Document Distributor

Version 5.6

Administrator's Guide

March 2022

www.lexmark.com

Contents

Overview

Lexmark™ Document Distributor (LDD) is a system that captures paper documents and converts them to digital format. It also captures existing digital documents, and then processes and routes these documents according to your business processes. Users can submit paper documents from multifunction products (MFPs), or digital documents from individual computers. Some functions, such as print release, can be accessed from some single-function printers (SFPs). For a list of supported printers in each device class, see "Supported printers" on page 11.

Each Lexmark MFP can print, copy, scan, e-mail, and fax. In addition to controlling and adjusting settings for these functions, LDD can add the following functions by using scripts:

- Show messages and prompt the user for input.
- Authenticate through prompts or card swipes.
- Combine scanned documents.
- Read bar codes.
- Use optical character recognition (OCR) to retrieve the text from scanned documents.

  Note: The OCR quality of images for colored documents in .docx format may be different from the quality of images in another format.
- Check or validate information in documents against templates.
- Automatically fill in the fields on a form template from a database or user input.
- Convert documents to specific formats, such as PDF, TIFF, and plain text.
- Route and store documents in a database, network location, or Enterprise Content Management (ECM) system.
- Provide a user confirmation for actions taken.

This document provides instructions on how to install, configure, use, and troubleshoot LDD.

Understanding the stages of a job

Document capture

In this stage, the paper document is converted into a digital document from a printer, or a digital document is selected on a computer. After a user selects a profile, scripts determine how the scanned document is processed and routed. On a printer, commonly used profiles are configured as buttons on the home screen.

Document processing

Document processing takes place on the LDD server after the document capture stage is complete. In this stage, scripts that are associated with the profile analyze or modify the document.

Common tasks in document processing are the following:

- Reading bar codes
- OCR
- Image processing and manipulation

Document routing

The main function of LDD is delivering captured documents to other systems. In this stage, LDD automatically prints, faxes, e-mails, or archives the document without further user intervention. A document is routed to either one destination or multiple destinations.

LDD can route documents to any of the following destinations:

- ECM software platforms, such as Microsoft SharePoint and EMC Documentum
- E-mail recipients
- Fax recipients
- Network folders
- FTP locations
- Printers

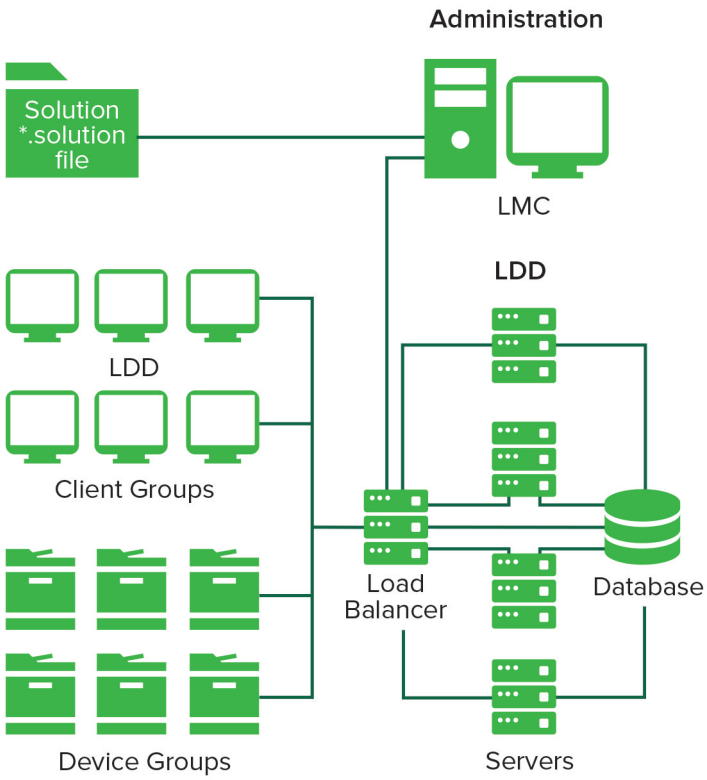
Confirmation

After document capture, processing, and routing, the user can be provided with feedback indicating the status of a job. A custom report may be printed, or for e-Task 2 or later printers, a confirmation can be shown on the screen. Other LDD services can also be used for confirmation purposes. For example, an e-mail notification can be sent to the user or other recipients each time a job is completed.

Understanding the Lexmark Document Distributor system

System components

- **Clients**—Clients can be either printers or workstations that use the Microsoft Windows application software Select'N'Send or the Lexmark Document Server Printer Port. The document capture and confirmation stages of a job occur at a client. In printer clients, prompts may be presented to the user to collect information during document processing and document routing.
- **Load balancer**—Receives jobs from clients and balances those jobs across servers, providing a transition between the document capture and document processing stages of a job.
- **LDD servers**—Process incoming jobs, which manage the document processing and document routing stages of a job.
- **Database**—Maintains information about clients, solutions, settings, and jobs.



Reliability, scalability, and disaster recovery

Reliability

To increase system reliability, we recommend having at least two server computers that are connected to a separate database and load balancer computers. If one server fails, then the load balancer directs jobs to other servers until the failed server is online again. Using a Microsoft Cluster Server (MSCS), pair each load balancer and database in a failover cluster. This configuration keeps the system online when a load balancer or database fails.

Scalability

To support many clients, LDD submits jobs to as many servers as required to handle the load. The load balancer maintains system performance by selecting a server for each received job, and then distributing the total load.

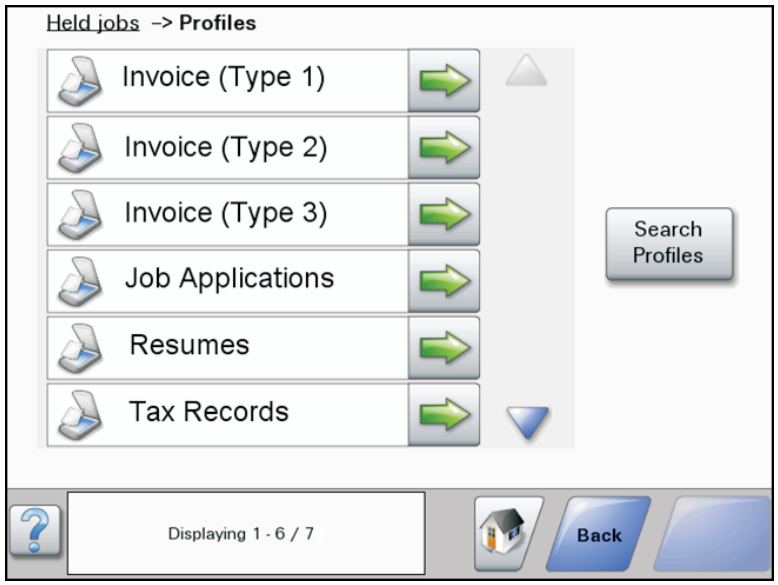
To manage load balancing in the system, LDD uses a Tomcat Connector. The default balancing method estimates the number of open sessions by counting requests to the system that do not have a session cookie. The server with the lowest number of estimated sessions is selected to process the request.

Disaster recovery

LDD lets you back up the databases and solutions from the database and load balancer to a network folder. If a recovery becomes necessary, then a new load balancer or database accesses the recovery data by using Restore Install. If necessary, existing servers are directed to the new database or load balancer, or new servers are installed.

Workflow solutions

In LDD, a workflow solution determines the specifics of each stage of a job to meet a business need. A workflow solution provides a new profile or job type that a user can initiate on a printer or software client to which it is deployed. Some solutions, however, may be scheduled to run at particular times.



A workflow solution contains one or more of the following elements:

- **Script**—Defines the actions executed when a solution is initiated. Scripts can be static, or they may require user input for processing and routing documents. For example, a script that processes bank loans may require more user inputs, such as a branch name, account number, or Social Security number.
- **Policy**—The settings for the solution and the printers to which it is deployed, which are the following:
  - **Device settings**—The required printer configuration to support the jobs. This configuration usually includes profiles but can include almost any device setting.
  - **Solution settings**—Settings that let you adjust jobs or printer configurations. Some settings are global to the solution across all printers, while others vary from one group of printers to another.
- **Embedded Solution Framework (eSF) application**—An application that is installed on printers to provide functionality needed by the solution, such as delayed sending of scanned documents.
- **Components**—JAR files that provide services not available in the base LDD installation, such as interaction with a custom ECM system.
- **Formsets**—Custom form files that are used for merging data with standard forms.
- **Custom reports**—Reports that a solution developer designs.

Client software

Client software is used to submit files from a Windows operating system computer to the LDD system for processing. A computer that uses client software is a *software client*. LDD can process documents submitted through client software in the same way as documents scanned at a printer.

Note: For more information on the latest LDD port monitor support, see the *Readme* file.

The following are the two types of client software:

- **Select'N'Send**—Users send files directly to LDD and select LDD profiles to use in processing the sent files. Selected files are submitted to the system in their current formats. This client software is a Windows operating system application that has both a command-line utility and a graphical user interface (GUI) version.

  Note: The Microsoft Windows application software Select'N'Send does not support prompting from an LDD server system profile.

- **Lexmark Document Server Printer Port**—Users submit documents to LDD by printing from any Windows operating system application to a print queue assigned to the port. Printed documents are submitted to the system in the format determined by the print driver used with the print queue.

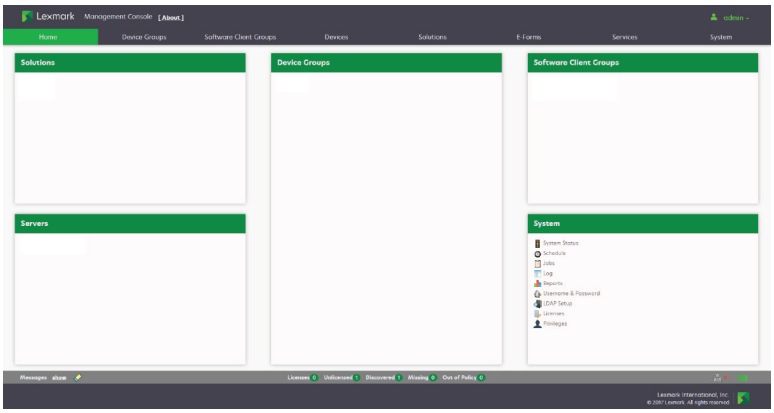
  An LDD printer port can be assigned to an LDD server system profile that prompts for user input at the time of printing. The profile or script running on the LDD server system that the LDD printer port is assigned to controls the prompting. For LDD printer port prompting, install the LDD port monitor software on the computer. Create and assign the LDD printer port to a profile that prompts to an existing print queue.

  Notes:

  - The LDD printer port allows printers that belong to a solution to accept multiple domain configurations. This feature allows a solution to distinguish the same user name across multiple domains. A user's domain name, legacy account name, principal name, or fully qualified distinguished name can be shown when viewing jobs from a solution.
  - LDD printer port prompting is not supported on print servers. If it is configured on a print server, then the spooler stops responding and may crash when print jobs start going into the print server. You can still use LDD printer ports on print servers, but you can assign them only to profiles that do not prompt.
  - Configure the nonprompting profiles with a property in the SDK that specifies that the profile does not prompt. It helps improve the performance of an LDD printer port assigned to a nonprompting profile. For more information, see the *Lexmark Document Distributor SDK Guide*.

Lexmark Management Console

Lexmark Management Console (LMC) provides system administration for LDD. LMC is a web application hosted on LDD servers and accessed through the computer where the load balancer is installed. LMC is accessible from anywhere on the network by using a supported browser.



Security overview

- **Administrative security**—LMC is password protected so that only authorized administrators can access it.
- **User authentication**—Printers may require users to log in to run profiles. Text and password prompts are available for use in scripts. Kerberos authentication is available for use only with printers that support it.

  Note: Enable secure communication between printers and servers in LMC for any device group that uses a solution with Kerberos authentication.
- **Data encryption**—Data encryption is available for communication between any two LDD system components or with any Lexmark printer that supports encryption. Encryption for communication between LDD system components is accomplished by using either of the following:
  - Transport Layer Security (TLS) version 1.2 in the Advanced Prompting Bundle (AP Bundle)

    Note: Only e-Task 5, e-Task 4, and some versions of e-Task 3 printers support TLS version 1.2.
  - Internet Protocol Security (IPsec) through your operating system

  Encryption for communication with printers can be enabled for each device group in LMC.

System setup overview

The different stages of the system setup process are represented in the following steps:

1. Activate the appropriate licenses, and then install the database, load balancer, and servers. For more information, see “Installing Lexmark Document Distributor” on page 22.
2. Perform initial system configuration, including setting up device groups, discovering printers, and scheduling a backup. For more information, see “Managing device groups and devices” on page 102 and “Backup and disaster recovery” on page 85.
3. Deploy solutions to printers. For more information, see “Managing solutions” on page 92.
4. If you are using software clients, then configure software client groups and install client software. For more information, see “Managing software clients” on page 121.
5. Test deployed solutions on printers and software clients. For more information, see “Testing and using Lexmark Document Distributor solutions” on page 130.

Supported printers

Multifunction products

Supported mono printers

Model	Print Release	Print tracking	Copy tracking	Badge authentication	User ID authentication	PIN authentication
MX310	✔[2]	✔	x	✔[2]	x	x
MX931	✔	✔	✔	✔	✔	✔
MX410	✔	✔	✔	x	✔	✔
MX421ade	✔	✔	✔	✔	✔	✔
MX51x	✔	✔	✔	✔	✔	✔
MX521de, MX521ade	✔	✔	✔	✔	✔	✔
MX522adhe	✔	✔	✔	✔	✔	✔
MX61x	✔	✔	✔	✔	✔	✔
MX622ade, MX622adhe	✔	✔	✔	✔	✔	✔
MX6500e	✔	✔	✔	✔	✔	✔
MX71x	✔	✔	✔	✔	✔	✔
MX721ade, MX721adhe	✔	✔	✔	✔	✔	✔
MX722ade, MX722adhe	✔	✔	✔	✔	✔	✔
MX81x	✔	✔	✔	✔	✔	✔
MX822ade, MX822adxe	✔	✔	✔	✔	✔	✔
MX826ade, MX826adxe	✔	✔	✔	✔	✔	✔
MX91x	✔	✔	✔	✔	✔	✔
X204	✔[2]	✔	x	✔[2]	x	x
X264	✔[2]	✔	x	✔[2]	x	x
X342	✔[2]	✔	x	✔[2]	x	x
X364, X363	✔[2]	✔	x	✔[2]	x	x

[1] Requires base memory upgrade to 256MB for eSF support.

[2] Requires Print Release Adapter RFIDeas 241.

[3] Not claiming support for this release.

Model	Print Release	Print tracking	Copy tracking	Badge authentication	User ID authentication	PIN authentication
X464, X463	✔	✔	✔	✔[1]	✔	✔
X466	✔	✔	✔	✔	✔	✔
X620	✔	✔	x	✔[2]	✔	✔
X632	✔	✔	x	✔[2]	✔	✔
X634	✔	✔	x	✔[2]	✔	✔
X642	✔	✔	✔	✔	✔	✔
X644	✔	✔	✔	✔	✔	✔
X646	✔	✔	✔	✔	✔	✔
X651	✔	✔	✔	✔	✔	✔
X652	✔	✔	✔	✔	✔	✔
X654	✔	✔	✔	✔	✔	✔
X656	✔	✔	✔	✔	✔	✔
X658	✔	✔	✔	✔	✔	✔
X820	✔	✔	x	✔[2]	✔	✔
X830	✔	✔	x	✔[2]	✔	✔
X832	✔	✔	x	✔[2]	✔	✔
X850	✔	✔	✔	✔	✔	✔
X852	✔	✔	✔	✔	✔	✔
X854	✔	✔	✔	✔	✔	✔
X860	✔	✔	✔	✔	✔	✔
X862	✔	✔	✔	✔	✔	✔
X864	✔	✔	✔	✔	✔	✔
XM1145	✔	✔	✔	✔	✔	✔
XM1242	✔[3]	✔[3]	✔[3]	✔[3]	✔[3]	✔[3]
XM1246	✔	✔	✔	✔	✔	✔
XM3150	✔	✔	✔	✔	✔	✔
XM3250	✔	✔	✔	✔	✔	✔
XM5163	✔	✔	✔	✔	✔	✔
XM5170	✔	✔	✔	✔	✔	✔
XM5370	✔	✔	✔	✔	✔	✔

[1] Requires base memory upgrade to 256MB for eSF support.

[2] Requires Print Release Adapter RFIDeas 241.

[3] Not claiming support for this release.

Model	Print Release	Print tracking	Copy tracking	Badge authentication	User ID authentication	PIN authentication
XM71xx	✔	✔	✔	✔	✔	✔
XM7355	✔	✔	✔	✔	✔	✔
XM7370	✔	✔	✔	✔	✔	✔
XM91x	✔	✔	✔	✔	✔	✔
XC9465	✔	✔	✔	✔	✔	✔

[1] Requires base memory upgrade to 256MB for eSF support.

[2] Requires Print Release Adapter RFIDeas 241.

[3] Not claiming support for this release.

Supported color printers

Model	Print Release	Print tracking	Copy tracking	Badge authentication	User ID authentication	PIN authentication
CX310	✔[2]	✔	x	✔[2]	x	x
CX410	✔	✔	✔	✔[2]	✔	✔
CX510	✔	✔	✔	✔	✔	✔
CX522ade	✔	✔	✔	✔	✔	✔
CX622ade, CX622adhe	✔	✔	✔	✔	✔	✔
CX625ade, CX625adhe	✔	✔	✔	✔	✔	✔
CX725	✔	✔	✔	✔	✔	✔
CX730	✔	✔	✔	✔	✔	✔
CX735	✔	✔	✔	✔	✔	✔
CX820	✔	✔	✔	✔	✔	✔
CX825	✔	✔	✔	✔	✔	✔
CX860	✔	✔	✔	✔	✔	✔
CX921de	✔	✔	✔	✔	✔	✔
CX922de	✔	✔	x	✔	✔	✔
CX923dte, CX923dxe	✔	✔	✔	✔	✔	✔
CX924dte, CX924dxe	✔	✔	✔	✔	✔	✔

[1] Requires base memory upgrade to 256MB for eSF support.

[2] Requires Print Release Adapter RFIDeas 241.

[3] Not claiming support for this release.

Model	Print Release	Print tracking	Copy tracking	Badge authentication	User ID authentication	PIN authentication
CX930	✔	✔	✔	✔	✔	✔
CX931	✔	✔	✔	✔	✔	✔
CX942	✔	✔	✔	✔	✔	✔
CX943	✔	✔	✔	✔	✔	✔
CX944	✔	✔	✔	✔	✔	✔
X500	x	x	x	x	x	x
X502	x	x	x	x	x	x
X543	✔[2]	✔	x	✔[2]	x	x
X544	✔[2]	✔	x	✔[2]	x	x
X546	✔[2]	✔	x	✔[2]	x	x
X548	✔	✔	✔	✔	✔	✔
X560	✔	✔	x	✔[2]	x	x
X734	✔[2]	✔	✔	✔	✔	✔
X736	✔	✔	✔	✔	✔	✔
X738	✔	✔	✔	✔	✔	✔
X746	✔	✔	✔	✔	✔	✔
X748	✔	✔	✔	✔	✔	✔
X752	✔	✔	x	✔[2]	✔	✔
X772	✔[3]	✔	x	✔[2]	x	x
X782	✔[3]	✔	✔	✔	✔	✔
X792	✔	✔	✔	✔	✔	✔
X912	✔	✔	x	✔[2]	✔	✔
X925	✔	✔	✔	✔	✔	✔
X940	✔	✔	✔	✔	✔	✔
X945	✔	✔	✔	✔	✔	✔
X950	✔	✔	✔	✔	✔	✔
X952	✔	✔	✔	✔	✔	✔
X954	✔	✔	✔	✔	✔	✔
XC2132	✔	✔	✔	✔	✔	✔
XC2235	✔	✔	✔	✔	✔	✔

[1] Requires base memory upgrade to 256MB for eSF support.

[2] Requires Print Release Adapter RFIDeas 241.

[3] Not claiming support for this release.

Model	Print Release	Print tracking	Copy tracking	Badge authentication	User ID authentication	PIN authentication
XC4140	✔	✔	✔	✔	✔	✔
XC4150	✔	✔	✔	✔	✔	✔
XC4240	✔	✔	✔	✔	✔	✔
XC4342	✔	✔	✔	✔	✔	✔
XC4352	✔	✔	✔	✔	✔	✔
XC6152	✔	✔	✔	✔	✔	✔
XC8155	✔	✔	✔	✔	✔	✔
XC8160	✔	✔	✔	✔	✔	✔
XC9235	✔	✔	✔	✔	✔	✔
XC9245	✔	✔	✔	✔	✔	✔
XC9255	✔	✔	✔	✔	✔	✔
XC9265	✔	✔	✔	✔	✔	✔
XC9325	✔	✔	✔	✔	✔	✔
XC9335	✔	✔	✔	✔	✔	✔
XC9445	✔	✔	✔	✔	✔	✔
XC9455	✔	✔	✔	✔	✔	✔
XC9465	✔	✔	✔	✔	✔	✔

[1] Requires base memory upgrade to 256MB for eSF support.

[2] Requires Print Release Adapter RFIDeas 241.

[3] Not claiming support for this release.

Single-function printers

Supported mono printers

Model	Print Release	Print tracking	Badge authentication	User ID authentication	PIN authentication
E120	✔[2]	✔	✔[2]	x	x
E250	✔[2]	✔[1]	✔[2]	x	x
E260	✔[2]	✔	✔[2]	x	x
E350	✔[2]	✔[1]	✔[2]	x	x
E352	✔[2]	✔	✔[2]	x	x
E360	✔[2]	✔	✔[2]	x	x

[1] Requires base memory upgrade to 256MB for eSF support.

[2] Requires Print Release Adapter RFIDeas 241.

[3] Not claiming support for this release.

Model	Print Release	Print tracking	Badge authentication	User ID authentication	PIN authentication
E450	✔[3]	✔	✔[2]	x	x
E460	✔	✔	✔[2]	x	✔
E462	✔	✔	✔[2]	x	✔
M3150	✔	✔	✔	✔	✔
M3250	✔	✔	✔	✔	✔
M5155	✔	✔	✔	✔	✔
M5163	✔	✔	✔	✔	✔
M5170	✔	✔	✔	✔	✔
M5255	✔	✔	✔	✔	✔
M5270	✔	✔	✔	✔	✔
MS310	✔[2]	✔	✔[2]	x	x
MS410	✔[2]	✔	✔[2]	x	x
MS510	✔[2]	✔	✔[2]	x	x
MS610dn	✔[2]	✔	✔[2]	x	x
MS610dte, MS610de	✔	✔	✔	✔	✔
MS622de	✔	✔	✔	✔	✔
MS710 , MS711	✔[2]	✔	✔[2]	x	x
MS810de	✔	✔	✔	✔	✔
MS810n, , MS810dn	✔[2]	✔	✔[2]	x	x
MS811	✔[2]	✔	✔[2]	x	x
MS812de	✔	✔	✔	✔	✔
MS812dn	✔[2]	✔	✔[2]	x	x
MS822de	✔	✔	✔	✔	✔
MS824de	✔	✔	✔	✔	✔
MS826de	✔	✔	✔	✔	✔
MS910	✔	✔	✔	✔	✔
T640	✔	✔	✔[2]	x	✔
T642	✔	✔	✔[2]	x	✔
T644	✔[3]	✔	✔[2]	x	✔

[1] Requires base memory upgrade to 256MB for eSF support.

[2] Requires Print Release Adapter RFIDeas 241.

[3] Not claiming support for this release.

