware and software load balancer address.

5 Depending on your configuration, log in using your LDAP or Active Directory credentials. For more information, see <u>"Understanding the mobile and e-mail configuration data" on page 10</u>.

Testing the Lexmark Print status without a mobile device

Part of the Lexmark Print software installation is Mobile Service. The service is used by the application to communicate with Lexmark Print Management.

1 From your computer, open a web browser, and then type **https://*IPaddress*/mobile/rest/info**, where ***IPaddress*** is the IP address of the load balancer.

2 Accept the self-signed certificate from the Lexmark Print Management system.

If the service is running successfully, then the following appears in your web browser:

```
{
        "printQueueName": "Lexmark Print Management",
        "version": {
                "printReleaseApiVersion": "1.3.5",
                "documentAccountingApiVersion": "1.3.5",
                "printSubmissionApiVersion": "1.3.5"
        },
        "capabilities": {
                "printSettings": {
                        "copies": "unavailable",
                        "duplex": "unavailable",
                        "nup": "unavailable",
                        "color": "unavailable",
                        "collation": "unavailable",
                        "title": "submitView",Lexmark & Lexmark Partner Internal Use Only
Page 18
                        "description": "unavailable"
                },
                "serverSettings": {
                        "thirdPartyReleaseEnabled": "true",
                        "quotaEnabled": "false",
                        "delegatorsEnabled": "true",
                        "serverReleaseEnabled": "true",
                        "policiesEnabled": "false"
                }
        },
        "api": {
                "currentVersion": "2.0",
                "supportedVersions": "1.0,1.1"
        }
}
```

Configuring Lexmark Email Watcher

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.
`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.