Model	Print Release	Print tracking	Badge authentication	User ID authentication	PIN authentication
T650	✔	✔	✔[2]	x	✔
T652	✔	✔	✔[2]	x	✔
T654	✔	✔	✔	x	✔
T656	✔	✔	✔	x	✔
W840	✔[3]	✔	✔[2]	x	✔
W850	✔	✔	✔	x	✔
W852	✔	✔	✔	x	✔
W854	✔	✔	✔	x	✔

[1] Requires base memory upgrade to 256MB for eSF support.

[2] Requires Print Release Adapter RFIDeas 241.

[3] Not claiming support for this release.

Supported color Printers

Model	Print Release	Print tracking	Badge authentication	User ID authentication	PIN authentication
C2240	✔	✔	✔	✔	✔
C4150	✔	✔	✔	✔	✔
C4342	✔	✔	✔	✔	✔
C4352	✔	✔	✔	✔	✔
C500	x	x	x	x	x
C520	✔	✔	✔[2]	x	✔
C522	✔[3]	✔	✔[2]	x	✔
C524	✔[3]	✔	✔[2]	x	✔
C530	✔[2]	✔	✔[2]	x	x
C532	✔[2]	✔	✔[2]	x	x
C534	✔[3]	✔	✔[2]	x	✔
C540	✔[2]	✔	✔[2]	x	x
C543	✔[2]	✔	✔[2]	x	x
C544	✔[2]	✔	✔[2]	x	x
C546	✔	✔	✔[2]	x	✔
C6160	✔	✔	✔	✔	✔
C734	✔	✔	✔[2]	x	✔

[1] Requires eSF-capable C736 part numbers.

[2] Requires Print Release Adapter RFIDeas 241.

[3] Not claiming support for this release.

Model	Print Release	Print tracking	Badge authentication	User ID authentication	PIN authentication
C736	✔	✔	✔[1]	✔[1]	✔
C746	✔	✔	✔[2]	x	✔
C748	✔	✔	✔	✔	✔
C780	✔	✔	✔[2]	x	✔
C782	✔	✔	✔[2]	x	✔
C792	✔	✔	✔	✔	✔
C920	✔[3]	✔	✔[2]	x	✔
C925	✔[3]	✔	✔	✔	✔
C935	✔	✔	✔[2]	x	✔
C950	✔	✔	✔	✔	✔
CS310	✔[2]	✔	✔[2]	x	x
CS410	✔[2]	✔	✔[2]	x	x
CS510	✔	✔	✔	✔	✔
CS622de	✔	✔	✔	✔	✔
CS720	✔	✔	✔	✔	✔
CS725	✔	✔	✔	✔	✔
CS730	✔	✔	✔	✔	✔
CS735	✔	✔	✔	✔	✔
CS820	✔	✔	✔	✔	✔
CS921de	✔	✔	✔	x	x
CS923de	✔	✔	✔	✔	✔
CS943	✔	✔	✔	✔	✔
XS925	✔	✔	✔	✔	✔
XS955dhe	✔	✔	✔	✔	✔

[1] Requires eSF-capable C736 part numbers.

[2] Requires Print Release Adapter RFIDeas 241.

[3] Not claiming support for this release.

Notes:

- For more information on the latest device and firmware level support, see the *Readme* file.
- Some printer models do not support double-byte characters. For more information, see “Double-byte character support” on page 19.

Prompts supported by SFPs

Some prompts may not be supported in some printer models.

	Touch-screen printers	Non-touch-screen printers
Supported prompts	• ArrayPrompt • AuthenticationPrompt[1] • BooleanPrompt • CustomVImlPrompt • ImageBooleanPrompt • ImageListPrompt • ImageMessagePrompt • IntegerPrompt • ListPrompt • MessagePrompt • NumericPrompt • PasswordPrompt • StringPrompt • NullPrompt	• ArrayPrompt • AuthenticationPrompt[1, 2] • BooleanPrompt • IntegerPrompt • ListPrompt • MessagePrompt • NumericPrompt • PasswordPrompt[3] • StringPrompt[2] • NullPrompt[4]

[1] Requires a supported card reader.

[2] Supported by T654 and W850 models only.

[3] Supports numeric PINs only in e-Task printers. Supported e-Task printers include C520, C522, C524, C530, C532, C534, C732, C734, C736, C780, C782, C920, C935, E450, E460, E642, T640, T642, T644, T650, T652, W840.

[4] Supported by e-Task printers only.

Double-byte character support

Double-byte characters may not be supported in some printer models.

Printer model	Simplified Chinese	Traditional Chinese	Japanese	Korean
6500	✓	✓	✓	✓
C748	✓	✓	✓	✓
C792	✓	✓	✓	✓
C925	✓	✓	✓	✓
C950	✓	✓	✓	✓
CS510	✓	✓	✓	✓
CS720	✓	✓	✓	✓
CS725	✓	✓	✓	✓
CS820	✓	✓	✓	✓
CS921	✓	✓	✓	✓
CS923	✓	✓	✓	✓

Printer model	Simplified Chinese	Traditional Chinese	Japanese	Korean
CX410	✓	✓	✓	✓
CX510	✓	✓	✓	✓
CX725	✓	✓	✓	✓
CX820	✓	✓	✓	✓
CX825	✓	✓	✓	✓
CX860	✓	✓	✓	✓
CX920	✓	✓	✓	✓
CX921	✓	✓	✓	✓
CX922	✓	✓	✓	✓
CX923	✓	✓	✓	✓
CX924	✓	✓	✓	✓
MS610	✓	✓	✓	✓
MS810, MS812, MS911	✓	✓	✓	✓
MX410, MX510, MX511	✓	✓	✓	✓
MX610, MX611	✓	✓	✓	✓
MX710, MX711	✓	✓	✓	✓
MX810, MX811, MX812	✓	✓	✓	✓
MX910, MX911, MX912	✓	✓	✓	✓
X463, X464, X466	✓	✓	X	✓
X548	✓	✓	✓	✓
X642	✓	X	X	X
X644, X646	✓	X	X	✓
X651, X652, X654, X656, X658	✓	✓	X	✓
X734, X736, X738	✓	✓	X	✓
X746, X748	✓	✓	✓	✓
X782	✓	X	X	✓
X792	✓	✓	✓	✓
X850, X852, X854	✓	X	✓	✓

Printer model	Simplified Chinese	Traditional Chinese	Japanese	Korean
X860, X862, X864	✓	✓	X	✓
X925	✓	✓	✓	✓
X940, X945	✓	X	✓	✓
X950, X952, X954	✓	✓	✓	✓

Supported ECM software platforms

- ImageNow 6.7 and 6.6
- Microsoft SharePoint
  - Microsoft SharePoint Foundation 2010
  - Microsoft SharePoint 2010
  - Microsoft Office SharePoint Server 2007
  - Windows SharePoint Services 3.0
- Autonomy iManage WorkSite with WorkSite Server 8.5 or 8.2

Notes:

- Integration with ECM systems may require specific licenses.
- For ECM platforms without direct integration, the LDD system saves documents and metadata to a directory where an ECM system is configured to poll for files.

Installing Lexmark Document Distributor

System requirements

Note: To install the bar code component, make sure that .Net Framework version 3.5 or later is enabled as a Windows Server role or feature.

Category	Required	Recommended for enterprise systems
Operating system	• Windows Server 2022 • Windows Server 2019 • Windows Server 2016 Core Edition **Note:** To use the core server, make sure that Service Pack 6 for Visual Basic 6.0: Run-Time Redistribution Pack is installed. • Windows Server 2016 Standard Edition (x64) • Windows Server 2012 R2 Standard or Enterprise Edition (x64) • Windows Server 2012 Standard or Enterprise Edition (x64) • Windows Server 2008 R2 SP1* • Windows Server 2008 Standard or Enterprise Edition with SP2 (x86 and x64)*	• Windows Server 2019 • Windows Server 2016 Standard Edition (x64) • Windows Server 2012 R2 (x64) • Windows Server 2008 R2 SP1*
Processor	2GHz dual-core	Dual 2.5GHz quad-core Intel Xeon or AMD Opteron
RAM	4GB	8GB
Note: Install the database on the fastest available hardware with the fastest disk I/O infrastructure. * In LDD 5.4 or later, Windows Server 2008 is not supported.		

Category	Required	Recommended for enterprise systems
Hard disk drive	20GB free space for each system component	Configuration 1-N, X-N, or X-Y-N: • Database and load balancer – The operating system and server configured for LMC are installed on two 15000 RPM Serial Attached SCSI drives. The drives are configured as a RAID 1 array with at least 80GB free space. – The database and load balancer are installed on four 15000 RPM Serial Attached SCSI drives. The drives are configured as a RAID 5 array with at least 300GB free space. • Servers – The operating system and server configured for jobs are installed on four 15000 RPM Serial Attached SCSI drives. The drives are configured as a RAID 5 array with at least 80GB free space. **Note:** For more information, see "Assigning servers to run LMC only or process jobs" on page 74.
Network speed	100Mbps network **Note:** For solutions that require intensive processing and more network traffic, use Gigabit Ethernet.	Gigabit Ethernet using dual-port network adapters
Network name resolution	Domain Name System (DNS) or Windows Internet Name Service (WINS) **Notes:** • Local hosts files can be used instead of external DNS. • For other network systems support, contact your Lexmark representative.	N/A
Static addressing	• In databases installed on a cluster • In load balancers installed on a cluster • In load balancers in a system with printers • In load balancers in a system with printers not configured to a DNS server	In all system components and any printer used with the system

Note: Install the database on the fastest available hardware with the fastest disk I/O infrastructure.

* In LDD 5.4 or later, Windows Server 2008 is not supported.

Category	Requirement
Browser	• Internet Explorer 11.0 or later • Mozilla Firefox • Google Chrome™ • Microsoft Edge **Notes:** • Make sure that JavaScript is enabled on your web browser. • Make sure that your web browser allows cookies for the address where you access LMC.
Video	Capable of showing a resolution of 1024 x 768 or higher.

Category	Requirement
Virtual machine monitor	VMware ESX software 3.0.1 or later VMware vSphere software 4.x or later
Note: We do not recommend installing the database on a virtual machine.	

Client software operating system compatibility

The Microsoft Windows application software Select'N'Send and the Lexmark Document Server Printer Port can be used on the following operating systems:

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016 Standard Edition (x64)
- Windows Server 2012 R2 Standard or Enterprise Edition (x64)
- Windows Server 2012 Standard or Enterprise Edition (x64)
- Windows Server 2008 R2 Standard or Enterprise Edition (x64)
- Windows Server 2008 Standard or Enterprise Edition with SP2
- Windows 11
- Windows 10
- Windows 8.1
- Windows 8
- Windows 7 with SP1
- Windows Vista with SP2

Notes:

- Enterprise Editions and Enterprise x64 Editions of Windows Server support an active/passive or active/active clustered print server with the Lexmark Document Server Printer Port.
- In LDD 5.4 or later, Windows Server 2008 is not supported.

Supported database servers

- Firebird® (default)
- Microsoft SQL Server 2019 Standard or Enterprise Edition
- Microsoft SQL Server 2017 Standard or Enterprise Edition

- Microsoft SQL Server 2016 Standard or Enterprise Edition
- Microsoft SQL Server 2014 Standard or Enterprise Edition
- Microsoft SQL Server 2012 Standard or Enterprise Edition
- Microsoft SQL Server 2008 R2 Standard or Enterprise Edition

Note: LDD does not support Microsoft SQL Server Express.

Ports used by the LDD system

Allow communication through the following ports on the network:

Notes:

- Ports depend on the implementation of each LDD system and may differ from the listing in the following table.
- The LDD administrator determines the ports used by forms printers.
- SSL communication is no longer supported in LDD 4.8.5 or later.
- To ensure restricted access to the following ports, apply the appropriate firewall restriction policy. For example, to configure restricted access to the Firebird database, see “Setting up firewall access for Firebird” on page 26.

Component	Port	Protocol	Function
Database (Firebird)	3050	TCP	Database communications
	8001	TCP	Backup or restore agent
Load balancer	443	TCP	Load balancer HTTPS TLS communications, including LMC
	4113	TCP	Web adapter (JMX)
	9700	TCP	Profile submission to e-Task printers, web adapter (JMX)
	9705	TCP	Apache® agent
	9780	TCP	Load balancer communications, including LMC
	9783	TCP	Load balancer HTTPS TLS communications, including LMC
Server	4111	TCP	JMX
	5111	TCP	RMI
	8009	TCP	AJP or Tomcat connector (load balancer worker)
	9743	TCP	HTTPS TLS profile job submission from printers or client software to a server, including LMC
	9788	TCP	Profile job submission from printers or client software to a server, including LMC

Component	Port	Protocol	Function
Printer	21	TCP	FTP, generic file downloads
	80	TCP	HTTP, device web services
	443	TCP	HTTPS, secure device web services
	8080	TCP	HTTP, device web services communication
	79	TCP	Finger
	161	UDP	SNMP, device discovery
	5000	TCP	Policy updates, ObjectStore plain text communication
	5353	UDP	Multicast DNS
	6000	UDP	Device discovery, ObjectStore communication using XML protocol
	6100	UDP	Device discovery, policy updates, Lexmark Secure Transport (LST) encrypted data
	6110	TCP	Device discovery, policy updates, LST authentication, and negotiation
	9100	TCP	Printing, policy updates
	9300	UDP	Device discovery, NPA protocol UDP communications
	9500	TCP	NPA protocol TCP communications

Obtaining licenses

- If your Lexmark representative has provided the license files, then save them in a folder that is accessible to the server. Continue with the server installation.
- For more information on licensing, contact your Lexmark representative.

Understanding installation types

You can install two types of LDD systems:

- **Workgroup system**—An LDD installation with a packaged solution for smaller systems. This system lets you install the database, load balancer, client software, and one server on one computer.
- **Enterprise system**—A standard LDD installation for larger systems and more demanding applications. This system lets you install the database, load balancer, and servers on different computers to create a reliable and scalable system.

Setting up firewall access for Firebird

1. From your computer, in the “Windows Firewall with Advanced Security” control panel, click **Inbound Rules** from the “View and create firewall rules” section.
2. Right-click **Inbound Rules**, and then click **New Rule**.
3. From the Rule Type section, select **Custom**, and then click **Next**.

4. From the Program section, select **This program path**, and then browse to the location of the database. Click **Next**.

   Note: The default location of the database is **C:\Program Files\Lexmark\Solutions\firebird\bin\fb_inet_server.exe**.

5. In the "Protocol type" menu, select **TCP**.
6. In the "Local port" menu, select **Specific Ports**, and then enter the port number of the database. Click **Next**.

   Note: The default port number of the database is 3050.

7. When prompted which remote IP addresses the rule applies to, select **These IP addresses**, and then click **Add**.
8. Specify the IP addresses of the server and load balancer, and then click **Next**.
9. From the Action section, select **Allow the connection**, and then click **Next**.
10. If necessary, From the Profile section, select **Domain**, **Private**, and **Public**. Click **Next**.
11. Type a unique name for the inbound rule.
12. Click **Finish**.

Note: Repeat these steps for the UDP protocol type.

Preparing for the installation

Before you begin, make sure that:

- Each system component is installed on a computer with a new Windows operating system installation and with no other software installed.
- Software that includes the following applications are not installed on the same computer where LDD components are installed:
  - Apache Software Foundation Apache HTTP Server software
  - Apache Software Foundation Apache Tomcat software
  - Firebird database server
- Microsoft Internet Information Services (IIS) is not installed.

1. Download the installation package and the license files.

   Note: Save the installation package and the license files in the same location.

2. If necessary, unblock the file properties of the installer:

   From the Properties window of the installation package, click **Unblock**, and then apply the changes.

3. Extract the installation package.

   Notes:

   - To install the bar code component on Windows 2008 R2, make sure that .Net Framework version 3.5 is installed. On Windows 2012 and Windows 2016, make sure that .Net Framework version 4.0 is installed.
   - Make sure that there are no pending restarts from the Lexmark Management Console.

Installing a workgroup system

Configuration type for workgroup systems

Description	Advantage	Disadvantage
Database (DB), load balancer (LB), and server on a single computer 	Minimum equipment	No failover for database or load balancer, limited resources

Installation overview for a workgroup system

1. Configure the computer where you are going to install LDD on the network.
2. Download and activate licenses.
3. Using a workgroup configuration, install LDD.
4. Change the administrator password. If necessary, change the administrator user name.
5. To test function, set all servers online temporarily. For more information, see "Viewing and changing server status" on page 64.

Note: Software clients are managed differently than printers. The client software must be installed later in the system setup process. For more information on managing software clients, see "Managing software clients" on page 121.

Installing system components in a workgroup system

1. From the LDD installation package, run **Setup.exe**.
2. Select a language for the installation, and then click **OK**.
3. From the LDD Setup window, click **Next**.
4. Select **Install LDD system components**, and then click **Next**.
5. Accept the license agreement, and then click **Next**.
6. From the list of components, select **Database**, **Load balancer**, **Server**, and **Client Software**, and then click **Next**.

   Note: You can install optional server components, such as Barcode Read, Barcode Write, and OCR, after the LDD installation.

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

8 For multiple networks, select the IP address of the server that is connected to the same network as your printers, and then click **Next**.

Note: If necessary, select **Allow only IP address**.

9 If you are installing a backup recovery system, then select **Restore Install (RI)**, browse to the .ri file, and then click **Next**.

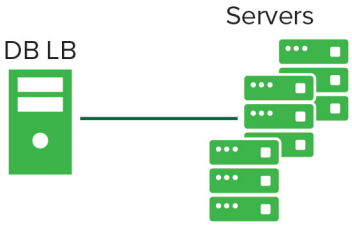
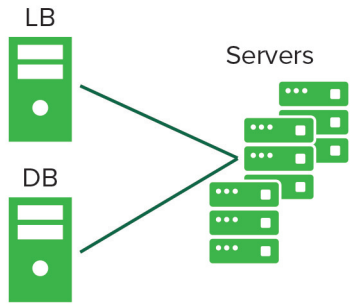
10 Review the setup information, and then click **Next**.

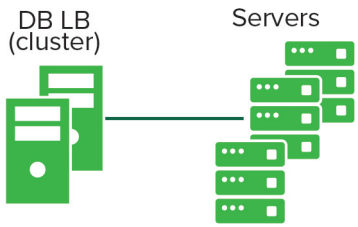
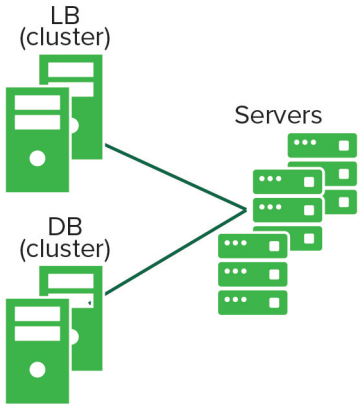
11 Click **Install**.

Installing an enterprise system

Configuration types for enterprise systems

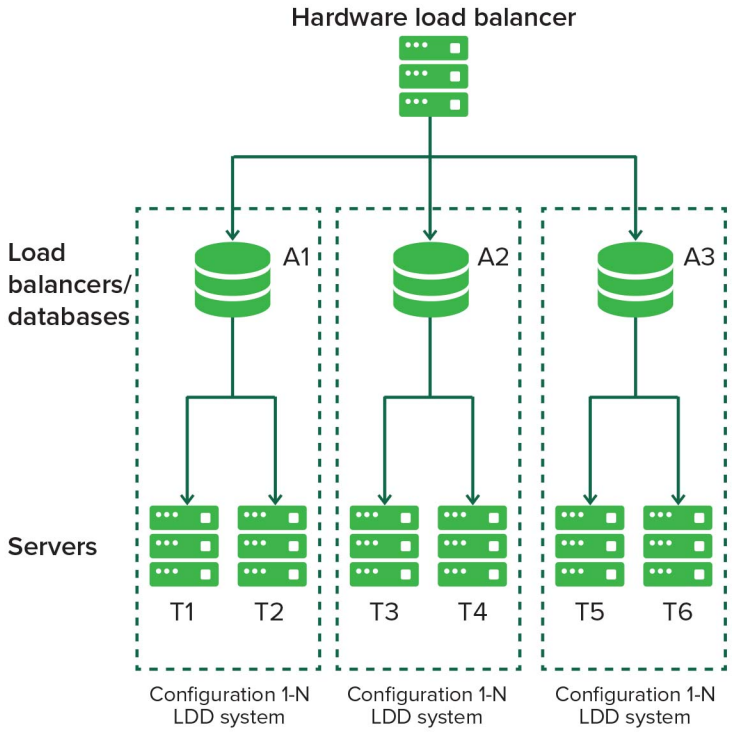
When installing an enterprise system, LDD can be installed by using the following hardware configurations:

Configuration	Description	Advantages	Disadvantages
1-N	The database (DB) and load balancer (LB) are on one computer, and the server is on one or more computers. This setup is the most common when failover is not used. 	Improved performance	Increased hardware needs, no failover for database or load balancer
1-1-N	The database (DB) and load balancer (LB) are on separate computers, and the server is on one or more computers.  **Note:** An external Microsoft SQL Server database may be installed in place of the standard database, resulting in an E-1-N configuration. The external database (E) and load balancer (LB) are on separate computers, and the server is on one or more computers.	Further improved performance	Further increased hardware needs, no failover for database or load balancer

Configuration	Description	Advantages	Disadvantages
X-N	The database (DB) and load balancer (LB) together are on X computers in an MSCS for failover. The server is on one or more computers. This setup is the most common when failover is used.  	High availability, improved performance	Increased hardware needs, cluster licensing
X-Y-N	The database (DB) is on X computers in an MSCS for failover. The load balancer (LB) is on Y computers in an MSCS for failover. The server is on one or more computers.  **Note:** An external Microsoft SQL Server database may be installed in place of the standard database, resulting in an E-Y-N configuration. The external database (E) on X computers and the load balancer (LB) on Y computers are in an MSCS for failover. The server is on one or more computers.	High availability, further improved performance	Further increased hardware needs, cluster licensing

Setting up multiple systems for high availability

When configuring multiple LDD systems, you can connect them to a hardware load balancer or Global Site Selector (GSS). This configuration provides high availability, without using clustering, and increased capacity.



Each system group contains two identical LDD systems. Jobs are balanced between these systems in each group by the hardware load balancer or GSS. If one system fails, then the hardware load balancer or GSS directs jobs to other systems in the group until the failed system is online again.

With this type of setup, you need extra computers and a hardware load balancer or GSS. The configuration of these systems must be identical.

Note: Printers that do not support eSF applications cannot be used with an LDD system that uses a hardware load balancer or GSS.

If a hardware load balancer is used with multiple LDD systems, then configure the hardware load balancer with the following:

- Insert the X-Forwarded-For HTTP header into incoming packets.

  The packets going into the LDD systems must not be from the hardware load balancer of the packet headers. This configuration enables the device or client groups and their settings to work properly.
- Disable cookie-based session persistence.

  If this setting is enabled, then LMC may not work properly when one of the LDD systems is down.
- Set the load balancing algorithm to Round Robin.

  LDD systems work better with Round Robin than other algorithms.

System sizing guidelines

To determine the number of servers required to process jobs efficiently, consider the following factors:

- **Peak demand**—The deciding factor when the average execution time for a solution is less than 30 seconds
- **Concurrency**—The deciding factor when the average execution time for a solution is more than 30 seconds

When installed on the recommended hardware and connected using Gigabit Ethernet, the database can also process 200000 logged messages per hour. When using a typical solution that logs five messages per job, this process generates approximately 40000 jobs per hour. If this limit is reached, then using multiple systems may be necessary.

Peak demand

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

(System-wide hourly job rate) = (system printer capacity) x (jobs per printer per day) / (length of business day)

(Peak demand) = 2 x (system-wide hourly job rate)

(Minimum number of servers) = (peak demand) / (single-server throughput for current solution)

Consider the following example:

- Using the solution, each server in your system can process 3000 jobs per hour.
- Your system has a 300-printer capacity.
- Each printer in your system processes an average of 100 jobs per day.

Perform the following calculations:

1. Determine the system-wide hourly job rate:

   (300 printers) x (100 daily jobs/printer) / (8 hours/day) = **3750 jobs/hour**

2. Determine the peak demand:

   2 x (3750 jobs/hour) = **7500 jobs/hour**

3. Determine the minimum number of servers:

   (7500 jobs/hour) / (3000 jobs/hour) = **2.5**

   Rounding up, the system must have three servers to handle the peak load reliably for a solution with average execution time of less than 30 seconds.

The typical throughputs on a server with the recommended hardware are the following:

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

Note: Using less than the recommended RAM significantly reduces throughput. For example, when using a solution with a heavy processing load, a dual-processor server with only 2GB of RAM can process 600–800 jobs/hour only.

For more information, see the *Lexmark Document Distributor SDK Guide*.

Concurrency

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

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

For example, assume that 1/3 of the 300 printers might be active at the same time:

100 / 30 = **3.33**

Rounding up, the system must have four servers to allow for 100 active printers for a solution with average execution time of less than 30 seconds.

Installation overview for an enterprise system

1. Select a system configuration, and then configure the appropriate hardware on the network.
2. Using a Network Time Protocol (NTP) server, synchronize the time on all computers that are used in the LDD system.
3. Install the system components. Do the following:

   Note: If you are using Firebird database when installing LDD, then the system components can be installed in any order. If you are using Microsoft SQL Server database, then see "Configuring LDD with a Microsoft SQL Server database" on page 41.

   a. Install the database.
   b. Download and activate licenses on the computer where the load balancer must be installed.
   c. Install the load balancer.
   d. If you are using one or more MSCS, then extend the database and load balancer to standby nodes.
   e. Install the servers.

      Note: When installing multiple servers, install one server at a time.
4. Change the administrator password. If necessary, change the administrator user name.
5. To test function, set all servers online temporarily. For more information, see "Viewing and changing server status" on page 64.

Notes:

- To maintain system performance, install the database on the fastest hardware with the fastest disk I/O infrastructure available. Install the servers on the second fastest hardware.
- We recommend using separate physical servers when installing LDD components. If you are using virtual servers, then you can install the LDD components on VMware ESX software 3.0.1 or later.

Installing the database and load balancer without clustering (configurations 1, 1-N, and 1-1-N)

Installing the database

Note: If you are using a Microsoft SQL Server database, then do not install the Firebird database component.

From the system where you want to install the database, do the following:

1. From the LDD installation package, run **Setup.exe**.
2. Select a language for the installation, and then click **OK**.
3. From the LDD Setup window, click **Next**.
4. Select **Install LDD system components**, and then click **Next**.
5. Accept the license agreement, and then click **Next**.
6. From the list of components, select **Database**, and then click **Next**.
7. Specify a location for the installation, and then click **Next**.

   Note: The installation path must not contain double-byte characters.
8. Select your database IP address, and then click **Next**.

   Note: If necessary, select **Allow only IP address**.
9. If you are installing a backup recovery system, then select **Restore Install (RI)**, browse to the .ri file, and then click **Next**.
10. Review the setup information, and then click **Next**.
11. Click **Install**.

Installing the load balancer

From the system where you want to install the load balancer, do the following:

1. From the LDD installation package, run **Setup.exe**.
2. Select a language for the installation, and then click **OK**.
3. From the LDD Setup window, click **Next**.
4. Select **Install LDD system components**, and then click **Next**.
5. Accept the license agreement, and then click **Next**.
6. From the list of components, select **Load balancer**, and then click **Next**.
7. Specify a location for the installation, and then click **Next**.

   Note: The installation path must not contain double-byte characters.
8. Select your load balancer IP address, and then click **Next**.

   Note: If necessary, select **Allow only IP address**.
9. Specify the host name or IP address of the database, select the database type, and then click **Next**.

Notes:

- If you are installing a Microsoft SQL Server database, then make sure that the database is installed before proceeding with the load balancer installation.
- To allow the domain account to access the Microsoft SQL Server database, enable integrated security when installing the database. Make sure that the domain account is granted access to the Microsoft SQL Server database. It must also have full control privileges to the LDD installation path on the application servers and all its subfolders.
- Do not use **`localhost`** or the loopback IP address (**`127.0.0.1`**) for the location of the database.
- When you are installing a configuration other than configuration 1, set the location of the database during installation. If the database is moved, or the IP address of the database changes, then reinstall the load balancer. For more information on changing the IP address of a configuration 1 system, see "Changing the IP address on a configuration 1 system" on page 66.

10 If you are installing a backup recovery system, then select **Restore Install (RI)**, browse to the .ri file, and then click **Next**.

11 Review the setup information, and then click **Next**.

12 Click **Install**.

Installing the database and load balancer with clustering (configurations X-N and X-Y-N)

Before you begin, make sure that:

- The failover clusters are using Microsoft Windows Server clustering services.
- A firewall is not blocking any physical and logical nodes in the cluster.

Setting up firewall exceptions on a Windows Server 2008 or Windows Server 2012 cluster node

1 Create a temporary directory.

2 From the **install\Cluster_Config_Script** folder of the installation package, copy the batch files to the temporary directory.

3 Run the command prompt as an administrator, and then access the temporary directory.

4 Run the batch files.

Note: If you are using a Microsoft SQL Server database, then do not run the database firewall batch file.

Installing the database

Notes:

- If you are using a Microsoft SQL Server database, then do not install the Firebird database component.
- If you are installing on an MSCS, then install Microsoft Visual C++ 2005 Redistributable Package on all servers in the cluster.

1 From the LDD installation package, run **Setup.exe**.

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

3 From the LDD Setup window, click **Next**.

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

5 Accept the license agreement, and then click **Next**.

6 From the list of components, select **Database**, and then click **Next**.

7 Specify a location on a shared cluster disk for the installation, and then click **Next**.

Note: The installation path must not contain double-byte characters.

8 Select the host name or IP address of the logical host of the cluster, and then click **Next**.

Note: If necessary, select **Allow only IP address**.

9 If you are installing a backup recovery system, then select **Restore Install (RI)**, browse to the .ri file, and then click **Next**.

10 Review the setup information, and then click **Next**.

11 Click **Install**.

Installing the load balancer

1 From the LDD installation package, run **Setup.exe**.

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

3 From the LDD Setup window, click **Next**.

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

5 Accept the license agreement, and then click **Next**.

6 From the list of components, select **Load balancer**, and then click **Next**.

7 Specify a location on a shared cluster disk for the installation, and then click **Next**.

Note: The installation path must not contain double-byte characters.

8 Select the host name or IP address of the logical host of the cluster, and then click **Next**.

Note: If necessary, select **Allow only IP address**.

9 Specify the host name or IP address of the logical host, select the database type, and then click **Next**.

Notes:

- If you are using a Microsoft SQL Server database, then make sure that the database is installed before proceeding with the load balancer installation.
- To allow the domain account to access the Microsoft SQL Server database, enable integrated security when installing the database. Make sure that the domain account is granted access to the Microsoft SQL Server database. It must also have full control privileges to the LDD installation path on the application servers and all its subfolders.
- Do not use **`localhost`** or the loopback IP address (**`127.0.0.1`**) for the location of the database.
- If you are installing on a cluster, then set the location of the database during installation. If the database is moved, or the IP address of the database changes, then reinstall the load balancer. You can also contact your Lexmark representative to help modify the current installation.

10 If you are installing a backup recovery system, then select **Restore Install (RI)**, browse to the .ri file, and then click **Next**.

11 Review the setup information, and then click **Next**.

12 Click **Install**.

Extending the database and load balancer to standby nodes

On the primary node of each failover cluster, do the following:

1. Run the Lexmark Solutions Cluster Configuration script:
   a. Create a temporary directory.
   b. From the **install\Cluster_Config_Script** folder of the installation package, copy either of the following to the temporary directory:
      - LexmarkSolutionsClusterConfigScript_WMIProvider.vbs
      - LexmarkSolutionsClusterConfigScript.vbs
   c. Run the command prompt as an administrator, and then access the temporary directory.
   d. Run the VBScript file by typing either of the following:
      - **`cscript LexmarkSolutionsClusterConfigScript_WMIProvider.vbs`**
      - **`cscript LexmarkSolutionsClusterConfigScript.vbs`**
2. Follow the instructions on the screen.

Installing servers

Note: When you are installing multiple servers, install one server at a time.

From the system where you want to install the server, do the following:

1. From the LDD installation package, run **Setup.exe**.
2. Select a language for the installation, and then click **OK**.
3. From the LDD Setup window, click **Next**.
4. Select **Install LDD system components**, and then click **Next**.
5. Accept the license agreement, and then click **Next**.
6. From the list of components, select **Server**, and then click **Next**.

   Note: You can install optional server components, such as Barcode Read, Barcode Write, and OCR, after the LDD installation.
7. Specify a location for the installation, and then click **Next**.

   Note: The installation path must not contain double-byte characters.
8. For multiple networks, select the IP address to which you want to bind the server, and then click **Next**.

   Note: If necessary, select **Allow only IP address**.
9. Specify the host name or IP address of the load balancer and of the database, select the database type, and then click **Next**.

   Notes:

   - If you are using a Microsoft SQL Server database, then make sure that the database is installed before proceeding with the server installation.
   - To allow the domain account to access the Microsoft SQL Server database, enable integrated security when installing the database. Make sure that the domain account is granted access to the Microsoft SQL Server database. It must also have full control privileges to the LDD installation path on the application servers and all its subfolders.

- Do not use **`localhost`** or the loopback IP address (**`127.0.0.1`**) for the location of the database or load balancer.
- If you are using DNS aliases when connecting to a backup system during a recovery, then use the DNS aliases of the database and load balancer.
- If necessary, select **Hardware Load balancer**, and then type the IP address of a hardware load balancer, such as F5 or GSS. Use this setting only if all the printers in the LDD system support eSF applications.

10 Review the setup information, and then click **Next**.

11 Click **Install**.

Notes:

- After installing each server, log in to LMC. Change the administrator password, install the licenses, and then set all servers online. You can install more servers to scale the LDD system, depending on the customer requirements.
- Make sure that all the optional server components are installed on each server.

Installing LDD on a network load balancer (NLB) cluster

Before you begin, make sure that:

- The LDD licenses for the two LDD units are installed via the local LMC URL, and not the virtual IP address URL.
- A common SSL certificate or key pair with the certificate common name (CN) is generated and installed on the Apache servers of the load balancers. The SSL certificate or key pair must be set to the cluster virtual IP address or DNS name.
- The Tomcat servers are accessible by the clients.

Configuring an NLB cluster

Note: All the LDD load balancers must be members of the NLB cluster.

1 From Network Load Balancing Manager on any cluster member, right-click on a cluster, and then click **Cluster Properties**.

2 From the Cluster IP Addresses tab, check that all load balancer IP addresses are added.

3 From the Cluster Parameters tab, check that the full internet name is resolvable by all the cluster members.

4 Set "Cluster operation mode" to **Multicast**, and then click **OK**.

5 From the Port Rules tab, check that the rules for the following port numbers are added:
   - TCP 9780
   - TCP 9783
   - TCP 443

6 For each port rule, do the following:
   a Check that the "Cluster IP address" or NLB virtual IP address is the same as the Hardware Load Balancer address set during the application server installation.
   b Set "Filtering mode" to **Multiple host**.

c Set "Affinity" to **Single**.

d Set the timeout between two to five minutes.

7 Click **OK**.

Installation overview for an NLB cluster

1 Install the central database. The central database may be Microsoft SQL Server or Firebird.

Note: We recommend using a central database with a RAID storage and that has NIC Teaming configured.

2 Install the load balancers on all NLB cluster nodes.

3 Using a text editor, open the **httpd.conf** file from the ***<install-Dir>*/Lexmark/Solutions/Apache2/conf** directory, where ***<install-Dir>*** is the installation folder of LDD, and then change the following:

- **`Listen y:9780`** to **`Listen *:9780`**
- **`<VirtualHost y:9780>`** to **`<VirtualHost *:9780>`**

Where ***y*** is the IP address of the load balancer.

4 Save and close the file.

5 Using a text editor, open the **httpd-ssl.conf** file from the same directory, and then change the following:

- **`Listen y:9783`** to **`Listen 9783`**
- **`Listen x:443`** to **`Listen 443`**
- **`<VirtualHost y:9783 y:443>`** to **`<VirtualHost *:9783 *:443>`**

Where ***y*** and ***x*** are the IP addresses that are associated with the system.

6 Save and close the file.

7 From the Services panel on the system, restart the Apache2.4 service.

8 Install the application servers.

Notes:

- LDD is supported only on a Multicast cluster operation mode.
- The database IP address must be the same as the central database IP address.
- The load balancer IP address can be different, but the hardware load balancer IP address must be the same as the NLB virtual IP address.

Configuring LDD for multiple subnet failovers for Microsoft SQL Server AlwaysOn Availability

1 From the LDD setup window, in the Install Load Balancer page, type the name of the availability group listener as the host name of the database.

2 Select **Microsoft SQL** as the database, and then click **Next**.

3 Leave the Instance Name field blank, and then enter the port number of the availability group listener.

4 Click **Next**, and then continue with the installation.

5 Configure the load balancer. Using a text editor, open the **mssql_database.properties** file from the ***<install-Dir>*\ApacheAgent\Classes** folder, where ***<install-Dir>*** is the installation folder of LDD, and then add **`multiSubnetFailover=true`**.

Sample configuration settings

```
database.connection.url=${database.jdbcstr}//${database.hostname}${database.port.urlstr};
integratedSecurity=true; multiSubnetFailover=true;${database.dataSourcePath}$
{database.instancename.urlstr}

database.quartz.dataSourcePath=databaseName=QUARTZ

database.quartz.connection.url=${database.jdbcstr}//${database.hostname}$
{database.port.urlstr};
integratedSecurity=true; multiSubnetFailover=true;${database.quartz.dataSourcePath}$
{database.instancename.urlstr}

database.monitor.dataSourcePath=databaseName=MONITOR

database.monitor.connection.url=${database.jdbcstr}//${database.hostname}$
{database.port.urlstr};
integratedSecurity=true; multiSubnetFailover=true;${database.monitor.dataSourcePath}$
{database.instancename.urlstr}
```

6 Using a text editor, open the **dbProduct.properties** file and then make sure that the **`database.hostname`** element points to the host name of the availability group listener. For example, change **`database.hostname=x`** to **`database.hostname=y`**, where ***x*** is any IP address, and *y* is the host name of the availability group listener.

7 Configure the server. Using a text editor, open the **mssql_database.properties** file from the ***<install-Dir>*apps\wf-ldss\WEB-INF\classes\dbProduct.properties** folder, where ***<install-Dir>*** is the installation folder of LDD, and then add **`multiSubnetFailover=true`**.

Sample configuration settings

```
database.connection.url=${database.jdbcstr}//${database.hostname}${database.port.urlstr};
integratedSecurity=true; multiSubnetFailover=true;${database.dataSourcePath}$
{database.instancename.urlstr}

database.quartz.dataSourcePath=databaseName=QUARTZ
database.quartz.connection.url =  ${database.jdbcstr}//${database.hostname}$
{database.port.urlstr};
integratedSecurity=true;multiSubnetFailover=true;${database.quartz.dataSourcePath}$
{database.instancename.urlstr}

database.monitor.dataSourcePath=databaseName=MONITOR
database.monitor.connection.url= ${database.jdbcstr}//${database.hostname}$
{database.port.urlstr};
integratedSecurity=true;multiSubnetFailover=true;${database.monitor.dataSourcePath}$
{database.instancename.urlstr}

database.solution.dataSourcePath =databaseName=SOLUTIONINFO
database.solution.connection.url= ${database.jdbcstr}//${database.hostname}$
{database.port.urlstr};
integratedSecurity=true;multiSubnetFailover=true;${database.solution.dataSourcePath}$
{database.instancename.urlstr}

database.eforms.dataSourcePath=databaseName=EFORMS
database.eforms.connection.url= ${database.jdbcstr}//${database.hostname}$
{database.port.urlstr}
;integratedSecurity=true;multiSubnetFailover=true;${database.eforms.dataSourcePath}$
{database.instancename.urlstr}

database.license.dataSourcePath=databaseName=LICENSE
database.license.connection.url= ${database.jdbcstr}//${database.hostname}$
{database.port.urlstr};
integratedSecurity=true;multiSubnetFailover=true;${database.license.dataSourcePath}$
{database.instancename.urlstr}
```

```
database.webappconfig.dataSourcePath=databaseName=WEBAPPCONFIG
database.webappconfig.connection.url= ${database.jdbcstr}//${database.hostname}$
{database.port.urlstr};
integratedSecurity=true;multiSubnetFailover=true;${database.webappconfig.dataSourcePath}$
{database.instancename.urlstr}
```

8. Save and close the file.
9. From the Windows Services control panel on the server computer, restart the Lexmark Solutions Apache Agent and the Lexmark Solutions Application Server. For more information, see "Restarting the Lexmark Solutions Application Server" on page 69.

In SQL Server Management Studio, tables are created for the databases.

Configuring LDD with a Microsoft SQL Server database

If you are using Microsoft SQL Server as the back-end database, then make sure that:

- The Microsoft SQL Server database is installed before proceeding with the LDD installation. For more information, see the help information for Microsoft SQL Server.

  Note: To view the list of supported database servers, see "System requirements" on page 22.
- The "Log on as a service" right is given to the service account user, if integrated security is enabled.

  Note: To configure the "Log on as a service" right using a Windows computer, navigate to **Local security policy** > **Local policy** > **User Rights Assignments**. From the "Log on as a service" section, add a user.
- LDD system components are not installed on the server that is running Microsoft SQL Server.
- The Firebird database in the LDD installer is not installed.

Note: To allow the domain account to access the Microsoft SQL Server database, enable integrated security when installing the database. Make sure that the domain account is granted access to the Microsoft SQL Server database. It must also have full control privileges to the LDD installation path on the application servers and all its subfolders.

For LDD to work with Microsoft SQL Server, create seven databases before the load balancer and server are installed. Do the following:

1. Open the CreateDatabase.sql file at ***installerpath*\mssql\scripts\CreateDatabase.sql**, where ***installerpath*** is the location of the LDD installer.
2. Modify the script to control the creation of the LDD databases in Microsoft SQL Server, and then save the file.

   Note: The CreateDatabase.sql file contains the minimum database size required for LDD. You can increase the database size as necessary.
3. From Microsoft SQL Server, run the command prompt as an administrator, and then type the following:

   sqlcmd -i *installerpath*\mssql\scripts\CreateDatabase.sql -o *outputfilepath*\MyOutput.txt

   where:

   - ***installerpath*** is the location of the LDD installer.
   - ***outputfilepath*** is the location where you want to save the log file.

4. Confirm that the databases are installed successfully. Do the following:
   a. Type **sqlcmd -S .** to connect to the default instance.
   b. Type **select name from sys.databases** to show all databases.
5. From the SQL Server Configuration Manager, enable the TCP/IP connections and then set the port number to **1433**. For more information, see the help information for Microsoft SQL Server.

Note: You can also migrate data from Firebird to Microsoft SQL Server. For more information, see the *Readme* file for database migration at ***InstallCD*\install\mssql_migration\readme_migration.txt**, where ***InstallCD*** is the location of the LDD installer CD.

Updating the Microsoft SQL Server password

1. Using a text editor, open the **mssql_database.properties** file from the ***<install-Dir>*\Solutions\apps\wf-ldss\WEB-INF\classes** folder, where ***<install-Dir>*** is the installation folder of LDD.
2. Update the encrypted password using plain text.

   ```
   database.password = newpassword
   ```

   Where **database.password** is the new password.
3. Restart the Lexmark Solutions Application Server service.

Managing certificates

1. From your computer, create a copy of the certificate and key PEM files, and then save the new PEM files in the same location.

   Note: A sample folder location is **\Lexmark\Solutions\Apache2\conf**.
2. In the ldd-cert.conf file, modify the old certificate and key file paths with the new file paths.
3. Save the file.

Verifying certificates

AP Bundle verifies the certificate that the LDD Tomcat server sends when running a profile in secure mode (HTTPS). The communication between the MFP and the LDD servers occurs only when secure communication is enabled for the device group to which it belongs to.

To verify that the certificate is valid, the printer must have the CA root certificate that is used to sign the server certificate. Also, to verify the authentication of the server, the host or domain in the certificate must match the server.

Validating LDD server certificates

1. From LMC, click the **Device Groups** tab.
2. From the Device Groups section, select a device group.
3. From the Tasks section, select **eSF Configuration**.

4 From the main section, select **advancedprompt(AdvancedPrompting Bundle)**.

5 From the eSF Application Settings section, select **Verify certificate**.

6 From the Verification Mode menu, select either of the following, and then browse to the .PEM certificate file:

- **Chain**—For CA-signed certificates. Make sure that the CA root certificate is installed in the truststore of the AP bundle. The eSF framework checks whether the CA has signed the server certificate.
- **Peer**—For self-signed certificates. Peer checking does a one-to-one check of the certificate file. Make sure that the self-signed certificate is installed in the truststore of the AP bundle.

Notes:

- The certificate file may be a CA root certificate or a peer certificate.
- If a certificate file is not specified, then the device trust store is used to get the root certificate.

7 Click **Save Settings**.

Note: CheckHosts is ignored for IP address installation of LDD. For more information, see "Understanding CheckHosts" on page 43.

The settings and the AP bundle are deployed to the printer during policy update.

Understanding CheckHosts

The eSF framework automatically sets the CheckHosts setting with the host name from the URL. If there are multiple entries in the certificate in subject alternate name (SAN), then you may use CheckHosts to specify the other entries. Make sure that the certificate has the correct host name in SAN. Otherwise, the authentication verification fails.

The eSF framework checks only the host name using the server access with fully qualified domain names (FQDN). If LDD is installed as **host only**, then the AP Bundle uses the host name in the URL to access the Tomcat server. Make sure that the server certificate has the correct host name in SAN.

For example, if the LDD Tomcat server host name is **`LDDServer.LPM.TEST`**, then the common name and the SAN entry in the certificate must be **`LDDServer.LPM.TEST`**.

Adding certificates to the server KeyStore

Certificates can be added to the KeyStore (server.ks) file using a keytool utility that is included in Java Development Kit (JDK). LDD has a self-signed certificate added to the server KeyStore (server.ks) in the **tomcat/conf** folder.

Notes:

- The default KeyStore password for the server.ks file is **`password`**.
- The default Tomcat password in the server.xml file is **`changeit`**.

Setting up a KeyStore file with signed certificates

When OpenSSL is used to generate private keys and certificates, it is stored as separate files in the PEM encoding. However, the files cannot be converted into Java KeyStore format directly. Do the following:

1 Convert the files to a single file in PKCS#12 format that has a private or public key.

Note: You may use the **`openssl pkcs12`** command to merge private keys and certificates into a PKCS#12 file.

Sample PKCS#12 format conversion

```
openssl pkcs12 -export -in servercert.pem -inkey serverkey.pem -out servercert.p12 -name
tomcat -CAfile cacert.pem -caname root
```

Where:

- ***`servercert.pem`*** is the server certificate file.
- ***`serverkey.pem`*** is the server private key file.
- ***`cacert.pem`*** is the CA certificate file.