Setting	Valid values	Notes
`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
```

Configuring printer nicknames

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.

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**.
> - 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.

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 10.

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**.

Option	Value	Notes
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 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:9780/#/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 .
- Configure BIND for Windows DNS Server. For more information, see .

Multicast

1 Access the AirPrint configuration page. For more information, see .

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

Viewing AirPrint jobs

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

3 From Print Management Console, click the **Printer Queue** tab.

4 From the Site column, locate jobs that are listed as IPP Print.

Configuring DNS servers

The following instructions are verified using BIND version 9.

Understanding LMC portal configuration for print queue filtering

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

2 Click ➕.

3 In the Add Device Group window, do the following:

    a Type a unique group name.

    b From the Select the group to copy menu, select **Print Release**.

    c Click **Add**.

4 Click **Tasks** > **Solutions**.

5 From Solutions to display menu, select **PrintReleaseV2**, and then click icon.

6 In the Edit a solution to deploy window, do the following:

    a In the Site to Exclude in Print Queue field, type the name of the jobs that you want to exclude.

    b In the Site to Include in Print Queue field, type the name of the jobs that you want to include.

    c Click **Finish**.

7 The changes are saved.

Sample site name configurations

Job Submission Method	Site Name
Job Router for MICR Jobs	JR-MICR
Job Router for non-MICR Jobs	JR-NON-MICR
Client Software (PrintReleasev2 Solution)	PR-Global
Email Watcher/Mobile Print	mobileprint
AirPrint	IPPPrint
Guest Print	guestprint

Use case 1: View all jobs in MICR printers, and non-MICR print jobs only in non-MICR printers

- **Device Group** > **MICR**, and then do either of the following:
  - Site to Include in Print Queue: <blank> or <specify all site names: `JR-MICR,JR-NON-MICR,PR-Global,mobileprint,IPPPrint,guestprint`>
  - Site to Exclude in Print Queue: <blank>

- **Device Group** > **Non-MICR**
  - Site to Include in Print Queue: <blank>
  - Site to Exclude in Print Queue: JR-MICR

Use case 2: View MICR print jobs only in MICR printers, and non-MICR print jobs only in non-MICR printers

- **Device Group** > **MICR**:
  - Site to Include in Print Queue: JR-MICR
  - Site to Exclude in Print Queue: <blank>
- **Device Group** > **Non-MICR**
  - Site to Include in Print Queue: <blank>
  - Site to Exclude in Print Queue: JR-MICR

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

Note: Make sure that the server is configured with a static IP address.

For Windows Server 2012

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**.

For Windows Server 2008

1 From the Windows Administrative Tools window, click **Server Manager**.

2 Click **Roles** > **Add Roles** > **Next**.

3 Select **DNS Server** > **Next**.

4 Click **Install**.

Creating a lookup zone

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**.

Configuring subdomains and resource records

Service records combine service types and transport protocols to form a registration type that creates resource records. Registration types are prefixed with an underscore (_) to differentiate them from domain names. To advertise your AirPrint service, create subdomains in the following order:

1 _tcp

2 _ipp

3 _sub

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 **lb**, 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 zone files

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 <u>"Installing the rf IDEAS Ethernet 241 adapter" on page 43</u>.

2 Configure the rf IDEAS Ethernet 241 adapters.

- For more information on using the discovery tool, see <u>"Configuring rf IDEAS Ethernet 241 using the rf IDEAS discovery tool" on page 43</u>.
- For more information on using the Lexmark Print Release Adapter Management tool, see <u>"Configuring rf IDEAS Ethernet 241 using the Lexmark Print Release Adapter Management tool" on page 44</u>.

3 If necessary, configure the rf IDEAS badge readers. For more information, see <u>"Configuring rf IDEAS badge readers" on page 45</u>.

4 Configure the client profiles. For more information, see <u>"Configuring client profiles" on page 45</u>.

5 Configure the user authentication. For more information, see <u>"Configuring user authentication" on page 45</u>.

6 Configure the Lexmark Print Management Console features. For more information, see <u>"Using the Print Management Console features" on page 46</u>.

7 Set the LDD server online. For more information, see <u>"Changing the status of the server" on page 6</u>.

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**.

Using the Print Management Console features

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

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 ![filter icon].

  Note: Do not use special characters or symbols.

- Show or hide columns by clicking ![columns icon].

- Refresh the list by clicking ![refresh icon].

- 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 badge columns

1 Click ![settings icon] 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**.

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 ![filter icon].

  Note: Do not use special characters or symbols.

- Show or hide columns by clicking ![columns icon].

- Refresh the list by clicking ![refresh icon] .

- 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 ![settings icon] 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**.

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 ![filter icon].

   Note: Do not use special characters or symbols.

- Refresh the list by clicking ![refresh icon].
- 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 delegation for existing jobs is not selected, then the delegate can print only future jobs.

Policies

Manage user or group restrictions when printing. Print policies are predefined 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 ![filter icon].

   Note: Do not use special characters or symbols.

- Refresh the list by clicking ![refresh icon].
- 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 ![gear icon] on the upper-right corner of the Print Management Console.

2 Click **Feature Options** > **Policies**.

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

4 Click **Save Changes**.

Understanding policy rules

A policy contains the business rules of the organization based on the following:

- User
- Document attributes

Policy rules and actions

Category	Operation	Value	Sub action	Job conversion
Job Type	N/A	Mono	Duplex	✓
		Color	Mono	✓
			Duplex	✓
Page Count	Greater Than or Less Than	<Number>	Duplex	✓
			Mono	✓
All Jobs	N/A	N/A	Duplex	✓
			Mono	✓

The allowed values for the page count category are the following:

- If Less Than is selected as the operation, then subtract 1 from the value for Greater Than. For example, if the value for Less Than is **10**, then the value for Greater Than must be **9**.
- If Greater Than is selected as the operation, then add 1 to the value for Less Than. For example, if the value for Greater Than is **9**, then the value for Less Than must be **10**.

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 printer, tap your badge on the card reader.

To acknowledge the tapping of 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. Also, 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 that its network connection is working properly.

- **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 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**—The print jobs are either printed on one side only or on both sides of the paper.
- Touch **Finishing Options**, and then configure either of the following:
  - **Staple**—The printed jobs are stapled.
  - **Hole punch**—The printed jobs are punched with holes.

   Note: The availability of these settings depends on the configuration of your Lexmark Print Management Client.

5 Touch **Print**.

Notes:

- The Lexmark Print Management Print Release server only attempts to transmit the print jobs 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 not a color printer but the released job is in color, then the color quota is updated. The Lexmark Print Management Print Release server does not check whether the printer has color capability or whether color is enabled on the printer.

- 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.

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

Configuring Lexmark Print Management Client

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, set `ServerIP` to the IP address of the LPM server.

5 If the LPM server is configured with SSL, then do the following:

- From the `ServerSettings` section, set `ServerPort` to either `443` or `9780`.
- From the `ServerSettings` section, set `ServerSSL` to either `true` or `false`.

6 From the `IDPServerSettings` section, set `ServerIP` to the IP address of the LPM server, and then add `/idm`.

7 From the `IDPServerSettings` section, set `ServerPort` to `443`.

Accessing the Embedded Web Server

1 Obtain the printer IP address. Do either of the following:

- Locate the IP address on the printer home screen.
- From the printer home screen, touch **Settings** > **Network/Ports** > **Network Overview**.

2 Open a web browser, and then type the printer IP address.

Configuring the Card Authentication application

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 to **211b5c35-9e05-4909-aafe-b1c5aa6a6630**.

Note: You can update the client secret.

7 Set Card Registration to **Identity Service**.

8 Set Manual Login to **Identity Service**.

9 Click **Save**.

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

Setting	Description
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** • **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
Client Secret	The client credentials from the identity service provider used with the client ID. **Default value** 211b5c35-9e05-4909-aafe-b1c5aa6a6630 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. **Default value** 211b5c35-9e05-4909-aafe-b1c5aa6a6630 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.

Troubleshooting

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>
```