2 Using the keytool utility included in the JDK, convert the PKCS#12 file to Java KeyStore (JKS) format.

Sample JKS format conversion

```
keytool -importkeystore -deststorepass password -destkeypass password -destkeystore
server.keystore -srckeystore servercert.p12 -srcstoretype PKCS12 -srcstorepass password    -
alias tomcat
```

Where ***`server.keystore`*** is the JKS format KeyStore file that must be copied into the **tomcat/conf** folder.

Configuring secure connection to the load balancer in the Advanced Prompt bundle

By default, the first call to the load balancer from the Advanced Prompt bundle is always secured.

To change the default settings, do the following:

1 From the Embedded Web Server, click **Apps** > **Advanced Prompt** > **Configure**.

2 Clear **Secure connection to load balancer**.

Antivirus policy requirements and recommendations

Required antivirus policies

- Exclude the following folders when performing real-time virus scanning:
  - Load balancer server or database server
    - **\Lexmark\solutions\firebird\data**
    - **\Lexmark\solutions\Apache2\logs**
    - **\Lexmark\solutions\Apache2\htdocs\apachewebdav**

    Note: If the load balancer is installed on another server, then exclude only the database.
  - All Tomcat transaction servers (**\Lexmark** and all subfolders)

    If excluding these servers are not allowed, then exclude the following folders:
    - **\Lexmark\Solutions\tomcat\temp**
    - **\Lexmark\Solutions\tomcat\logs**

    - **\Lexmark\Solutions\tomcat\webapps\webdav** and all subfolders
    - **\Lexmark\Solutions\apps\wf-ldss** and all subfolders
  - Print servers, where applicable
    - Directory where print jobs are spooled
      For example, **C:\spool** or **C:\Windows\system32\spool\printers**.
    - Windows temporary directory (**C:\Windows\temp**)
  - Network folders and subdirectories where solutions installed are writing files
- Make sure that full virus scans and virus definition updates on all Lexmark servers are scheduled to run during off-peak hours. Include the following servers:
  - Load balancers or databases
  - Application servers
  - Print servers

Recommended antivirus policy

If you are running the system on a virtual server environment, then run the following on the virtual server environment during off-peak hours:

- Full virus scans
- Virus definition updates

Installing LDD components silently

LDD components may be installed silently by using the batch files that are located in the **install \Silent_Install_Script_Examples** folder of the installation CD. The folder also includes a batch file for uninstallation and cleanup. All batch files included in the installation CD contain usage instructions. The included batch files are examples for basic setups and may be modified as necessary for your system.

Note: To run an installation script from a network folder, map a drive letter to the network folder. The UNC path cannot be used when running an installation script.

1. Run the command prompt as an administrator.
2. Run one of the following batch files, and then use the "**/?**" switch to view the usage instructions for the batch file:
   - **Install_All_on_One_PC.bat**—Installs the database, load balancer, and server components on the local computer for configuration 1.
   - **Install_All_on_One_PC_wo_OCR.bat**—Installs all the LDD 4.x components except for the OCR engine on the local computer.
   - **Install_Client_Software.bat**—Installs client software on the local computer.
   - **Install_Database.bat**—Installs the database component on the local computer for configurations 1-1-N and X-Y-N.
   - **Install_LoadBalancer.bat**—Installs the load balancer component on the local computer for configurations 1-1-N and X-Y-N.
   - **Install_LoadBalancer_MSSQL.bat**—Installs the LDD 4.x load balancer on the local computer for an existing Microsoft SQL Server that is configured for LDD. By default, the script uses a Microsoft SQL Server named instance with a Microsoft SQL Server account.

- **Install_Server_MSSQL.bat**—Installs the LDD 4.x Tomcat server on the local computer for an existing Microsoft SQL Server that is configured for LDD. By default, the script uses a Microsoft SQL Server named instance with a Microsoft SQL Server account.
- **Install_Server.bat**—Installs the server component on the local computer for configurations 1-N, 1-1-N, X-N, and X-Y-N.
- **Uninstall_DB_LB_Server_on_One_PC.bat**—Uninstalls the database and load balancer components from the local computer.

Note: For **Install_LoadBalancer_MSSQL.bat** and **Install_Server_MSSQL.bat**, make sure to allow the domain account to access the Microsoft SQL Server database by enabling integrated security when installing the database. Make sure that the domain account is granted access to the Microsoft SQL Server database. It must also have full control privileges to the LDD installation path on the application servers and all its subfolders.

3 Run the batch file again by using the appropriate configurations as shown in the usage instructions.

4 Follow the instructions on the screen.

Upgrading the LDD system

Note: Make sure that LDD version 4.6 or later is installed.

1 From LMC, click the **System** tab.

2 From the System menu, select **System Status**.

3 Set all servers offline. For more information, see “Viewing and changing server status” on page 64.

Note: Make sure that all jobs are completed before the server goes offline.

4 If the database or load balancer is installed on a failover cluster, then do the following:

a On the primary node of each cluster, close all applications that are using the shared drive where LDD components are installed.

b From Failover Cluster Manager, move all cluster resources to the primary node where the LDD components are originally installed.

c Stop the cluster service on standby nodes.

Before continuing the upgrade, wait for confirmation that the standby nodes are disabled.

d Set all Lexmark resources offline.

5 From the LDD database and load balancer servers, run the LDD installer, click **Update**, and then follow the instructions on the screen.

Notes:

- If you are using Microsoft SQL Server database, then do not upgrade the database component.
- To allow the domain account to access the Microsoft SQL Server database, enable integrated security when installing the database. Make sure that the domain account is granted access to the Microsoft SQL Server database. It must also have full control privileges to the LDD install path on the application servers and all its subfolders.

6 If the database or load balancer is installed on a failover cluster, then do the following:
   a From Failover Cluster Manager, set all Lexmark resources online.
   b On the primary node of each cluster, run the **LexmarkSolutionsClusterConfigScript.vbs** script from the **Install\Cluster_Config_Script** folder of the LDD installation package. Follow the instructions on the screen.

      Note: During an upgrade, the clustering script may fail the first time it is run. Run the script again.
   c Start all Lexmark cluster resources.
   d Start the cluster service on standby nodes.
7 In all LDD servers, run the LDD installer, click **Update**, and then follow the instructions on the screen.
8 Reinstall custom components on the servers.
9 Reinstall all previously installed solutions, including those solutions that were automatically added during a previous installation.

   Note: Make sure that device groups, software client groups, solutions, and all settings are correct.
10 From LMC, set all servers online. For more information, see "Viewing and changing server status" on page 64.

Configuring Kerberos authentication

If a user logs in at a printer by using Kerberos, then the LDD system uses the credentials to do the following:

- Manipulate network files.
- Interact with ECM systems.

Notes:

- Enable secure communication between printers and servers in LMC for any device group that uses a solution with Kerberos authentication. For more information, see "Enabling secure communication between servers and printers in a device group" on page 113.
- Make sure that the date and time on the printer, LDD server, and key distribution center (KDC) server are correct and synchronized.

Configuring Kerberos authentication on printers

Notes:

- The following procedure applies only to e-Task 2+ printers. If these steps do not apply to your printer, then see the documentation that came with your printer.
- The names and locations of the settings mentioned in the following procedure may vary depending on the firmware installed on your printer.

1 Obtain the printer IP address. Do either of the following:
   - Locate the IP address on the top of the printer home screen.
   - View the IP address in the TCP/IP section of the Network/Ports menu.
2 From the Embedded Web Server, click **Settings** > **Security** > **Security Setup**.
3 From the Advanced Security Setup section, click **Kerberos 5**.

4 Import or create a Kerberos configuration file.

- To import a configuration file, do the following:

  Note: Importing a configuration file allows more control over Kerberos tickets.

  a From the Import Kerberos File section, browse to the Kerberos configuration file.

  b Click **Submit**.

  The following example represents a minimal configuration file:

```
[libdefaults]
    default_realm = MY.REALM
    kdc_timesync = 1
    forwardable = true

[realms]
    MY.REALM = {
        kdc = MY.KDC.ADDRESS
    }
```

  Note: When a configuration file is used, tickets must be marked forwardable by default. For more information, see the Kerberos documentation.

- To create a configuration file, do the following:

  a From the Simple Kerberos Setup section, in the KDC Address field, type the KDC address.

  b In the KDC Port field, enter the port number that is used by the Kerberos server. You can set the value to **1–88**.

  c In the Realm field, type the realm that is used by the Kerberos server.

  d Click **Submit**.

5 Add a security template. Do the following:

a From the Advanced Security Setup section, click **Security Template**.

b From the Manage Security Templates section, click **Add a Security Template**, and then type a security template name.

c In the Authentication Setup menu, select **Kerberos Building Block**.

d Click **Save Template** > **Return to Security Setup**.

6 Configure access controls for profiles.

a From the Advanced Security Setup section, click **Access Controls**, and then select a security template. Do either of the following:

- To apply the security template to all profiles on the printer, in the Use Profiles menu, select the security template that you created.
- To apply the security template to an individual profile, do the following:

  1 From LMC, determine the access control number of the profile.

  Note: Keep the Embedded Web Server open while accessing LMC.

  a Click the **Device Groups** tab.

  b From the Device Groups section, select the device group that contains the printer and the solution.

  c From the Tasks section, select **Profiles**.

d From the main section, select a device class tab that corresponds to the device class of the printer.

e Find the number beside Access Control.

Note: If **0** appears beside Access Control, then an access control number is not assigned to the profile. For more information, contact your Lexmark representative.

2 From the Embedded Web Server, in the Access Controls page, select a security template for the application corresponding to the access control number of the profile.

b Click **Submit**.

Depending on the authentication setup, the printer may require user authentication before accessing the home screen or when accessing an LDD profile from the printer.

Configuring LDD servers for Kerberos authentication

The LDD server that is requesting a Kerberos ticket must have the following components:

- KDC address
- Realm

If the KDC address and realm are determined from the ticket that is forwarded from the printer, then configuration is not necessary. A warning is included in the log indicating that the server is attempting to determine the KDC address and realm from a forwarded ticket.

To configure each LDD server for Kerberos authentication manually, do either of the following:

- Create a duplicate Kerberos configuration file for the server.

  We recommend specifying only the KDC address and realm for the server configuration. Name the configuration file **`krb5.ini`**, and then save it in the **\Lexmark\Solutions\Security** folder on each server where LDD is installed. You may need to create the Security folder.

  Note: For more information on reading the Kerberos configuration file from another location, see the Apache Tomcat documentation.

- Set the KDC address and realm from the script. For more information, see the *Lexmark Document Distributor SDK Guide*.

Installing Lexmark Keep Alive Service

Lexmark Keep Alive Service is a Windows service that queries the status of the software load balancer from the hardware load balancer in an enterprise environment. The service is a web-based application that is used by other applications that serve as an HTTP client. It can be installed on the software load balancer or other machines.

1 From the computer, run the CD, and then navigate to the **\tools\LDDKeepAliveService** folder.

2 Run the **LDDKeepAliveSetup.exe** file, and then click **Next**.

Installing Lexmark Keep Alive Service silently

Lexmark Keep Alive Service can also be installed silently.

1 Navigate to **<LDD Installation directory>\install\Silent_Install_Script_Examples**.

2 Run the command prompt as an administrator.

3 Run the **Install_KeepAliveService.bat** batch file.

Note: For help information, at the command prompt, type **`Install_KeepAliveService.bat /?`**.

Accessing Lexmark Keep Alive Service

Lexmark Keep Alive Service is a Windows service that queries the status of the software load balancer from the hardware load balancer in an enterprise environment. The service is a web-based application that is used by other applications that serve as an HTTP client. It can either be installed on the software load balancer or other machines.

Open a web browser, and then do either of the following:

- If the software load balancer and LddKeepAliveService are installed on the same machine, then type **`http://y:7999/LDD/KeepAlive`**, where ***y*** is the IP address of the LddKeepAliveService.
- If the software load balancer and LddKeepAliveService are installed on different machines, then type **`http://y:7999/LDD/KeepAlive/IP=x`**

  where:

  - ***y*** is the IP address of the LddKeepAliveService.
  - ***x*** is the IP address of the load balancer.

Monitoring and maintaining the system

Setting up AD FS Single Sign-On for LDD

Active Directory Federation Services (AD FS) is a software component to provide single sign-on (SSO) authorization services to users. This feature enables users to access multiple applications on the server.

1. Add the certificate of AD FS server to the Java runtime environment (JRE) trust store located at **<LDD installation directory>\jre\lib\security\cacerts** using keytool.

   Note: For more information, see https://docs.oracle.com/cd/E19798-01/821-1841/gjrgy/.

2. Configure **<server.properties>**.

Parameter	Value	Description
server.oauth.isEnabled	**<TRUE>**	Enables server oauth. **Note:** To allow some users to log in to LDD, log in to LDD using default credentials and then set proper roles against the AD FS administrator or user groups.
server.oauth.providerName	**<ADFS>**	Used to generate the URL to be used as the redirect URL in the AD FS server during client registration.
server.oauth.authorizatonUrl	**https://<adfs fully qualified domain name>/adfs/oauth2/authorize/**	The server oauth authorization URL available from the AD FS server configuration.
server.oauth.clientAuthenticationMethod	**NONE**	The value is set to **NONE** when the client secret is unavailable.
server.oauth.scopes	**openid** **profile** **email** **allatclaims**	**openid** is required to trigger openid flow, and **allatclaims** is required to get LDAP user attributes in idtoken.
server.oauth.tokenUrl	**https://<adfs fully qualified domain name>/adfs/oauth2/token/**	The server oauth token URL.
server.oauth.jwkSetUrl	**https://<adfs fully qualified domain name>/adfs/discovery/keys**	The server ouath jwk set URL.
server.oauth.usernameAttribues	**UPN**	Available in AD FS server setup.
server.oauth.clientid	**<ClientID>**	The client ID of the client. This value cannot be empty.

Parameter	Value	Description
server.oauth.clientSecret	**<ClientSecret>**	The password of the client. This value cannot be empty.
server.oauth.userInfoUri	**<UserInfoUri>**	Required for Oauth2 flow to call this URI to get user properties.
server.oauth.sessionlogouturl	**https://adcpremise1.lpm.lex/adfs/oauth2/logout**	Required to enable true logout in AD FS or else logout implementation does not work properly.
server.oauth.langattributename	**LANG**	User-specific language attribute in Active Directory.
server.oauth.groupnameattribute	**GROUP**	Must be configured correctly as LDD detects the correct group name for the logged-in user to apply roles and authorization.

Notes:

- For information on public client registration, use transform rules to send LDAP user attributes. For more information, see **Issuance transform rules**.
- For information on client registration in AD FS, see **https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/development/ad-fs-openid-connect-oauth-concep** .
- For more information on configuring AD FS, see *AD FS SSO Configuration Guide*.

Configuring Lexmark Management Console

Accessing Lexmark Management Console

Note: LDD version 5.0 supports accessing LMC using only HTTPS mode by default. To disable this feature, open the **server.properties** file, and then set the **server.hsts.enable** property value to **false**.

1. From your web browser, launch LMC by using either of the following URLs:
   - **http://*loadbalancer*:9780/lmc**
   - **https://*loadbalancer*/lmc**

   where ***loadbalancer*** is the IP address of the computer where the load balancer is installed.

   To access LMC on a particular server, do either of the following:
   - If HTTP Strict Transport Security (HSTS) is enabled, then use the URL **https://*server*:9743/lmc**
   - If HSTS is disabled, then use the URL **http://*server*:9788/lmc**

   Where ***server*** is the IP address of the computer where the particular server is installed.

   Notes:
   - On a computer where a server is installed, you can use the LMC desktop shortcut.
   - Starting all services may take several minutes when the system is first booted. If LMC cannot be accessed immediately after starting the system, then wait a few minutes, and then try again.

- Make sure that your web browser allows cookies for the address where you access LMC.

2 Type the administrator user name and password.

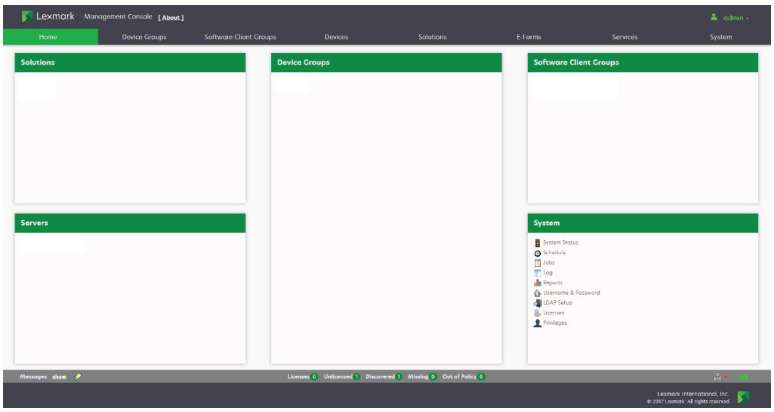
Notes:

- The default user name and password is **admin**.
- If LMC is configured to connect to an LDAP server, then use any valid user name and password.

3 Click **Login**.

Notes:

- LMC admin user should be able to create groups and assign privileges without specifying LDAP configuration in LMC.
- Even if the user receives a warning message that there is no LDAP setup or an error occurs during validation of the group, the user can still add the group to assign privileges in LMC.



A green arrow beside the server address indicates the server that hosts the LMC session.

Changing the administrator user name

1 From LMC, click the **System** tab.

2 From the System section, select **Username & Password**.

3 Type the new user name, and then retype it to confirm.

4 Click **Apply**.

Changing the administrator password

1 From LMC, click the **System** tab.

2 From the System section, select **Username & Password**.

3 Type the current password.

4 Type the new password, and then retype it to confirm.

5 Click **Apply**.

Enabling LDAP authentication for LMC

To authenticate users other than the administrator account, set up a connection with an LDAP server.

1. From LMC, click the **System** tab.
2. From the System section, click **LDAP Setup**.
3. Select **Enable LDAP Authentication**.
4. If your LDAP server requires a secure connection, then select **Use Secure Connection (SSL/TLS)**.
5. Type the LDAP server address and port number.

   Note: For non-secure communication, use port **389**. For secure communication, use port **636**.
6. In the User Search Filter field, type the attribute that is used to identify a user name, such as **cn**, **sn**, **uid**, or **sAMAccountName**.
7. In the User Search Base field, type the relative distinguished name (RDN) where a subtree search for a user must begin, such as **ou=Employees**.
8. To filter the search to users in specific groups, do the following:
   a. In the Group Search Filter field, type the attribute that is used to identify a member of the group, such as **member** or **uniquemember**.
   b. In the Group Search Base field, type the RDN where a subtree search for groups must begin in the directory, such as **ou=Groups**.
   c. In the "Member of Groups" field, type a comma-delimited list of group names to search. The user name must be a member of at least one of the groups listed.
   d. In the Group Identifier field, type a name for the object class.

      Note: The object class name can be used to search for the group base when assigning privileges to groups.

      ### Example

      - User Search Filter: **uid**
      - User Search Base: **ou=Employees**
      - Group Search Filter: **uniquemember**
      - Group Search Base: **ou=Groups**
      - Group Identifier: **groupOfNames**
      - Member of Groups: **Dept A,Dept C**

        If the user name **testuser** is used to log in to LMC, then the user can be authenticated if each of the following is true:
        - The distinguished name **uid=testuser,ou=Employees,o=MyOrganization** is found in the directory.
        - The distinguished name **cn=Dept A,ou=Groups,o=MyOrganization** or **cn=Dept C,ou=Groups,o=MyOrganization** is found in the directory and contains the attribute **uniquemember: uid=testuser,ou=Employees,o=MyOrganization**.
        - The object class is **groupOfNames**.
        - The correct password is supplied for the user.

9 Select an authentication method:
- If the LDAP server accepts anonymous connections, then select **Anonymous**.
- If the LDAP server requires authentication, then do the following:
  a Select **Username**.
  b In the Username field, type a distinguished name that is used to log in to the LDAP server, such as **uid=ldapuser,ou=Employees,o=MyOrganization**.
  c Type the password that is associated with the selected user name.

Note: If ***** is used instead of the distinguished name and password, then the user is an LDAP binding user. For example, **uid=***, **ou=Employees**, **o=MyOrganization**, and **password=***.

10 To test the connection settings, click **Test Settings**.

Note: For anonymous connections, the test cannot determine whether a user name and password are correct if they are used for authentication. If the test reports an anonymous connection when a user name and password are used, then manually check them.

11 In the Search Base field, type the distinguished name where the directory search must begin, such as **o=MyOrganization**.

12 Click **Save Settings**.

Assigning privileges to groups

Adding access control to users accessing LMC lets you restrict system access to specific groups. The Privileges settings depend on the role that is assigned to the user.

Notes:

- Add a group before defining privileges. By default, the Default Group has access to all tabs and tasks of LMC and is already added to the group list. The administrator can modify the privileges of the default group.
- If a user belongs to multiple groups, then group privileges are combined. Privileges can be modified for LDAP users only. The administrator has access to all tabs and tasks, but these settings cannot be modified.

1 From LMC, click the **System** tab.

2 From the System section, select **Privileges**.

3 In the “Group Names from LDAP" list, select or add a group.

To add a group, do the following:

a Click ✚ or **Add**, type the group name, and then click **Search**.

b In the list, select a group name, and then click **Add**.

4 Select the tabs and tasks that the group is allowed to access and perform.

When assigning privileges, you can select specific tasks in each tab.

5 Click 🖫 or **Save Privileges**.

Understanding the Device Groups tab

When a device group is selected, the following tasks are shown:

Task	Operation
Summary	Shows the following information: • List of solutions that are deployed to the device group. • The number of discovered, unlicensed, missing, and out-of-policy printers in the device group. • Whether the device group is configured to use a secure communication channel when submitting jobs. When **Secure Server Communication** is enabled, communication between the server and printers that are associated with the selected group is encrypted. Some of these values are linked to appropriate tasks that let you view more information or change the settings.
Name*	Lets you change the unique name of the device group.
Discovery Profiles*	Lets you add, edit, import, and remove discovery profiles for the device group.
Discovery	Finds printers on the network that match the discovery profile for the device group. For more information, see “Manually discovering printers” on page 105.
Discovered Devices	Shows the following information for printers in the device group: • IP address • Host name • Model • Serial number • Contact name • Contact location • Property tag • Last discovered date • Last credential used • Last SNMP settings used • Policy last applied date **Note:** To export the discovered devices list, click **Export**.
Unlicensed Devices	Shows the unlicensed printers in the device group. **Note:** To export the unlicensed devices list, click **Export**.
Solutions*	Lets you select solutions to deploy to the printers in the device group. It also lets you configure the local settings for the device group.
eSF Configuration*	Lets you edit the settings of eSF applications associated with hybrid solutions that are deployed to the device group.
Security Setup Files*	Lets you manage any printer security setup files of solutions that are deployed to the device group.
Home Screen*	Lets you customize the layout of the home screen for the printers in the device group. Click the appropriate device class to customize the printer home screen.
Profiles*	Shows each profile and the associated settings for each device class in the device group.

* These tasks are not available when **All Device Groups** is selected.

Task	Operation
Fax Forwarding*	Lets you configure MFPs to forward incoming faxes to a fax number, e-mail address, FTP site, or Lexmark Document Solution Services (LDSS). Depending on the printer configuration, you can set the system to manage all incoming fax requests for processing before the MFP prints and forwards received faxes.
Policy Update	Deploys group device policies to printers in the device group.
Out of Policy Devices	Lists all out-of-policy printers in the device group.
Missing Devices	Shows a list of previously discovered printers that are not responding in the device group. **Note:** To export the missing devices list, click **Export**.
Schedule	Lets you add, edit, and delete Discovery, Policy Update, and script tasks that are scheduled to run for the device group.
Security*	Enables or disables secure communication between the server and the printers in the device group.
SNMP	Lets you select whether the global SNMP settings must be used for the selected device group. For more information on configuring SNMP, see "Configuring SNMP for discovering devices" on page 76
* These tasks are not available when **All Device Groups** is selected.	

Understanding the Software Client Groups tab

When a software client group is selected, the following tasks are shown:

Task	Operation
Summary	Shows the following information: • Group name • List of solutions that are deployed to the software client group
Name*	Lets you change the unique name of the software client group.
Client Profiles*	Lets you add, edit, import, and remove client profiles in the software client group.
Solutions*	Lets you add, edit, or delete solutions that are deployed to the software clients in the software client group.
Profiles*	Shows each profile and the associated settings for the software client group.
Schedule	Lets you add, edit, and delete script tasks that are scheduled to run for the software client group.
* These tasks are not available when **All Software Client Groups** is selected.	

Understanding the Devices tab

The Devices tab is used for maintenance of printers that have already been discovered. Only discovered printers can be found using the search function on this tab.

When a device is selected, the following tasks are shown:

Task	Description
Summary	Shows the following information: • IP address • Host name • List of device groups that the device belongs to • List of solutions that are deployed to the device • Model • Serial number • Contact name • Contact location • Property tag • Last discovered date and time • Unlicensed status When multiple devices are selected, a table containing the preceding information for all devices in the system is shown. The total number is shown for Device Groups and Solutions and may be expanded to show the list for each.
Profiles	Shows each profile and the associated settings for a device. **Note:** This task shows only one device at a time. When multiple devices are selected, the first device that is selected is shown. If you want to select other devices, then click **Next** or **Previous**.
Policy Update	Deploys policy updates to devices.
Missing Devices	Shows a list of previously discovered printers that are not responding.
Unlicensed Devices	Shows a list of unlicensed devices.
Home Screen	Lets you customize the layout of the home screen for the device. **Note:** This task shows only one device at a time. When multiple devices are selected, the first device that is selected is shown. If you want to select other devices, then click **Next** or **Previous**.
Jobs	Shows a table of the jobs for the device.
Log	Shows a table of logged messages for the device.

Understanding the Solutions tab

When a solution is selected, the following tasks are shown:

Task	Description
Summary	Shows the following information: • Solution name • Version number • Installation time • Update time • List of device groups and software client groups that the solution is deployed to • List of formsets, reports, eSF applications, and security setup files in the solution
Configuration*	Lets you configure the global settings for the solution. The parameters are predetermined for each solution.
EForms*	Shows a list of the formsets that are associated with the solution.
eSF*	Shows a list of eSF applications that are associated with the solution.
Jobs*	Shows a table of the jobs that use the solution.
Log*	Shows a table of the logged events and messages that the solution generates.
Security Setup Files*	Lets you manage any printer security setup files in a solution.
* This task is not available when **All Solutions** is selected.	

Understanding the E-Forms tab

Task	Description
Form printers	Lets you view and manage the virtual printers that process e-forms
Formsets	Lets you view and manage formsets for all solutions

Understanding the Services tab

Task	Description
Confirm	Lets you set the font parameters for all services
DeviceSecurity	Lets you set the authentication type for security-enabled devices
Email	Lets you set the e-mail server parameters
General	Lets you configure the chunk size for device discovery and policy updates
NPA	Lets you set the default unsecured port and the timeout periods between retries during device discovery
PolicyUpdate	Lets you set the policy update parameters, and whether to overwrite function overrides on the device such as copy or fax
Reports	Lets you configure the e-mail parameters, such as the default sender, receiver, and e-mail message
SNMP	Lets you configure the SNMP parameters

Understanding the System tab

Task	Description
System Status	Lists all servers in the system. It also shows the following information for each server: • Server address • Host name • Status • License • Number of running tasks • CPU usage • Memory usage • Network load • Thread count • List of installed components and their versions A green arrow beside the server address in the table indicates the server where the current LMC session is running. You can also set a server online or offline.
Schedule	Shows all report, backup and restore, discovery, policy update, and script tasks that are scheduled to run on the system. It also lets you add, edit, and delete scheduled tasks.
Jobs	Shows a table of all pending and completed jobs from all printers in the system.
Log	Shows a table of the logged event and messages that are generated from all pending and completed jobs from all printers in the system.
Reports	Lets you manage and schedule built-in and custom reports.
Username & Password	Lets you create an administrator user name and password for LMC.
LDAP Setup	Lets you set up a connection with the LDAP server to enable other user accounts.
Licenses	Lists all licenses that are installed on the system. It also shows the feature ID (where the license applies), expiration date, number of licenses, licenses in use, and license type for each license. You can also add new licenses to the system.
AP Bundle	Lets you update the AP Bundle eSF application that e-Task 2 printers require for support. Specifying updated files here updates the applications on printers during the next policy update.

Task	Description
Privileges	Lets you add access control to users. You can assign privileges to users depending on the group to which they belong to.

Finding basic information

Understanding the Home tab

The Home tab provides shortcuts to tasks on the System tab and individual items on other tabs. It also indicates the status of each server and device group in the system.

Home tab section	Description
Solutions	Lists all solutions that are available in the system. Clicking a solution in the list links to that solution on the Solutions tab.
Servers	Lists all servers in the system. The icon of each server indicates the status of that server. Clicking a server in the list links to the System Status task on the System tab.
Device Groups	Lists all device groups that have been created. A yellow exclamation mark appears on the icon of a device group that contains out-of-policy printers. Clicking a device group in the list links to that group on the Device Groups tab.
Software Client Groups	Lists all groups of software clients in the system. Clicking a software client group in the list links to that group on the Software Client Groups tab.
System	Provides shortcuts for all tasks on the System tab. Clicking a task in the list links to that task on the System tab.

Understanding the status bar

The status bar and the message bar appear on all tabs. The message bar provides feedback when the system setup or device discovery changes and lists any errors or warnings.

Status bar item	Description
Messages	Shows or hides the message bar
Licenses	Shows the number of licenses that are available in the system
Discovered	Shows the number of discovered printers that are stored in the database
Unlicensed	Shows the number of discovered printers that do not have a license
Missing	Shows the number of previously discovered printers that are not responding
Out of Policy	Shows the number of discovered printers that have settings different from profiles required by solutions that are deployed to those printers
System status icon	Indicates the overall status of the system

Status bar item	Description
Progress bar	Shows the progress of the current task

System status information on the status bar and Home tab

The overall system status icon is the three server boxes at the right side of the status bar. If any servers are offline or not communicating, then a yellow exclamation mark appears on the system status. This icon indicates that the system is operating at reduced capacity. If all servers are offline or not communicating, then a red X appears on the system status icon.

To view the detailed system status information, do the following:

1. From LMC, click the **System** tab.
2. From the System section, select **System Status**.

Viewing information summaries for LDD elements

1. From LMC, click the **Device Groups**, **Software Client Groups**, **Devices**, or **Solutions** tab.
2. Do either of the following:
   - From the Device Groups section, Software Client Groups section, or Solutions section, select a group name or a solution.
   - From the Devices section, select or search for a printer.
3. From the Tasks section, click **Summary**.

Viewing jobs or system logs

You can view all jobs that are initiated in the system, including the following:

- Tasks that are performed in LMC
- Print jobs that are initiated by using a printer or software client

Data for both jobs and logs are saved for seven days.

1. From LMC, 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 LMC
  - 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 LMC

Note: You can also view jobs and logs for specific solutions or printers through the Jobs and Log tasks in the Solutions and Devices tabs.

Customizing columns for jobs and system logs

1. From LMC, click the **System** tab.
2. From the System section, select **Jobs** or **Log**.
3. Click **Customize Table**.
4. Adjust the columns. Do one or more of the following:
   - To remove a column from view, select it in the Current Columns list, and then click or **Remove**.
   - To add a column back to the Current Columns list, select it in the Available Columns list, and then click or **Add**.
   - To adjust the position of a column, select it in the Current Columns list, and then click or **Move Up**, or or **Move Down**.
   - To return all columns to view in the default order, click **Reset**.
5. Click **OK**.

Custom selections for columns are saved in a cookie in your browser, so they are available each time LMC is used.

Viewing device group profiles

1. From LMC, click the **Device Groups** tab.
2. From the Device Groups section, select a device group.
3. From the Tasks section, select **Profiles**.
4. From the main section, select a device class tab.
5. Select a profile name.

Viewing software client group profiles

1. From LMC, click the **Software Client Groups** tab.
2. From the Software Client Groups section, select a software client group.

3 From the Tasks section, select **Profiles**.

Viewing forms associated with a solution

Solutions that include forms merge functionality are associated with forms that are installed along with the solution.

1 From LMC, click the **Solutions** tab.

2 From the Solutions section, select a solution.

3 From the Tasks section, select **EForms**.

Viewing version information

Viewing version numbers for all system components helps you troubleshoot problems and make sure that all components are updated.

1 From LMC, click the **System** tab.

2 From the System section, select **System Status**.

3 In the Components column, click **Versioninfo**.

You may need to scroll to the right to see the Components column.

Note: To export all system status information and component version information, click **Export Report**.

Managing the LDD system

Viewing and changing server status

When viewing the server status, a table is shown with information about each server in the system. The Status column indicates whether the server is online, offline, or has a communication problem. A yellow exclamation mark appears beside the status when the server is offline, and a red X appears to indicate a communication problem.

A green arrow beside the server address indicates the server that hosts the LMC session.

Note: Multiple non-communicating servers may affect system performance. If you do not expect a non-communicating server to reestablish communication quickly, then remove it.

1 From LMC, click the **System** tab.

2 From the System section, select **System Status**.

3 Do any of the following:

- To change the online status of a server, select a server, and then click **Set Online** or **Set Offline**.
- To remove a server that is not communicating, select a server, and then click **Remove Server(s)**. If the server later reestablishes communication, then it automatically reappears in the server list.

Note: You may also export all system status information and component version information. From the main section, click **Export Report**.

Viewing and managing scheduled tasks

The LDD system lets you view and manage the schedule of the following tasks:

- Discovery
- Policy Update
- Script
- Report
- Backup & Restore

1. From LMC, click the **System** tab.
2. From the System section, select **Schedule**.
3. Do either of the following:
   - To add a task, click **Add**, and then select a task to schedule.
   - To edit a task, select a task, and then click **Edit**.

   Note: You can also delete a task.
4. If necessary, create a description for the task, and then click **Next**.
5. Configure the settings. Do one of the following:
   - To schedule a Discovery task or a Policy Update task, select a device group, and then click **Next**.
   - To schedule a Report task, select a report, and then configure its parameters. Click **Next**. For more information, see "Scheduling a report" on page 79.
   - To schedule a Backup & Restore task, type the path of the backup share and the credentials required to access the specified share, and then click **Next**. For more information, see "Scheduling automatic backups" on page 85.
   - To schedule a Script task, select a group type, and then click **Next**. For more information, see "Scheduling scripts" on page 90.
6. Configure the date, time, and frequency for the task.
7. Click **Finish**.

Configuring the confirmation page

When a job is completed, a confirmation is automatically delivered unless it is disabled within a particular solution.

1. From LMC, click the **Services** tab.
2. From the Services section, select **Confirm**.
3. From the Tasks section, select **Parameters**.
4. Select the lowest level of messages to include in confirmations:
   - **debug**—Includes detailed messages that are used to diagnose problems, and other message levels lower than this level
   - **info**—Includes messages that indicate successful job activities, and other message levels lower than this level
   - **warn**—Includes messages that indicate potential problems, and other message levels lower than this level

- **error**—Includes messages that indicate unsuccessful job activities, and other message levels lower than this level
- **fatal**—Includes only messages that indicate complete failure of jobs

5 Type a title for the confirmation page or message.

6 Select the task used to deliver the confirmation page:

- **confirm.printPS**—Prints a confirmation page in PostScript format
- **confirm.printPDF**—Prints a confirmation page in PDF format
- **confirm.emailAdmin**—Sends a message to the administrator e-mail address with a PDF confirmation page attached
- **confirm.emailAdminTextOnly**—Sends a message containing the confirmation information to the administrator e-mail address with no attachments

Note: To use the confirm.emailAdmin or confirm.emailAdminTextOnly tasks, the e-mail service must be configured correctly.

7 If you are using e-mail confirmations, then in the "Admin email address" field, type the address where e-mail confirmations are sent.

8 If necessary, configure the remaining parameters.

9 Click **Apply**.

Adding servers to the system after initial installation

New servers may be added to an existing system to increase capacity, or servers may be replaced without reinstalling other components. When a new server is installed on a system that has existing solutions, the solutions and all associated settings must be added to the new server. If the new server does not have the same services as existing servers, then jobs that use the solution with missing services fail.

Note: Any third-party services that are used with existing solutions must be installed manually.

1 Add the computer where you are going to install the new server.

2 Using an NTP server, synchronize the time on all computers that are used in the LDD system.

3 Install the server. For more information, see “Installing servers” on page 37.

4 On the new server, install any third-party services that the existing solutions require.

5 From LMC, click the **System** tab.

6 Set the new server online. For more information, see “Viewing and changing server status” on page 64.

Changing the IP address on a configuration 1 system

The following allow the IP address of the components to be changed without reinstallation:

- An incorrect IP address or FQDN is used when installing a configuration 1 system.
- The IP address of the computer on which the components of a configuration 1 system are installed changes.

1. From the command line on the computer where all components are installed, navigate to the **Lexmark \Solutions\InstallHelper** folder in the location where the components are installed.
2. Do either of the following:
   - To use the IP address of the local computer, type **`update-addr.bat -ip`**, and then press **Enter**.
   - To use the FQDN of the local computer, type **`update-addr.bat -hostname`**, and then press **Enter**.
3. Change the LMC desktop shortcut to the new IP address or host name. Do the following:
   a. On the desktop of the computer where the components are installed, right-click the LMC shortcut, and then click **Properties**.
   b. Click the **Shortcut** tab, and then click **Find Target** or **Open File Location**.
   c. Right-click the LMC shortcut, and then click **Properties**.
   d. In the URL field, type the new IP address or host name of the local computer. The complete URL must be **`http://hostname:9780/lmc/`**, where ***`hostname`*** is the host name or IP address of the computer where the components are installed.

Changing the IP address on a configuration X-Y-N system

In an enterprise environment, an error may occur when the following are installed in three different computers and their IP addresses change:

- Database server (Firebird or Microsoft SQL Server)
- Load balancer
- LDD application server

For the database server (Firebird)

Note: Configuration is not necessary for Microsoft SQL Server.

1. From your computer, navigate to the **C:\ProgramFiles\Lexmark\Solutions\InstallHelper** folder.
2. Run **Update-addr.bat**, and then enter **`update-addr.bat –ip <DB_IPaddress>`**, where ***`<DB_IPaddress>`*** is the new database server IP address.
3. From the Framework DB section, make sure that the LOADBALANCER and SERVER tables are blank.

For the load balancer

1. From your computer, navigate to the **C:\ProgramFiles\Lexmark\Solutions\InstallHelper** folder.
2. Run **lpm-update-address.bat**, and then enter **`lpm-update-addr.bat –ip <LB_IPaddress>`**, where ***`<LB_IPaddress>`*** is the new load balancer server IP address.
3. Stop all LDD services and Apache 3.
4. From the registry, do either of the following:

   For Firebird

   Update **`HKLM\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\ApacheAgent\Parameters\Start`** to the following:

   ```
   Params [REG_MULTI_SZ] = "start <DB_IPaddress> <LB_IPaddress> 9705 C:\Program Files
   \Lexmark\Solutions Firebird"
   ```

For Microsoft SQL Server

Update **HKLM\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\ApacheAgent\Parameters\Start** to the following:

```
Params [REG_MULTI_SZ] = "start <DB_IPaddress> <LB_IPaddress> 9705 C:\Program Files
\Lexmark\Solutions MSSQL"
```

Where:

- ***<DB_IPaddress>*** is the new database server IP address.
- ***<LB_IPaddress>*** is the new load balancer server IP address.

For the LDD application server

1. From your computer, navigate to the **C:\ProgramFiles\Lexmark\Solutions\InstallHelper** folder.
2. Run **lpm-update-address.bat**, and then enter **lpm-update-addr.bat -ip *<LB_IPaddress>***, where ***<LB_IPaddress>*** is the new load balancer server IP address.
3. Navigate to the **C:/Program Files/Lexmark/Solutions/apps/wf-ldss/WEB-INF/classes/adaptor.properties** file, and then update the following:
   - **adaptor.canonicalhostname=*<LB_IPaddress>***
   - **adaptor.address=*<LB_IPaddress>***
   - **centralwebdav.canonicalhostname=*<LB_IPaddress>***

   Where ***<LB_IPaddress>*** is the new load balancer server IP address.
4. Navigate to the **C:/Program Files/Lexmark/Solutions/apps/wf-ldss/WEB-INF/classes/dbProduct.properties** file, and then update the following:

   database.hostname=*<DB_IPaddress>*

   Where ***<DB_IPaddress>*** is the new database server IP address.
5. Navigate to the **C:/Program Files/Lexmark/Solutions/apps/wf-ldss/lmc.url** file, and then update the following:

   URL=http://*<LB_IPaddress>*:9780/lmc

   Where ***<LB_IPaddress>*** is the new load balancer server IP address.
6. Restart all LDD services.

Open LMC using the new load balancer IP address.

Restarting the LDD system

1. From LMC, click the **System** tab.
2. From the System section, select **System Status**.
3. Set all servers offline. For more information, see “Viewing and changing server status” on page 64.

   Note: Make sure that all jobs are completed before the server goes offline.
4. Turn off all server computers, load balancer computers, and database computers.
5. Turn on all database computers, load balancer computers, and server computers.

   Note: You can turn on the server components in any order.
6. From LMC, click the **System** tab.

7 From the System section, select **System Status**.

8 Set all servers online. For more information, see "Viewing and changing server status" on page 64.

Note: Starting all services may take several minutes when the system is first booted. If LMC cannot be accessed immediately after starting the system, then wait a few minutes, and then try again.

Restarting the Lexmark Solutions Application Server

When installing a workflow solution that includes a component, restart the Lexmark Solutions Application Server.

Restarting the Lexmark Solutions Application Server reverts the solution-related files of the following folders to the default version that is stored with the solution package:

- **\Lexmark\Solutions\apps\wf-ldss**
- **\Lexmark\Solutions\apps\wf-ldss\solutions**

1 From LMC, click the **System** tab.

2 From the System section, select **System Status**.

3 Set all servers offline. For more information, see "Viewing and changing server status" on page 64.

Note: Make sure that all jobs are completed before the server goes offline.

4 From the Windows Services control panel, restart the Lexmark Solutions Application Server.

Uninstalling LDD components

1 From LMC, click the **System** tab.

2 From the System section, select **System Status**.

3 Set all servers offline. For more information, see "Viewing and changing server status" on page 64.

Note: Make sure that all jobs are completed before the server goes offline.

4 If the database or load balancer is installed on a failover cluster, then do the following:

a On the primary node of each cluster, close all applications that are using the shared drive where LDD components are installed.

b From Failover Cluster Manager, move all cluster resources to the primary node where the LDD components are originally installed.

c Stop the cluster service on standby nodes.

Before continuing the upgrade, wait for confirmation that the standby nodes are disabled.

5 From the computer where the components are installed, navigate to the Lexmark folder, and then uninstall LDD.

Note: If a database or a load balancer is installed on a failover cluster, then use the node where the component is originally installed.

6 Follow the instructions on the screen.

Updating the AP Bundle

The AP Bundle is an eSF application that LDD installs on X642 printers and e-Task 5, e-Task 4, e-Task 3, e-Task 2+, and e-Task 2 MFPs and SFPs. This application is required for LDD support and provides prompting capabilities, application profiles or held jobs support, and security support for printers with LDD.

1. From LMC, click the **System** tab.
2. From the System section, select **AP Bundle**.
3. Browse to the AP Bundle application file (.fls), and then browse to the AP Bundle descriptor file (.xml).

   Notes:

   - To prevent overwriting existing files, clear **Overwrite if file already exists**.
   - To update the AP Bundle, the descriptor file is required.
   - To change the default settings of the AP Bundle on e-Task 2+ printers, edit the value attributes of the property elements in the descriptor file. Adding or removing settings in the descriptor file does not affect the application.
4. Click **Upload**.

   During the next policy update, LDD updates the AP Bundle on printers where it has not been installed or when an older version is installed.

   Note: If a printer already has a newer version of the AP Bundle installed, then the version specified for the update is not installed.

Enhancing security for Denial of Service attacks

1. Using a text editor, open the **httpd.conf** file from the ***<install-Dir>*/Lexmark/Solutions/Apache2/conf** directory, where ***<install-Dir>*** is the installation folder of LDD.
2. From the **`LoadModule`** section, uncomment the **`mod_evasive`** module.

   ```
   #LoadModule evasive2_module modules/mod_evasive2.so
   ```
3. From the white list section, add the appropriate IP addresses.

Sample white list

```
DOSWhitelist 127.0.0.1
DOSWhitelist 127.0.0.*
```

   Note: The IP addresses must be in the white list because the **`mod_evasive`** module restricts access to the Apache WebDAV folder.
4. Save the file.

Managing system performance

Note: The System Health feature is available only on LDD version 5.1 or earlier.

Accessing the System Health dashboard

1. From LMC, click the **System** tab.
2. From the System section, select **System Status**.
3. Click **System Health**.

Monitoring system health

From LMC, access the System Health dashboard. For more information, see "Accessing the System Health dashboard" on page 71.

Note: Make sure that Adobe Flash® Player 10 or later is installed and ActiveX controls are enabled on your web browser.

The following indicators show the overall health of the LDD system:

- **Overloaded**—The indicator changes color depending on the overload condition of the system:
  - **Green**—No servers are overloaded, and all servers are operating at normal capacity.
  - **Yellow**—One or more servers are overloaded, but at least one server is not. Overloaded servers operate at diminished capacity until they are no longer overloaded.
  - **Red**—All servers are overloaded and operating at diminished capacity.
- **Task / Hour**—Shows the current hourly task rate, based on tasks done in the past minute.
- **Threshold Exceptions**—Shows the hourly rate of tasks that exceed the threshold time set for each job on each server, based on tasks done in the past minute.

To view the performance data for an individual server, from the Server Health section, select the address of the server from the list. The following data are shown for overall server performance:

- **Task Count**—Shows the number of jobs running on the server over time.
- **Overload Events**—Shows the hourly rate of overload events. An overload event occurs when the number of tasks exceeds the configured design load and ends when the number of tasks reaches the configured recover load.

  Note: For more information on design load and recover load, see "Tuning the load balancer for unequal servers" on page 73.

The following task-specific data are shown for the task selected from the list:

- **Task / Hour**—Shows the current hourly task rate for the selected task, based on tasks done in the past minute.
- **Threshold Exceptions**—Shows the hourly rate of the task that exceeds the threshold time set for the selected task, based on tasks done in the past minute.

  Note: To change the threshold time for the selected task on the selected server, enter a new value beside "Set threshold (seconds)," and then click **Apply**.

To view a specific performance graph, from the Server Health section, click the graph. To return to the view of all graphs, click the graph again.

Notes:

- If a graph reaches a significant number of data points, then each two points are averaged. New data is recorded as normal until the maximum number of data points is reached.
- The Concurrently Running Task Limit and Load Factor slider controls are used to tune system performance. For more information, see "Adjusting limits on concurrent jobs" on page 73 and "Tuning the load balancer for unequal servers" on page 73.