Note: For more information, see the *Lexmark Print Management On‑Premises Administrator's Guide*.

For Mac OS operating system software

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

Note: For more information, see the *Lexmark Print Management On‑Premises Administrator's Guide*.

- 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

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

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 is printed

Jobs appear to be printing but no output is 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

Mobile device configuration troubleshooting

Job submission failed

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, then 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 <u>"Configuring Lexmark Email Watcher" on page 18</u>.

\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

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, external images, 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 18.

> **\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

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 15.

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 17.

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 9.

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 15.

Cannot authenticate from Lexmark Print

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 9.

Note: To maintain performance, solution settings are cached, so 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 .

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 .

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)

Appendix

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.

Solutions setting index

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.
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 - 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.
[*] The default value of a setting.			

Setting	Can be local	Values	Description
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.
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.
[*] The default value of a setting.			

Setting	Can be local	Values	Description
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.
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, and users in different domains can use the printer.
LDAP Server	X	<Any text string>	The LDAP server used for authentication.

* The default value of a setting.

Setting	Can be local	Values	Description
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.
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.
* The default value of a setting.			

Setting	Can be local	Values	Description
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 LDAP Custom Attribute 2 LDAP Custom Attribute 3	X	<Any text string>	Lets you specify more LDAP attributes in tracked usage data.
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.
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.

[*] The default value of a setting.

Setting	Can be local	Values	Description
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.
Fax - Track Destination	X	Yes No*	Tracks fax destination numbers after completing a fax job.
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**.
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.			

Notices

Edition notice

December 2023

The following paragraph does not apply to any country where such provisions are inconsistent with local law: LEXMARK INTERNATIONAL, INC., PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions; therefore, this statement may not apply to you.

This publication could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in later editions. Improvements or changes in the products or the programs described may be made at any time.

References in this publication to products, programs, or services do not imply that the manufacturer intends to make these available in all countries in which it operates. Any reference to a product, program, or service is not intended to state or imply that only that product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any existing intellectual property right may be used instead. Evaluation and verification of operation in conjunction with other products, programs, or services, except those expressly designated by the manufacturer, are the user's responsibility.

For Lexmark technical support, go to **http://support.lexmark.com**.

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

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

© **2019 Lexmark International, Inc.**

All rights reserved.

Trademarks

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

Apple, Macintosh, Mac, OS X, and AirPrint are trademarks of Apple Inc., registered in the U.S. and other countries. Use of the Works with Apple badge means that an accessory has been designed to work specifically with the technology identified in the badge and has been certified by the developer to meet Apple performance standards.

Google Chrome and Android are trademarks of Google LLC.

Adobe and PostScript are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

All other trademarks are the property of their respective owners.

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.

Index