Understanding the LDD server health check APIs

URL	Method	Headers key	Value	Body	Description
http://<*IPaddress*>:9780/lmc/rws/status/getserversinfo Where ***<IPaddress>*** is the IP address of the load balancer.	POST	Accept	application/json or application/xml	data type application/json	This API lets you specify a list of servers, and the API can be called to each one of the LDD servers to get a status of each server. The API returns a payload that contains each server and the corresponding status of each server. This payload must be returned in a JSON response format. **Note:** Depending on the LDD installation type, send a JSON array with the IP address or host name. For example, **["ipaddress1", "ipaddress2"]**.
http://<*IPaddress*>:9780/lmc/rws/systemhealth/overloaded Where ***<IPaddress>*** is the IP address of the load balancer.	GET	Accept	application/json or application/xml		This API provides the results of the existing "SystemHealth" MBean "Overloaded" method in XML or JSON format.
http://<*IPaddress*>:9780/lmc/rws/systemhealth/overloadedeventsperhour Where ***<IPaddress>*** is the IP address of the load balancer.	GET	Accept	application/json or application/xml		This API provides the results of the existing "SystemHealth" MBean "Overloadedeventsperhour" method in XML or JSON format.

Adjusting limits on concurrent jobs

A server that meets recommended requirements can process 30 concurrent jobs from clients. If a server is faster than the recommended system, then raise the limit on concurrent jobs for that server to increase system capacity. If a server is slower than the recommended system, then lower the limit on concurrent jobs to maintain system reliability.

Warning—Potential Damage: Setting high limits on concurrent jobs may cause failures with some solutions, including insufficient memory errors, timeouts, very slow system response, and database failures. Make sure that databases are properly backed up before raising limits.

The adjustment sets the baseline design load for the server, and the recover load is set at 80 percent of the design load. If jobs running on the server exceed the design load, then the load balancer reduces job submissions to the server until the recover load is reached.

To change the limit on concurrent jobs, do the following for each server:

1. From LMC, access the System Health dashboard. For more information, see "Accessing the System Health dashboard" on page 71.
2. From the Server Health section, select a server address.
3. Adjust the Concurrently Running Task Limit slider to the preferred limit for the server.
4. Click **Apply**.

   Note: These settings are not saved when performing a system upgrade. Configure the settings again after upgrading.

Tuning the load balancer for unequal servers

The ideal job distribution depends on the following:

- Hardware
- Network environment
- Solution being run

When all servers in the system are approximately equal, server loads must be optimal without manually tuning the load balancer. If servers are unequal, then the least powerful machine determines the overall throughput. To increase the overall job capacity of the system, assign a load balancing factor to each server. This configuration routes more traffic to more powerful machines and helps prevent overloading.

Each load balancer distributes jobs to servers in proportion to the load balancing factors that are assigned to each server. For example, in a system with three servers with load balancing factors of 10,10, and 20, do the following configuration:

- The first two servers must each receive 25 percent of jobs.
- The third server must receive 50 percent of jobs.

To determine the optimal proportions for load balancing factors, run performance tests on each server. Some factors such as memory, number of processors, or CPU speed may suggest an initial value for the load balancing factor to add more system capacity.

Note: Performance improvements are not linear functions of numerical improvements in hardware.

To assign a load balancing factor to each server, do the following:

1. From LMC, access the System Health dashboard. For more information, see “Accessing the System Health dashboard” on page 71.
2. From the Server Health section, select a server address.
3. Adjust the Load Factor slider to the preferred load balancing factor for the server.
4. Click **Apply**.

   Note: These settings are not saved when performing a system upgrade. Configure the settings again after upgrading.

The load balancer is composed of three different Tomcat load balancing workers that separately manage LMC sessions and job submissions from e-Task 3, e-Task 2, and e-Task printers. The adjustment affects the e-Task 3, e-Task 2, and e-Task load balancers, but not the LMC load balancer.

Assigning servers to run LMC only or process jobs

When using more than one server in a system, you can assign some servers to run LMC only and other servers to only process jobs.

When using a configuration 1-N, X-N, or X-Y-N system with the recommended hardware, we recommend doing the following:

- Install the server component on the RAID 1 array where the operating system is installed on the load balancer computer. Configure it to run LMC only.
- Configure the servers that are installed on dedicated computers to only process jobs.

1. From your web browser, launch JK Status Manager by using the URL **`http://loadbalancer:9780/status/?opt=454`**. ***`Loadbalancer`*** is the IP address of the computer where the load balancer is installed.

   Server information and the worker status for each of the three load balancing workers appear. Each server in the system is listed as a worker in each Balancer Members list.
2. For each server that must only process jobs, stop the associated worker on the adminloadbalancer load balancing worker. Do the following:
   a. From the “Worker Status for adminloadbalancer” section, click **E** beside the server name.
   b. Stop the activation.
   c. Click **Update Worker**.
3. For each server that must run LMC only, stop the associated worker on the clientloadbalancer and adaptorloadbalancer load balancing workers. Do the following:
   a. From the “Worker Status for clientloadbalancer” and "Worker Status for adaptorbalancer" sections, click **E** beside the server name.
   b. Stop the activation.
   c. Click **Update Worker**.

Notes:

- Make sure that at least one server is assigned to run LMC and at least one server is assigned to process jobs.
- We do not recommend changing other load balancer and server properties.

Configuring chunk size for device discovery and policy updates

When using three or more servers, reducing the chunk size may increase the speed of device discovery and policy updates.

1. From LMC, click the **Services** tab.
2. From the Services list, select **General**.
3. From the Tasks list, select **Parameters**.
4. In the ChunkSize field, enter a new value. When using three or more servers, a value as low as **2** is sufficient.
5. Click **Apply**.

Configuring communications

Configuring the connection to an SMTP server

1. From LMC, click the **Services** tab.
2. From the Services section, select **Email**.
3. From the Tasks section, select **Parameters**.
4. Type the e-mail server host name or IP address.
5. Type the user name and password used to log in to your SMTP server.
6. Enter the e-mail server connection timeout in seconds. The default value is **60**.
7. Enter the e-mail server I/O timeout in seconds.
8. Click **Apply**.

Configuring NPA device communication

To improve reliability during device discovery, configure the timeout periods between communication retries.

1. From LMC, click the **Services** tab.
2. From the Services section, select **NPA**.
3. From the Tasks section, select **Parameters**.
4. In the NPANT Timeout field, enter a timeout period in milliseconds for each retry in sequence, separating each by a space. The default values are **1000** and **5000**.
5. In the Unsecure Port field, enter the port number used for NPA on your network. The default value is **9300**.
6. Click **Apply**.

Configuring SNMP for discovering devices

Enabling the local settings

1. From LMC, click the **Device Groups** tab.
2. From the Device Groups section, select a device group.
3. From the Tasks section, select **SNMP**, and then clear **Use Global**.
4. In the Port field, enter the port number used for SNMP on your network. The default value is **161**.
5. In the Timeouts/Retries field, enter a timeout period in milliseconds for each retry in sequence, separating each by a space.
6. Do either of the following:
   - Configure SNMP version 3.
     a. Select **SNMP v3**.
     b. Configure the SNMPv3 minimum authentication level.
     c. In the SNMPv3 Read/Write User field, type the read and write user name.
     d. In the SNMPv3 Read/Write Password field, type the read and write user name.
     e. In the SNMPv3 Read Only User field, type the read user name.
     f. In the SNMPv3 Read Only Password field, type the read password.
     g. Configure the following:
        – SNMPv3 Authentication Hash
        – SNMPv3 Privacy Algorithm
   - Configure SNMP versions 1 and 2.
     a. In the Write Community Name field, type the write community string for printers on your network.
     b. In the Read Community Name field, type the read community string for printers on your network.
     c. Clear **SNMP v3**.
7. Click **Apply**.

Enabling the global settings

Do either of the following:

- Using the Device Groups tab
  1. From LMC, click the **Device Groups** tab.
  2. From the Device Groups section, select a device group.
  3. From the Tasks section, select **SNMP**, and then select **Use Global**.
  4. Click **Apply**.
- Using the Services tab
  1. From LMC, click the **Services** tab.
  2. From the Services section, select **SNMP**.
  3. From the Tasks section, select **Parameters**.
  4. In the Port field, enter the port number used for SNMP on your network. The default value is **161**.
  5. In the Timeouts/Retries field, enter a timeout period in milliseconds for each retry in sequence, separating each by a space.

6 Do either of the following:
   - Configure SNMP version 3.
     a Select **SNMP v3**.
     b Configure the SNMPv3 minimum authentication level.
     c In the SNMPv3 Read/Write User field, type the read and write user name.
     d In the SNMPv3 Read/Write Password field, type the read and write user name.
     e In the SNMPv3 Read Only User field, type the read user name.
     f In the SNMPv3 Read Only Password field, type the read password.
     g Configure the following:
       - SNMPv3 Authentication Hash
       - SNMPv3 Privacy Algorithm
   - Configure SNMP versions 1 and 2.
     a In the Write Community Name field, type the write community string for printers on your network.
     b In the Read Community Name field, type the read community string for printers on your network.
     c Clear **SNMP v3**.
7 Click **Apply**.

Note: Global settings are used for printers that are in multiple device group discovery profiles.

Configuring printer security

Note: Only authentication through password, PIN, LDAP, or LDAP+GSSAPI is supported. Make sure that the Basic Security template matches the authentication type and the password or PIN that are configured in Lexmark Management Console.

Enabling the local settings

1 From Lexmark Management Console, click the **Device Groups** tab.
2 From the Device Groups section, select a device group.
3 From the Tasks section, select **SNMP**, and then clear **Use Global**.
4 Select the authentication type for the printer.
5 Type the authentication value for Password or PIN, or the LDAP setup name for LDAP or LDAP+GSSAPI.

   Note: Make sure that the LDAP setup name is configured when using an e-Task 5 printer.
6 Click **Apply**.

Enabling the global settings

Do either of the following:

- Using the Device Groups tab
  1 From Lexmark Management Console, click the **Device Groups** tab.
  2 From the Device Groups section, select a device group.
  3 From the Tasks section, select **SNMP**, and then select **Use Global**.
  4 Click **Apply**.

- Using the Services tab
  1. From Lexmark Management Console, click the **Services** tab.
  2. From the Services section, select **DeviceSecurity**.
  3. From the Tasks section, select **Parameters**.
  4. Select the authentication type for the printer.
  5. Type the authentication value for Password or PIN, or the LDAP setup name for LDAP or LDAP+GSSAPI.

     Note: Make sure that the LDAP setup name is configured when using an e-Task 5 printer.
  6. Click **Apply**.

  Note: Global settings are used for printers that are in multiple device group discovery profiles.

Managing licenses

Adding licenses to an existing server

Note: Back up your current license files before updating with new files. To obtain the new license files, contact your Lexmark representative.

1. From Lexmark Management Console, click the **System** tab.
2. From the System section, select **Licenses**.
3. Click **Add License**.
4. Browse to the license file.
5. Click **Upload**.

   Notes:

   - Uploading license files copies them to the program folder. You can safely move the license files from the temporary location where you saved them.
   - Licenses that belong in the same file are selected together in the list. To remove licenses, click **Remove**. For more information on obtaining licenses, see “Obtaining licenses” on page 26.

Managing reports

Running a report

Note: We recommend running reports during off-peak hours to avoid affecting system performance.

1. From LMC, click the **System** tab.
2. From the System section, select **Reports**.
3. In the Available Reports list, select a report.

4 Specify the reporting period, and then select an output format.

Note: Each report has a default output format. For more information on custom reports, contact the designer of your custom report.

5 Save the report or send it in an e-mail.

- To save the report, do the following:
  a Select **Save To**, and then click ... beside the field.
  b Using a UNC path for a shared folder, type a destination folder path.
  c Type your credentials.
  d Click **OK**.
- To send the report in an e-mail, do the following:
  a Select **Email To**, and then click ... beside the field.
  b If necessary, edit the e-mail, and then click **OK**.

6 If other query parameters are available for the selected report, then click **Additional Parameters** to specify values for those parameters. For more information, see "Adding special LDD parameters" on page 83.

Note: Additional Parameters can be defined only when including a report with a workflow solution during development. For more information, see the *Lexmark Document Distributor SDK Guide*.

7 Click **Run Report**.

The report is shown in a new window.

Notes:

- Only summary reports are supported. If a custom report does not have a summary section, then the finished report is blank.
- To view reports, enable pop-ups for LMC in your web browser.
- Adobe Reader® is required to view PDF reports.

Scheduling a report

Note: We recommend running reports during off-peak hours to avoid affecting system performance.

1 From LMC, click the **System** tab.

2 From the System section, select **Schedule**.

3 Click **Add** > **Report**.

4 If necessary, type a description for the task, and then click **Next**.

5 In the Available Reports list, select a report.

6 Specify the reporting period, and then select an output format.

Note: Each report has a default output format. For more information on custom reports, contact the designer of your custom report.

7 Save the report or send it in an e-mail.

- To save the report, do the following:
  a Select **Save To**, and then click ... beside the field.
  b Using a UNC path for a shared folder, type a destination folder path.

c Type your credentials.

d Click **OK**.

- To send the report in an e-mail, do the following:
  a Select **Email To**, and then click ... beside the field.
  b If necessary, edit the e-mail, and then click **OK**.

8 If other query parameters are available for the selected report, then click **Additional Parameters** to specify values for those parameters. For more information, see "Adding special LDD parameters" on page 83.

Note: Additional Parameters can be defined only when including a report with a workflow solution during development. For more information, see the *Lexmark Document Distributor SDK Guide*.

9 Click **Next**.

10 Configure the date, time, and frequency for the task.

11 Click **Finish**.

Note: Some solutions may include a script that runs a report with a predetermined configuration, which can be scheduled like any other script. Reports that run through a script can also be run separately for each server in the system. For more information, contact your solution developer.

Understanding built-in reports

Built-in reports show commonly used data and are designed for PDF output, except for those reports that specify CSV in the report title.

- **Jobs Report - CSV**—Shows the jobs list in CSV format.
- **Log Report - CSV**—Shows all log entries in CSV format.
- **Log Report - Failed Jobs**—Shows log entries for failed jobs.
- **Printer Report**—Shows printer usage data, such as printer success rates, printer model usage, printer usage per profile, and most active users per printer.
- **Report by Time**—Shows daily and hourly data, such as job totals, job success rates, printer usage, user usage, server usage, and job durations.
- **Server Report**—Shows server usage data, such as job success rates, hourly job rates, job duration, and server distribution. A summary for all servers and details for individual servers are available.
- **Software Client Report**—Shows software client usage data, such as software client success rates, software client usage per profile, and most active users per software client.
- **Solution Report**—Shows solution usage data, such as solution success rates, most used solutions, and how solutions are accessed.
- **Task Summary Report**—Shows task data, such as task attempts, task success rates, and task times. A summary and details for all tasks are available.
- **Tops Report**—Shows the most active of the following elements:
  - Users
  - Printers
  - Printer models
  - Profiles
  - User for each profile
  - Servers
  - User for each printer

  - Software client for each profile
  - User for each software client
  - Tasks
  - Printer for each profile
  - Scheduled scripts
- **User Report**—Shows user data, such as user job success rates, most active users, and job duration.

Adding a report

Note: Only summary reports are supported. If a custom report does not have a summary section, then the finished report is blank.

1. From LMC, click the **System** tab.
2. From the System section, click **Reports**.
3. Upload the report files. Do the following:
   a. Click **Upload Report Files**, and then browse to one of the following files:
      - .jasper compiled report file
      - .jpg or .png graphics included in the report
      - .jrxml report source files (optional)

      Note: To prevent overwriting existing files, clear **Overwrite if file already exists**.
   b. Click **Upload**.
      Selected files are copied to the **\Lexmark\Solutions\apps\wf-ldss\WEB-INF\reports** folder where the system is installed on each server.
4. In the Available Reports list, click ✚ or **Add**.
5. Type a descriptive report name.
6. Select the report file name for the compiled report that you uploaded.
7. Select the default output format.

   Note: Each report has a default output format. For more information on custom reports, contact the designer of your custom report.
8. Select the data source that the report is designed to access. Commonly used databases include the following:
   - **MONITOR**—Used by reports that access the jobs list and the log
   - **SOLUTIONINFO**—Used by some solutions to store custom data
9. Click **Save**.

Editing report settings

1. From LMC, click the **System** tab.
2. From the System section, click **Reports**.
3. In the Available Reports list, select a report, and then click ✎ or **Edit**.

4 Edit the report settings. Do one or more of the following:
   - Type a descriptive report name.
   - Select the report file name for the compiled report that you uploaded.
   - Select the default output format.

     Note: Each report has a default output format. For more information on custom reports, contact the designer of your custom report.
   - Select the data source that the report is designed to access. Commonly used databases include the following:
     - **MONITOR**—Used by reports that access the jobs list and the log
     - **SOLUTIONINFO**—Used by some solutions to store custom data
5 Click **Save**.

Removing a report

1 From LMC, click the **System** tab.
2 From the System section, click **Reports**.
3 In the Available Reports list, select a report.
4 Click or **Delete** > **Yes**.

Notes:

- Scheduled report tasks that are associated with the deleted report are automatically deleted.
- Scheduled script tasks that use the deleted report are not detected and must be deleted manually.

After removing a report from the Available Reports list, you can optionally delete associated files from the **\Lexmark\Solutions\apps\wf-ldss\WEB-INF\reports** folder on each server where LDD is installed.

Configuring default report options

1 From LMC, click the **System** tab.
2 From the System section, click **Reports**.
3 In the Available Reports list, select a report.
4 Configure one or more of the following report options:
   - Reporting period
   - Output format
   - Folder destination
   - E-mail destination
   - Other parameters

   Note: Clicking **Refresh Defaults** while configuring a report returns settings to defaults.
5 Click **Run Report**.

Creating custom reports

LDD uses JasperReports for custom reports. You can create custom reports by using the open-source application iReport 3.5.2. For more information on overall report design, see the documentation for iReport.

Note: Only summary reports are supported. If a custom report does not have a summary section, then the finished report is blank.

Adding special LDD parameters

To use special LDD parameters in other parts of a report, add the following parameters to the report design:

- **`start_date`**—Retrieves the start date for report data, as specified in a script or by the administrator when the report is run
- **`end_date`**—Retrieves the end date for report data, as specified in a script or by the administrator when the report is run
- **`SUBREPORT_DIR`**—Retrieves the reports at the **\Lexmark\Solutions\apps\wf-ldss\WEB-INF\reports** folder on each server where LDD is installed

Note: Special parameters can be defined only when including a report with a workflow solution during development. For more information, see the *Lexmark Document Distributor SDK Guide*.

Querying the database

Information for built-in reports and many custom reports are retrieved from the MONITOR database, which contains information about tasks. Custom reports may also retrieve information from the SOLUTIONINFO database, where some solutions store custom data.

The credentials for Firebird databases are the following:

- **User name**—**`framework`**
- **Password**—**`rivet`**

The TASK_LOG table in the MONITOR database contains the following fields:

- **ID**—A unique ID number that is assigned to each entry in the log.
- **LOG_TIME**—The time when an entry is added to the log.
- **STATUS**—The status reported by the solution that added the log entry.
- **PERCENT_COMPLETE**—The progress reported by the solution that added the log entry.
- **TASK_MESSAGE**—The log message reported by the solution.
- **TASK_ID**—The unique ID number that is assigned to a task. Each entry recorded from the same task has the same TASK_ID.

The TASK_INFO table in the MONITOR database contains the following fields:

- **TASK_ID**—The unique ID number that is assigned to each task.
- **HOST_NAME**—The host name of the server where the job is run.
- **TASK_NAME**
- **SOLUTION_NAME**—The name of the solution where the task is run.
- **STATUS**—The status that is reported when the job is completed or abandoned.
- **START_TIME**—The time when the job is received.
- **END_TIME**—The time when the job is completed or abandoned.

- **PERCENT_COMPLETE**—The progress reported by the job when it is completed or abandoned.
- **USER_ID**—The user who submitted the job (if applicable).
- **PRINTER**—The IP address of the printer or software client that submitted the job (if applicable).
- **ADDRESS**—The unique ID number of the printer that processed the job.
- **SCHEDULE_ID**—The unique ID number of the scheduled task that ran (if applicable).
- **PARENT_ID**—The unique ID number of the previous task that started the listed task (if applicable).
- **THREAD_NAME**—The name of the thread that is used by the task.
- **CLIENT_NAME**—The host name of the printer or software client that submitted the job (if applicable).
- **PRINTER_MODEL**—The printer model number reported by the printer that submitted the job (if applicable).
- **JOB_TYPE**—The device class for which the task runs a profile (if applicable).
- **HAS_SCANNER**—The Boolean value (**0** or **1**) for identifying whether the printer that submitted the job has a scanner.

Understanding included subreports

Some subreports are included with the installation, and may be useful in developing custom reports.

When using a subreport in a custom report, pass the following to any of the subreports by using the Parameters property of the subreport element:

- **`start_date`**
- **`end_date`**
- **`SUBREPORT_DIR`**

The different subreports are the following:

File name	Page orientation	Description
_portrait_title.jasper	Portrait	Shows a default header image, the title of the report, and the selected reporting period for use as a header in a report.
_landscape_title.jasper	Landscape	
_portrait_footer.jasper	Portrait	Shows the date when the report was created and the page number for use as a footer in the report.
_landscape_footer.jasper	Landscape	
_portrait_no_data_message.jasper	Portrait	Shows a message indicating that data was not found within the selected period. **Note:** By default, iReport does not generate a report if data is not found. To use a No Data node, change the setting for when data is not found in the report to **No Data Section**.
_landscape_no_data_message.jasper	Landscape	
_Printers_Least_Used	Either	Shows the printers that are least used to submit jobs.
_Printer_Models_Most_Used	Either	Shows the printer models that are most used to submit jobs.
_Printers_Most_Used	Either	Shows the printers that are most used to submit jobs.

File name	Page orientation	Description
_Server_Stats	Either	Shows a breakdown of job types that are run on a server. **Note:** This subreport uses the additional parameter **SERVER**, which contains the host name of the server for which the subreport must be run.
_Servers_Most_Used	Either	Shows the servers that have processed the most jobs.
_SoftwareClients_Most_Used	Either	Shows the software clients that are most used to submit jobs.
_Solution_Profile_Most_Used	Either	Shows the solution profiles that are most used for submitted jobs.
_Solution_Profile_Printers	Either	Shows the printers from where the most jobs are submitted for each profile.
_Solution_Profile_Scheduled_Scripts	Either	Shows the solution profiles that scheduled tasks run most frequently.
_Solution_Profile_SoftwareClients	Either	Shows the software clients from where the most jobs are submitted for each profile.
_Solution_Profile_Users	Either	Shows the users who have submitted the most jobs for each profile.
_Solutions_Most_Used	Either	Shows the solutions that are most used for submitted jobs.
_Task_Most_Run	Either	Shows the most frequently run tasks.
_Users_Most_Active	Either	Shows the users who have submitted the most jobs.
_Users_Most_Cancellations	Either	Shows the users who have canceled the most jobs.
_Users_Printers	Either	Shows the users who have submitted the most jobs for each printer.
_Users_SoftwareClients	Either	Shows the users who have submitted the most jobs from each software client.

Backup and disaster recovery

Note: The database backup and recovery tasks apply only to Firebird. If you are using Microsoft SQL Server, then contact your database administrator.

Scheduling automatic backups

You can back up the databases and solutions in an LDD system to a network folder. If a recovery is necessary, then a new system can access the recovery data by using Restore Install. You can direct existing servers from a partially failed system to the new load balancer and database, or you can install new servers.

When a scheduled backup occurs, the system does the following processes:

- Validate backup database files on the network folder.
- Send an e-mail message that indicates success or failure to the address specified for the “Admin email address” setting of the Confirm service.

- Record failures in the system log.

Note: We recommend scheduling backups during off-peak hours to avoid affecting system performance.

1. From LMC, click the **System** tab.
2. From the System section, select **Schedule**.
3. Click **Add** > **Backup & Restore**.
4. If necessary, type a description for the task, and then click **Next**.
5. Type the UNC path of the existing network folder where the system must be backed up.

   For example, **\\myserver\myshare**.

   Note: When storing backup data from multiple LDD systems, assign a different folder to each LDD system. Assigning a backup folder for each LDD system prevents existing data from being overwritten by another system. This configuration also helps you identify which LDD system the backup data belongs to.
6. If the network folder requires authentication, then type the user name and password.
7. To back up the jobs list and the log, select **Backup Jobs Logs Database**.
8. To keep previous backup sets, select **Keep previous backups**. This setting stores data from each backup in a folder named with the date of the backup within the specified network folder. If it is cleared, then backup data is stored directly in the specified network folder, overwriting any existing data.

   Note: The database containing the jobs list and the log may be very large. Make sure that you have sufficient space on the network folder where the files are backed up.
9. Click **Next**.
10. Configure the date, time, and frequency for the task.
11. Click **Finish**.

Note: You can delete dated backup folders containing entire previous backups, but do not modify the internal folder structure of backup data.

Recovering backup data with a new installation

If you are recovering backup data from a network folder, then use Restore Install. This feature enables a load balancer or both a database and a load balancer to access backup data.

1. Run the LDD installer, and then select the appropriate installation options. Do one of the following:
   - If a workgroup system has failed, then install a workgroup system.
   - If both the database and load balancer or only the database has failed in an enterprise system, then install the database only.
   - If only the load balancer has failed in an enterprise system, then install the load balancer only.
2. Before proceeding to the final step of each installation, select **Restore Install (RI)**, and then browse to the .ri file.
3. Follow the instructions on the screen.
4. If you are using an enterprise system and you have just installed the database, then run the installation again for the load balancer.

5 If you are using an enterprise system, then add servers to the system and set them online.
- If you are installing new servers, then see "Installing new servers during recovery" on page 87.
- If you are using existing servers, then see "Connecting existing servers during recovery" on page 87.

6 If a new IP address or FQDN is identified for the load balancer, then do the following:
   a Recreate any LDD printer ports on software clients. For more information, see "Recreating LDD printer ports after a change of IP address or FQDN" on page 89.
   b Change the settings for any associated eSF applications that specify the load balancer address. For more information, see "Configuring an eSF application associated with a solution" on page 99.

Installing new servers during recovery

1 Using an NTP server, synchronize the time on all computers that are used in the LDD system.

2 Using the new database or load balancer, install the server. For more information, see "Installing servers" on page 37.

3 On the new server, install any third-party services that the existing solutions require.

4 Do either of the following:
- Perform a policy update for any device groups that contain e-Task printers. This configuration applies when the same IP address or FQDN is identified for the new database and load balancer.
- Perform a policy update for all device groups. This configuration applies when a new IP address or FQDN is identified for the backup database or load balancer.

Note: Clear **Only update those devices which are Out of Policy** when performing the policy update.

5 From LMC, click the **System** tab.

6 From the System section, select **System Status**.

7 Set all servers online. For more information, see "Viewing and changing server status" on page 64.

Note: Multiple non-communicating servers may affect system performance. If you do not expect a non-communicating server to reestablish communication quickly, then remove it. For more information, see "Viewing and changing server status" on page 64.

Connecting existing servers during recovery

After the database or load balancer is recovered, do either of the following:

- If the same IP address or FQDN is identified for the new database and load balancer, then do the following:
  1 Using an NTP server, synchronize the time on all computers that are used in the LDD system.
  2 Restart the Lexmark Solutions Application Server. For more information, see "Restarting the Lexmark Solutions Application Server" on page 69.
  3 Perform a policy update for any device groups that contain e-Task printers. For more information, see "Updating policies for device groups" on page 112.

  Note: Clear **Only update those devices which are Out of Policy** when performing the policy update.
  4 From LMC, click the **System** tab.
  5 From the System section, select **System Status**.
  6 Set all servers online. For more information, see "Viewing and changing server status" on page 64.

- If a new IP address or FQDN is identified for the new database or load balancer, then do the following:
  1. Using an NTP server, synchronize the time on all computers that are used in the LDD system.
  2. From LMC, click the **System** tab.
  3. From the System section, select **System Status**.
  4. Set all servers offline. For more information, see "Viewing and changing server status" on page 64.

     Note: Make sure that all jobs are completed before the server goes offline.
  5. From the Windows Services control panel, stop the Lexmark Solutions Application Server.
  6. Change the property of the adaptors.

     If you are using a new load balancer, then do the following:
     a. Locate the **\Lexmark\Solutions\apps\wf-ldss\WEB-INF\classes\adaptor.properties** file where the server is installed.
     b. Change the **`adaptor.address`** and the **`adaptor.canonicalhostname`** properties to the FQDN of the new load balancer.

        Note: If the setting is an IP address, then use the IP address of the new load balancer. If the setting is an FQDN, then use the FQDN of the new load balancer.

     If you are using a new database, then do the following:
     a. Locate the **\Lexmark\Solutions\apps\wf-ldss\WEB-INF\classes\database.properties** file where the server is installed.
     b. Change the **`database.hostname`** property to the FQDN of the new database.

        Note: If the setting is an IP address, then use the IP address of the new database. If the setting is an FQDN, then use the FQDN of the new database.
  7. Change the LMC desktop shortcut on the server. Do the following:
     a. On the desktop of the computer where the server is installed, right-click the LMC desktop shortcut, and then click **Properties**.
     b. Click the **Shortcut** tab, and then click **Find Target** or **Open File Location**.
     c. In the URL field, type the new IP address or host name of the new load balancer. The complete URL must be **`http://hostname:9780/lmc/`**, where ***`hostname`*** is the host name or IP address of the new load balancer.
  8. Restart the Lexmark Solutions Application Server. For more information, see "Restarting the Lexmark Solutions Application Server" on page 69.
  9. Perform a policy update for all device groups. For more information, see "Updating policies for device groups" on page 112.

     Note: Clear **Only update those devices which are Out of Policy** when performing the policy update.
  10. From LMC, click the **System** tab.
  11. From the System section, select **System Status**.
  12. Set all servers online. For more information, see "Viewing and changing server status" on page 64.

Recreating LDD printer ports after a change of IP address or FQDN

If a new IP address or FQDN is identified for the database or load balancer, then recreate LDD printer ports on software clients.

1. From your computer, in the Windows "Devices and Printers" control panel, right-click an LDD print queue, and then click **Properties**.

   Note: For more information on accessing the properties for the Lexmark Document Server port, see "Configuring a Lexmark Document Server port" on page 128.

2. Click the **Ports** tab, and then click **Change Port Settings**.
3. Click **Add Port** > **Lexmark Document Server Port - Enterprise** > **New Port**.

   Note: The port name must be 75 characters or fewer.

4. Add a Lexmark Document Server port. Do the following:
   a. Click **Manage List**.
   b. From the Server Setup dialog box, click **Add**.
   c. Type the IP address or FQDN of the load balancer, and then click **OK**.
   d. Select the old database or load balancer from the list, and then click **Remove** > **Yes**.
   e. Click **OK**.
5. Select the new server from the Document Server list, and then click **Next**.
6. Select a profile on the server to use with the port, and then click **Next**.

   Note: If the server is running multiple jobs, then profiles on the server may not appear in the list. Wait until the server is not busy, and then add the port again.

7. Click **Finish**.
8. If necessary, when using pooled ports, add other ports by using the same server and profile.
9. Check that only newly created ports are selected, and then click **Apply**.
10. For each port associated with the failed load balancer, do the following:
    a. Select the port from the list.
    b. Click **Delete** > **Yes**.

       Note: If a port cannot be deleted, then it may still be associated with the print queue. Make sure that only newly created ports are selected, click **Apply**, and then try again.

11. If necessary, select the newly created ports again.
12. Click **Close**.

Manually backing up databases

You can back up the LDD databases by using any normal Firebird backup procedure. For manual backups, you can use **GBAK.exe**, located in the **\Lexmark\Solutions\firebird\bin** folder within the folder where the LDD load balancer or database is installed.

The following databases, located in the **\Lexmark\Solutions\firebird\data** folder within the folder where the LDD database is installed, must be included in the backup:

- EFORMS.FDB
- FRAMEWORK.FDB
- LICENSE.FDB
- MONITOR.FDB
- QUARTZ.FDB
- SOLUTIONINFO.FDB
- WEBAPPCONFIG.FDB

The credentials for each database are the following:

- **User name—framework**
- **Password—rivet**

The following command is recommended for each file:

***LDD_folder*\firebird\bin\gbak.exe -v -t -user framework -password rivet "*DB_IP_address*:*LDD_folder*\firebird\data*source_db*" "*backup_db*"**

where:

- ***LDD_folder*** is the folder where the LDD database is installed. This folder typically starts with a prefix **C:\Program Files\Lexmark\Solutions**.
- ***DB_IP_address*** is the IP address of the LDD database.
- ***source_db*** is the file name of the database file to back up.
- ***backup_db*** is the path and file name of the backup database file (.fbk).

Scheduling scripts

1. From LMC, click the **System** tab.
2. From the System list, select **Schedule**.
3. Click **Add** > **Script**.
4. If necessary, type a description for the task, and then click **Next**.
5. Select a group type. Do one of the following:
   - To associate the script with a device group, click **DeviceGroup** > **Next**. Select a device group, and then click **Next**.
   - To associate the script with a software client group, click **SftClientGroup** > **Next**. Select a software client group, and then click **Next**.

     Note: You can select only one device group or one software client group for a script task.
   - To schedule the script without associating it with a device group or software client group, click **None** > **Next**.

     Note: A script that is not associated with a device group or software client group can access global solution settings only.

6 Select a solution, and then select a script.

Note: If the script applies to individual servers, then click **Run on All Servers**. If the script uses information on the Additional Options field, then type the necessary information. For more information on the Additional Options settings, contact your solution developer.

7 Click **Next**.

8 Configure the date, time, and frequency for the task.

9 Click **Finish**.

Managing solutions

Deployment process overview

1. From LMC, click the **System** tab.
2. From the System section, select **System Status**.
3. Set all servers offline. For more information, see “Viewing and changing server status” on page 64.

   Note: Make sure that all jobs are completed before the server goes offline.
4. Upload the solution to the system. For more information, see “Uploading solutions to the LDD system” on page 98.
5. Configure the global settings. For more information, see “Configuring global solution settings” on page 98.
6. Create a device group for printers where you are going to deploy the solution. For more information, see “Creating a device group” on page 102.
7. To add printers to the device group, create discovery profiles. For more information, see “Creating a discovery profile” on page 103.
8. Discover printers in the device group. For more information, see “Manually discovering printers” on page 105.
9. Deploy the solution to the device group. For more information, see “Deploying solutions to a device group” on page 107.
10. Customize the home screens for the device group. For more information, see “Customizing the home screen for a device group” on page 107.
11. Perform a policy update. For more information, see “Updating policies for device groups” on page 112.
12. Set all servers online. For more information, see “Viewing and changing server status” on page 64.

Note: If your solution developer included automatic configuration, then one or more steps may be completed automatically. For more information, see the documentation associated with the solution.

Understanding security setup configuration files for e-Task 5 printers

When setting up security for e-Task 5 printers, provide the security configuration data in specific XML tags of the UCF files that come with a solution.

The following tags enable LDD to do the following:

- Parse and extract the content in the tags.
- Pass inputs to the appropriate interface of the printer to configure the corresponding security settings.

Notes:

- To configure non-security parameters for e-Task 5 printers, deploy UCF files by using the **`configuration_files_ldd`** or **`configuration_data_ldd`** tags.

- LDD only passes these settings to the printer and does not validate them.
- For e-Task 4 or earlier printers, set up security for LDD by deploying UCF files.

Node data	Settings	Location	Description
ldap	• **name** • **address** • **port** • **anon_bind** • **machine_dn** • **machine_password** • **userid_attr** • **fax_attr** • **email_attr** • **fullname_attr** • **search_base** • **search_timeout** • **ssl_tls** • **require_cert** • **follow_referrals** • **use_obj_class_person** • **obj_class1** • **obj_class2** • **obj_class3** • **user_input** • **ab_cn** • **ab_sn** • **ab_givenname** • **ab_samaccountname** • **ab_uid** • **ab_mail_attr** • **ab_fax_attr** • **ab_display_name** • **size_limit** • **ab_use_user_creds** • **Group permissions**	1 From the Embedded Web Server, click **Settings** > **Security**. 2 In the Network Accounts section, click the LDAP network account.	Configures LDAP security blocks for the printer. **Note:** This section in the configuration file is similar to the **ldap** section in the security_settings.ucf file when exporting the printer configuration.

Node data	Settings	Location	Description
solution_ldd	N/A	1 From the Embedded Web Server, click **Settings** > **Security**. 2 In the Additional Login Methods section, click **Manage Permissions** for a solution account. 3 In the Group Name section, click **All Users**.	Configures specific Pluggable Authentication Modules (PAM) login permissions for the printer. **Note:** This section in the configuration file is similar to the **solution** section in the security_settings.ucf file when exporting the printer configuration.
public_permissions_ldd_clear	N/A	1 From the Embedded Web Server, click **Settings** > **Security** > **Login Methods**. 2 In the Public section, click **Manage Permissions**.	Configures public permissions for the printer. **Note:** This section in the configuration file is similar to the **public_permissions** section in the security_settings.ucf file when exporting the printer configuration.
device_security	N/A	1 From the Embedded Web Server, click **Settings** > **Security**. 2 From the Network Accounts section, in the Default Control Panel Login Method setting, click **Change**.	Configures the default control panel login method for the printer. **Note:** This section in the configuration file is similar to the **default_login_method** section in the security_settings.ucf file when exporting the printer configuration.
configuration_files_ldd	N/A	N/A	Deploys UCF files that contain non-security settings such as Embedded Solutions Framework (eSF) Instance strings, and specific eSF settings such as **esf.mobileauth.settings.organizationid "12345"**. **Note:** This section in the configuration file is similar to the **default_login_method** section in the security_settings.ucf file when exporting the printer configuration.

Node data	Settings	Location	Description
configuration_data_ldd	N/A	N/A	Embeds non-security eSF settings before deploying to the printer.
kerberos	N/A	N/A	Adds Kerberos configuration information that LDD extracts and sends to e-Task 5 printers.
kerberos_file	N/A	N/A	
permissions	N/A	N/A	

Checking the validity of the settings in the solution_ldd tag

1. Obtain the printer IP address. Do either of the following:
   - Locate the IP address on the top of the printer home screen.
   - View the IP address in the Network Overview section or TCP/IP section of the Network/Ports menu.
2. Open a web browser, and then type the printer IP address.
3. From the Embedded Web Server, set all printer permissions and settings manually.
4. Export the security settings UCF file.
5. Check the security settings UCF file for possible settings and values.

Sample configuration settings for the configuration_files_ldd tag

Note: The UCF file can contain either a subset of the settings or an entire configuration of the application.

```
<configuration_files_ldd>
<file>\\10.252.2.151\lexmark\omnikey5427ckdriver_instance.ucf</file>
<file>\\10.252.2.151\lexmark\IdleScreen_instance.ucf</file>
</configuration_files_ldd>

<configuration_files_ldd>
<file>C:\Users\Administrator\Downloads\omnikey5427ckdriver.ucf</file>
<file>C:\Users\Administrator\Downloads\IdleScreen.ucf</file>
</configuration_files_ldd>
```

Sample configuration settings for the configuration_data_ldd tag

Note: The UCF file can contain either a subset of the settings or an entire configuration of the application.

```
omnikey5427ckdriver_instance.ucf:
esf.version.omnikey5427ckdriver 1.2.1
esf.omnikey5427ckdriver.inst.1.settings.customproxformat.label "Dev2"
esf.omnikey5427ckdriver.inst.1.settings.customproxformat.type "64"
.....
.....
esf.omnikey5427ckdriver.inst.1.settings.customproxformat.adjust.mask "FF"
esf.omnikey5427ckdriver.inst.1.universally.unique.identifier "5cb6e113-7f6a-4c87-8656-
fdd181c4edf4"

mobileAuth_config_v0.2.10_premise.ucf:
esf.version.mobileAuth 0.2.10
esf.mobileAuth.settings.custom.text "To log in, hold your device to the label on the printer
control panel."
esf.mobileAuth.settings.custom.loginscrn.img ""
esf.mobileAuth.settings.organizationid "12345"
esf.mobileAuth.settings.identityserver.addr "https://10.199.64.254:8080/identity-
gateway/info"
esf.mobileAuth.settings.identityserver.ssl.cert ""
```

```
esf.mobileAuth.settings.clientid "sampleclientid"
esf.mobileAuth.settings.clientsecret "sampleclientsecret"
esf.mobileAuth.settings.socket.timeout "15"
```

Sample security setup configuration file

```
<?xml version="1.0" encoding="UTF-8"?>
<auth version="1">
  <ldap>
      <ab_cn>1</ab_cn>
      <ab_custom_attr1></ab_custom_attr1>
      <ab_custom_attr2></ab_custom_attr2>
      <ab_custom_attr3></ab_custom_attr3>
      <ab_display_name>0</ab_display_name>
      <ab_fax_attr>1</ab_fax_attr>
      <ab_givenname>1</ab_givenname>
      <ab_mail_attr>1</ab_mail_attr>
      <ab_samaccountname>1</ab_samaccountname>
      <ab_sn>1</ab_sn>
      <ab_uid>1</ab_uid>
      <ab_use_user_creds>0</ab_use_user_creds>
      <address>directory.lex.lexmark.com</address>
      <anon_bind>1</anon_bind>
      <email_attr>mail</email_attr>
      <fax_attr>facsimiletelephonenumber</fax_attr>
      <follow_referrals>0</follow_referrals>
      <fullname_attr>cn</fullname_attr>
      <homedir_attr>homeDirectory</homedir_attr>
      <machine_dn></machine_dn>
      <machine_realm></machine_realm>
      <name>Upasana</name>
      <obj_class1></obj_class1>
      <obj_class2></obj_class2>
      <obj_class3></obj_class3>
      <port>389</port>
      <require_cert>0</require_cert>
      <search_base>ou=employees,o=lexmark</search_base>
      <search_timeout>30</search_timeout>
      <size_limit>50</size_limit>
      <ssl_tls>0</ssl_tls>
      <use_ad_creds>0</use_ad_creds>
      <use_gssapi>0</use_gssapi>
      <use_kerberos_server>0</use_kerberos_server>
      <use_kerberos_ticket>1</use_kerberos_ticket>
      <use_obj_class_person>1</use_obj_class_person>
      <user_input>1</user_input>
      <userid_attr>uid</userid_attr>
      <machine_password></machine_password>
      <groups>
       <group>
        <name>All Users</name>
        <dn></dn>
        <is_all_users_group>1</is_all_users_group>
        <permissions>
         <name>esf.IdleScreen.chgBkgndFAC</name>
         <name>esf.IdleScreen.ChgBkgnd</name>
         <name>esf.IdleScreen.Idle</name>
         <name>esf.IdleScreen.showroomFAC</name>
        </permissions>
       </group>
      </groups>
  </ldap>

  <solution_ldd>
      <name>Card Authentication</name>
      <groups>
       <group>
        <name>All Users</name>
        <is_all_users_group>1</is_all_users_group>
        <permissions>
         <name>esf.IdleScreen.chgBkgndFAC</name>
         <name>esf.IdleScreen.ChgBkgnd</name>
```

```
        <name>esf.IdleScreen.Idle</name>
        <name>esf.IdleScreen.showroomFAC</name>
       </permissions>
      </group>
     </groups>
  </solution_ldd>

  <public_permissions_ldd_clear>
      <name>esf.IdleScreen.chgBkgndFAC</name>
      <name>esf.IdleScreen.ChgBkgnd</name>
      <name>esf.IdleScreen.Idle</name>
      <name>esf.IdleScreen.showroomFAC</name>
  </public_permissions_ldd_clear>

  <device_security>
      <default_control_panel_login_method>Card
Authentication</default_control_panel_login_method>
  </device_security>

  <configuration_files_ldd>
      <file>\\ip address\shared location\ mobileAuth_config_v0.2.10_premise.ucf</file>
      <file>\\ip address\shared location\ omnikey5427ckdriver_instance.ucf</file>
  </configuration_files_ldd>



  <configuration_data_ldd>
  <configuration>--Put the eSF configuration here--</configuration>
  </configuration_data_ldd>

  <kerberos>
     <kerberos_file>
        <![CDATA[[libdefaults]
  default_realm = SOLUTIONS.LEXMARK.COM
  [realms]
  SOLUTIONS.LEXMARK.COM = {
  kdc = tis-dc1.solutions.lexmark.com
  kdc = tis-dc2.solutions.lexmark.com
  }

  NA.DS.LEXMARK.COM = {
  kdc = USLEXDCT06.na.ds.lexmark.com
  kdc = USLEXDCT05.na.ds.lexmark.com
  }
  ]]>
     </kerberos_file>
     <krb_disable_reverse_ip1 or 0</krb_disable_reverse_ip>
     <kerberos_permissions>
         <name>copy</name>
         <name>email</name>
     </kerberos_permissions>
  </kerberos>

  </auth>
```

Understanding solution settings

Setting type	Location in LMC	Initial configuration	Scope
Global	1 Click the **Solutions** tab. 2 From the Tasks section, select **Configuration**.	After uploading the solution in LMC	All printers in all device groups to which the solution is applied, or all software clients in all software client groups to which the solution is applied

Setting type	Location in LMC	Initial configuration	Scope
Local	1 Click the **Device Groups** or **Software Client Groups** tab. 2 Select a group. 3 From the Tasks section, select **Solutions**.	During deployment to a device group or assignment to a software client group	All printers in the selected device group, or all software clients in the selected software client group

Uploading solutions to the LDD system

1 From LMC, click the **Solutions** tab.

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

3 Click **Install/Upgrade**.

4 Browse to the solution file.

Note: To prevent overwriting existing files, clear **Overwrite if file already exists**.

5 Click **Upload**.

Notes:

- If you are upgrading an existing solution, then we recommend setting all servers offline so that jobs for the solution are not accepted during the upgrade. Servers can be set online again after performing a policy update for the associated device groups. For more information, see "Viewing and changing server status" on page 64.
- If you install a workflow solution that includes a component, then restart the Lexmark Solutions Application Server. For more information, see "Restarting the Lexmark Solutions Application Server" on page 69.
- Remove all solutions from home screens, device groups, and software client groups before removing them from the system. For more information, see "Removing solutions" on page 100.
- Adding a solution to the LDD 4.x System list enables you to upload a solution to the LDD system directly from the Eclipse software. For more information, see the *Lexmark Document Distributor SDK Guide*.

Configuring global solution settings

1 From LMC, click the **Solutions** tab.

2 From the Solutions section, select a solution.

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

4 Configure the settings. For more information, see the documentation that came with the solution.

Note: Make sure that the shortcut number of a profile matches the shortcut number in the Home Screen settings. For more information on customizing the home screen, see "Customizing the home screen for a device group" on page 107.

5 Click **Apply**.

Configuring local settings for a deployed solution

1. From LMC, select a group. Do either of the following:
   - Click the **Device Groups** tab. From the Device Groups section, select a device group.
   - Click the **Software Client Groups** tab. From the Software Client Groups section, select a software client group.
2. From the Tasks section, select **Solutions**.
3. From the main section, select a solution, and then click or **Edit**.
4. Configure the deployment settings of the solution for the device group, and then click **Finish**.
5. Perform a policy update. For more information, see “Updating policies for device groups” on page 112.

Configuring an eSF application associated with a solution

If a hybrid solution is installed and an associated eSF application includes a descriptor file, then you can edit the eSF application settings. This option applies to e-Task 5, e-Task 4, e-Task 3, and e-Task 2+ printers. Each device group contains separate settings for any eSF application.

Note: LDD can manage eSF application settings for e-Task 5, e-Task 4, e-Task 3, and e-Task 2+ printers only. For e-Task 2 and X642 printers, configure the eSF application settings by using the Embedded Web Server on each printer after the application is deployed.

1. From LMC, click the **Device Groups** tab.
2. From the Device Groups section, select a device group.
3. From the Tasks section, select **eSF Configuration**.
4. From the main section, select an eSF application.
5. Select **Verify eSF application deployment and deploy these eSF settings**.
6. From the “Deploy to” section, select an e-Task printer.

   Note: If you are configuring advanced prompt, then select **All** to install the AP Bundle in all printers running the LDD solution.
7. Configure the settings.
8. Click **Save Settings**.
9. Perform a policy update. For more information, see “Updating policies for device groups” on page 112.

Locating solution-related files

Some solutions include properties files or other associated files, which are located in the following:

- Files associated with a single solution only are located in the **\Lexmark\Solutions\apps\wf-ldss\solutions*SolutionName*\WEB-INF** folder where each server is installed. ***SolutionName*** is the name of the solution.
- Files added by a solution to be shared with all solutions are located in the **\Lexmark\Solutions\apps\wf-ldss** folder where each server is installed.

For more information, contact your solution developer.

Restarting the Lexmark Solutions Application Server reverts the solution-related files of the following folders to the default version that is stored with the solution package:

- **\Lexmark\Solutions\apps\wf-ldss**
- **\Lexmark\Solutions\apps\wf-ldss\solutions**

Removing solutions

Removing home screen buttons for a solution

1. From LMC, click the **Device Groups** tab.
2. From the Device Groups section, select a device group where a home screen button is assigned to the solution.
3. From the Tasks section, select **Home Screen**.
4. Click the tab for each device class with a button assigned to the solution, and then do the following:
   a. In the Layout menu, select the number of buttons to include.
   b. If necessary, select a page, and then select a button.
   c. In the Action menu, select **None**.
   d. Click **Apply**.

   Note: If necessary, repeat these steps for other device groups.

Deleting a solution from device groups or software client groups

1. From LMC, click the **Device Groups** tab.
2. From the Device Groups section, select a device group where the solution has been deployed.
3. From the Tasks section, select **Solutions**.
4. Select a solution.
5. Click or **Delete**.

   Note: If necessary, repeat these steps for other device groups.

Removing a solution from the system

1. From LMC, click the **Solutions** tab.
2. From the Solutions section, select **All Solutions**.
3. Select a solution.
4. Click **Remove**.

   If a solution has associated forms, then you are prompted whether to remove the associated forms along with the solution.

   Notes:

   - Forms may be shared among solutions, and removing forms that use any remaining solutions stops those solutions from working correctly.

- Removing a solution removes any associated scheduled tasks automatically.

Managing device groups and devices

Creating and populating device groups

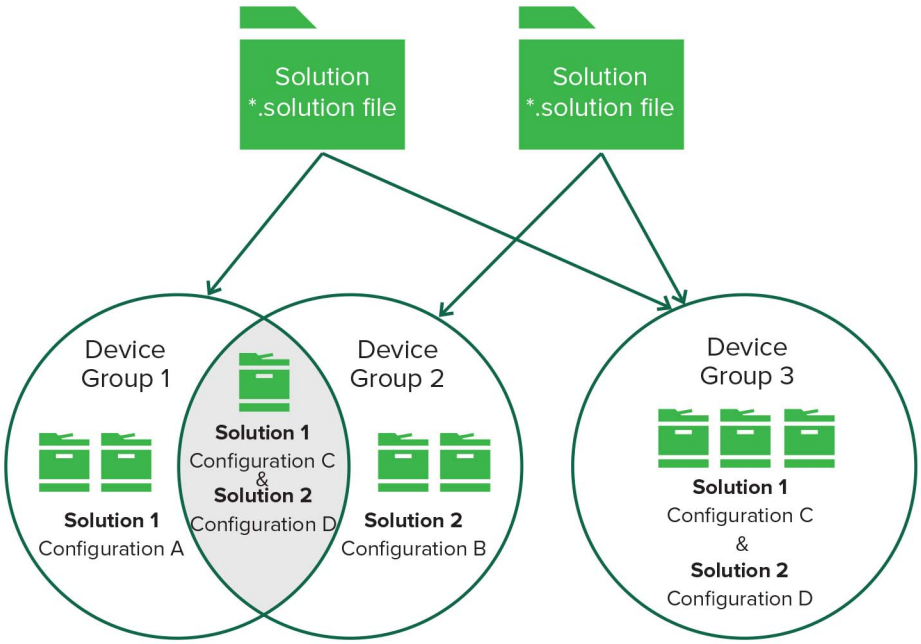
Understanding device groups

A device group is a collection of printers that share one or more deployed solutions with the same local configuration.

To deploy solutions, create at least one device group. Multiple device groups are created when any of the following is applicable:

- More than one solution is deployed to different sets of printers.
- One solution is deployed with different local configurations for different printers.

Printers can be members of more than one device group. Solutions from each device group to which a printer belongs to are deployed to that printer.



Creating a device group

1. From LMC, click the **Device Groups** tab.
2. From the Device Groups section, click + or **Add**.
3. Type a unique name for the device group.
4. Click **Save** or **Add**.

Creating a device group from an existing device group

1. From LMC, click the **Device Groups** tab.
2. From the Device Groups section, click ✚ or **Add**.
3. Type a unique name for the device group, and then select the existing group to copy.
4. Click **Save** or **Add**.

   The following settings are copied from the existing device group to the new device group:
   - Solution associations
   - Solution settings
   - eSF application associations
   - eSF application settings
   - Home screen configurations
   - Fax forwarding configurations
   - Security settings

Configuring policy updates

1. From LMC, click the **Services** tab.
2. From the Services section, select **PolicyUpdate**.
3. From the Tasks section, select **Parameters**.
4. Enter a timeout period in seconds for each device during a policy update.

   Note: If a large eSF application or several eSF applications are included with a hybrid solution, then increase the timeout period for policy updates. This configuration allows sufficient time for policy updates that include the deployment of eSF applications to complete.
5. Select **Overwrite all function overrides on the device**.

   Note: If one or more eSF applications installed on the device can override the device function, then clear **Overwrite all function overrides on the device**.
6. Click **Apply**.

Creating a discovery profile

1. From LMC, click the **Device Groups** tab.
2. From the Device Groups section, select a device group.
3. From the Tasks section, select **Discovery Profiles**.
4. In the Address field, type one of the following:
   - IP address (For example, **`10.10.2.100`**)
   - IP address range (For example, **`10.10.2.1-10.10.2.127`**)
   - Subnet (For example, **`10.10.2.*`**)

- Host name (For example, **printer-host-name**)
- FQDN (For example, **printer-host-name.domain-name**)

Note: Using the asterisk wildcard character (*****) to represent the sections at the end of the IP address returns all devices in that subnet. For example, typing **10.10.*.*** searches for all devices that have been discovered within the range 10.10.0.1–10.10.255.255.

5 If necessary, configure the filters.

6 Click **Add**.

Notes:

- You can also edit or delete profiles.
- To discover profiles in a device group, select a device group, and then click **Discover All**.
- To discover specific device profiles, select a profile, and then click **Discover**.
- To discover multiple device groups, select **All Device Groups**.

Importing a list of printers to a device group

A list of printers can be imported from an XML, TXT, or CSV file exported from Markvision™ or other systems.

1 From LMC, click the **Device Groups** tab.

2 From the Device Groups section, select a device group.

3 From the Tasks section, select **Discovery Profiles**.

4 Click **Import**, and then browse to the file.

Note: To prevent overwriting existing files, clear **Overwrite if file already exists**.

5 Click **Upload**.

The entries in the file are added to the list of discovery profiles. To search for the imported printers, perform a device discovery. For more information, see “Manually discovering printers” on page 105.

In a TXT file, each line contains the host name or IP address for a single printer.

In a CSV file, each line contains the record for a single printer. The lines contain one or more of the following parameters:

- IP address or FQDN
- SNMP read name
- SNMP write name
- Device class
- Device model
- Serial number
- Contact name
- Contact location
- Property tag

In the CSV file, include a comma for a blank field followed by populated fields.

The following is an example of an XML file structure:

```
<?xml version="1.0" encoding="UTF-8" ?>
<filters>
  <filter>
    <addressRange>10.10.2.200</addressRange>
    <snmpRead>public</snmpRead>
    <snmpWrite>public</snmpWrite>
    <contactName>John Doe</contactName>
    <contactLocation>Office 1A</contactLocation>
    <serialNumber>0123456789</serialNumber>
    <propertyTag>XYZ123</propertyTag>
    <deviceClass>All</deviceClass>
  </filter>
  <filter>
    <addressRange>10.10.2.150</addressRange>
    <snmpRead>public</snmpRead>
    <snmpWrite>public</snmpWrite>
    <contactName>Don Joseph</contactName>
    <contactLocation>Office 2B</contactLocation>
    <serialNumber>1234567890</serialNumber>
    <propertyTag>ABC789</propertyTag>
    <deviceClass>All</deviceClass>
  </filter>
</filters>
```

Manually discovering printers

Before deploying a solution to a printer, discover the printer as part of a device group. Printers may be manually discovered or automatically discovered on a schedule. For more information on scheduled discovery, see "Scheduling a discovery task" on page 106.

1. From LMC, click the **Device Groups** tab.
2. If necessary, create a discovery profile. For more information, see "Creating a discovery profile" on page 103.
3. From the Device Groups section, do either of the following:
   - To discover a specific device group, select a device group.
   - To discover multiple device groups, select **All Device Groups**.
4. From the Tasks list, select **Discovery**.

   Notes:

   - If you are discovering printers in a device group where you have previously discovered printers, then select **Discover new devices only**. This setting allows the system to discover profiles faster.
   - If you are discovering printers from multiple device groups, then from the main section, select the device groups.
5. If necessary, configure the SNMP timeout retries period in milliseconds for each retry in the sequence, separating each by a space.

   Note: For more information on adjusting timeout periods for device discovery, see "Configuring NPA device communication" on page 75.
6. Click **Discover**.

   After device discovery, the system reports the number of printers that are discovered. To see the discovered printers, select **Discovered Devices**.

Notes:

- If the discovery process is stopped, then the discovery task may take a few minutes to stop completely.
- After a printer has been discovered, removing the related device group or discovery profile does not remove the printer from the system. For more information on removing printers from the system, see "Removing devices from the system" on page 120.
- After the discovery process, the number of missing devices appears, if applicable. To launch the Missing Devices task, click **Missing Devices Count**. For more information, see "Discovering missing printers" on page 106.
- To export the discovered devices list, click **Export**.

Discovering missing printers

If a printer is offline during a discovery, then it is identified as missing.

1. From LMC, click the **Device Groups** tab.
2. From the Device Groups section, select a device group, or select **All Device Groups** to discover printers in multiple device groups.

   Note: Make sure that discovery profiles exist for device groups to be included in the operation.
3. From the Tasks section, select **Missing Devices**.

   Notes:

   - If you are discovering printers in a device group where you have previously discovered printers, then select **Discover new devices only**. This setting allows the system to discover profiles faster.
   - If you are discovering printers from multiple device groups, then from the main section, select the device groups.
   - To export the missing devices list, click **Export**.
4. If necessary, configure the SNMP timeout retries period in milliseconds for each retry in the sequence, separating each by a space.
5. Click **Discover**.

Viewing all printers with outdated policies

1. From LMC, click the **Device Groups** tab.
2. From the Device Groups section, select **All Device Groups**.
3. From the Tasks section, select **Out of Policy Devices**.

Scheduling a discovery task

1. From LMC, click the **Device Groups** tab.
2. From the Device Groups section, select a device group, or select **All Device Groups** to discover printers in multiple device groups.

   Note: Make sure that discovery profiles exist for device groups to be included in the operation.

3 From the Tasks section, select **Schedule**.

4 Click **Add** > **Discovery**.

5 If necessary, type a description for the task, and then click **Next**.

6 If you are discovering printers from multiple device groups, then from the main section, select the device groups, and then click **Next**.

7 Enter a start date and a start time.

8 Configure the frequency of the scheduled event.

9 Click **Finish**.

Deploying solutions to a device group

1 From LMC, click the **System** tab.

2 From the System section, select **System Status**.

3 Set all servers offline. For more information, see "Viewing and changing server status" on page 64.

Note: Make sure that all jobs are completed before the server goes offline.

4 Click the **Device Groups** tab.

5 From the Device Groups section, select a device group.

6 From the Tasks section, select **Solutions**.

7 From the main section, click ✚ or **Add**.

8 Select a solution from the list, and then click **Next**.

9 Configure the deployment settings of the solution for the device group, and then click **Finish**.

10 Perform a policy update. For more information, see "Updating policies for device groups" on page 112.

Customizing the home screen for a device group

You can configure printers in a device group so that buttons for deployed solutions appear on printer home screens or in the menus of non-touch-screen printers. A custom home screen is not a requirement to deploy a solution.

If the default home screen is used, then to access solutions, do either of the following:

- For e-Task 5 printers, touch **App Profiles**.
- For e-Task 4, e-Task 3, or e-Task 2+ printers, touch **Held Jobs** > **Profiles**.

Different device classes may have different capabilities. Configure a separate custom home screen for each device class.

Actions included in a custom home screen must be set in the printer settings to appear on the home screen.

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

- Locate the IP address on the top of the printer home screen.
- View the IP address in the TCP/IP section of the Network/Ports menu.

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

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

- For e-Task 5 printers, click **Settings** > **Device** > **Visible Home Screen Icons**.
- For e-Task 4, e-Task 3, or e-Task 2+ printers, click **Settings** > **General Settings** > **Home screen customization**.

Note: For a list of supported printers in each device class, see "Supported printers" on page 11.

In printers assigned to more than one device group with a custom home screen, the last policy update determines which home screen is used. If multiple-device-group membership is necessary, then do not configure a home screen for more than one of the device groups to which the printer belongs.

Note: Customizing the device group home screen after customizing the printer home screen overwrites the custom printer home screen during the next policy update.

1 From LMC, click the **Device Groups** tab.

2 From the Device Groups section, select a device group.

3 From the Tasks section, select **Home Screen**.

4 Click the tab for each device class that you want to customize.

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

6 Configure the settings.

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

  Notes:

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

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

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

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

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

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

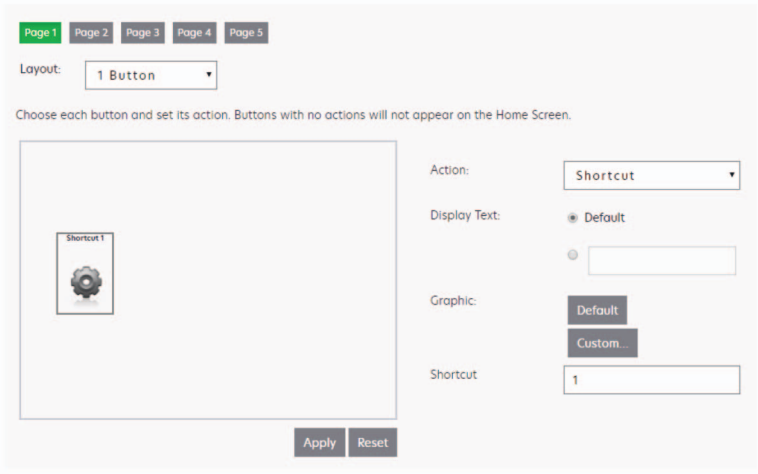
[1] Some selections may not be available in some models.

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

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

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

– If you selected **Shortcut**, then enter the number of the shortcut.

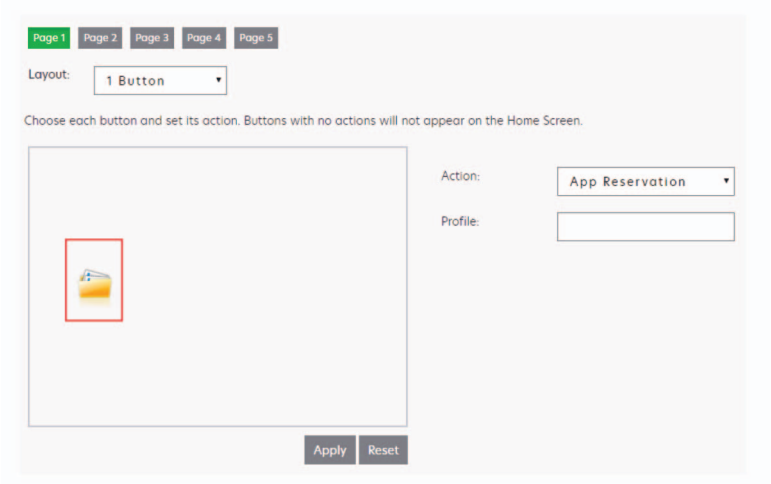


Notes:

- Shortcuts added in LMC are device-class shortcuts, and not eSF-application-specific shortcuts.
- When updating the shortcut number of a profile, make sure to match it with the shortcut number in the Home Screen settings.

– If you selected **Single Profile** or if you are overriding a standard function with a profile, then select a profile.

- If you selected **App Reservation**, then type the profile name of the eSF application that uses the button.



e If necessary, type a custom text.

Note: You cannot set a custom text for Placeholder or App Reservation.

f The graphic that appears on the button is the default graphic of the action. If you want to select a custom graphic for any action except Placeholder or App Reservation, then do the following:

1. Click **Custom**.
2. Click **Change**, and then browse to a JPEG, GIF, or PNG file for the Up and Down icons.
3. Click **Upload** > **Apply**.

Note: If you want to revert to the default graphic, then click **Default**.

The images that you selected are resized automatically to the following dimensions for each device class. For best results, resize or crop source images to the correct size before uploading.

- **e-Task 5**—140 x 140 pixels
- **e-Task 4**—172 x 254 pixels
- **e-Task 3**—172 x 254 pixels
- **e-Task 2+, e-Task 2, and SFP e-Task 2+**—120 x 75 pixels
- **e-Task**—120 x 80 pixels
- **X642**—120 x 55 pixels

Note: For a list of supported printers in each device class, see “Supported printers” on page 11.

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

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

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

Notes:

- The only action available is Single Profile. You cannot modify other menu items on a printer without a touch screen.
- To remove a button, select it in the list, and then click **Remove**.

c If necessary, type a custom text.

d Select a profile to associate with the button.

7 Configure the remaining buttons on the home screen.

8 Click **Apply**.

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

Updating policies for device groups

To apply the changes to the printers after configuring and deploying solutions, perform a policy update.

Notes:

- To avoid affecting system performance, schedule policy updates during off-peak hours.
- To monitor all changes, schedule policy updates after the system is set up. For more information, see "Scheduling policy updates" on page 113.
- If a large eSF application or several eSF applications are included with a hybrid solution, then increase the timeout period for policy updates. This configuration allows sufficient time for policy updates that include the deployment of eSF applications to complete.

Policy updates that include the deployment of eSF applications to e-Task 2 printers are the following:

- Deployment of the AP Bundle when updating policies for the first time
- First deployment of eSF applications that are associated with hybrid solutions
- Any policy updates that occur immediately after updating the AP Bundle or other eSF applications

  Note: If the validation occurs during deployment of eSF applications, then policy updates that include deployments of eSF applications take longer to complete. If you do not want to validate the deployment of eSF applications on each printer, then see "Disabling the validation of eSF application deployment" on page 114.

1 From LMC, click the **Device Groups** tab.

2 From the Device Groups section, select a device group, or select **All Device Groups** to update policies for printers in multiple device groups.

3 From the Tasks section, select **Policy Update**.

Note: The Policy Update task can also be accessed from the Policy Update link in the reminder shown when working with the Solutions and Home Screen tasks.

4 Select the update method. Do either of the following:

- To update only out-of-policy printers in the device group, select **Only update those devices which are Out of Policy**.
- To update all printers in the device group, clear **Only update those devices which are Out of Policy**.

Note: If you are updating policies for printers from multiple device groups, then from the main section, select the device groups.

5 Click **Update Policy**.

Note: After updating policies, the number of devices that failed to update appears, if applicable. To view the error logs, click **Failed Devices Count**. To view the full set of logs, clear the message filter.

Scheduling policy updates

In a scheduled policy update, all printers in the device group are updated.

Notes:

- To avoid affecting system performance, schedule policy updates during off-peak hours.
- To monitor all changes, schedule policy updates after the system is set up.
- If a large eSF application or several eSF applications are included with a hybrid solution, then increase the timeout period for policy updates. This configuration allows sufficient time for policy updates that include the deployment of eSF application to complete.
- If you do not want to validate the deployment of eSF applications on each printer, then see "Disabling the validation of eSF application deployment" on page 114.

1. From LMC, click the **Device Groups** tab.
2. From the Device Groups section, select a device group, or select **All Device Groups** to update policies for printers in multiple device groups.
3. From the Tasks section, select **Schedule**.
4. Click **Add** > **Policy Update**.
5. Type a description for the task, and then click **Next**.

   Note: If you are updating policies for printers from multiple device groups, then from the main section, select the device groups.
6. Enter a start date and a start time.
7. Configure the frequency of the scheduled event.
8. Click **Finish**.

Enabling secure communication between servers and printers in a device group

Note: Secure communication between printers and servers is required when using a solution with Kerberos authentication.

1. From LMC, click the **Device Groups** tab.
2. From the Device Groups section, select a device group.
3. From the Tasks section, select **Security**.
4. Enable secure communication. Do either of the following:
   - To secure the session completely, select **Enabled for Session**.
   - To secure only the credentials such as user name and password of the session, select **Enabled for Credentials**.

     Note: This configuration is faster than a communication that is set to "Enabled for Session."
5. Click **Apply**.

Disabling the validation of eSF application deployment

1. From LMC, click the **Device Groups** tab.
2. From the Device Groups section, select a device group.
3. From the Tasks section, select **eSF Configuration**.
4. From the main section, select an eSF application, and then clear **Verify eSF application deployment and deploy these eSF settings**.
5. Click **Save Settings**.

   Note: If necessary, repeat these steps for other device groups.

Configuring the print queue

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

1. From your computer, run the UPD administrator installer.

   Note: Download UPD from **http://lexmark.com**.
2. When prompted for the installation type, select **Extract**, and then clear **Start the installation software**.
3. Browse to the location of the extracted UPD files.

   Note: We recommend extracting files to the root of the C:\ drive or a directory off the C:\ drive.
4. Click **Add a printer using TCP/IP address or host name**, and then click **Next**.
5. Enter the following information:
   a. **Device type**—Select the device type.
   b. **Hostname or IP address**—Type the client IP address or host name.
   c. **Port name**—Type the name of the port.

      Note: Query the printer and automatically select the driver to use is selected by default.
6. From the **Device type** menu, click **Standard**, and then select **Generic Network Card**.
7. Click **Next**.
8. When prompted to select a printer, select **Have Disk**, and then browse to the ***<extract_path>*** **\InstallationPackage\Drivers\Print\GDI** folder, where ***<extract_path>*** is the location of the extracted UPD files.

   Note: We recommend extracting files to the root of the C:\ drive or a directory off the C:\ drive.
9. Run any of the .inf files.
10. Type a descriptive printer name, and click **Next**.
11. Right-click the new print queue, and then select **Printer properties**.
12. Accept the certificate.
13. From the Printer properties window, click **Encryption** tab.
14. Select **Always encrypt**, to encrypt print jobs.

15 Click **Apply**.

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

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

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

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

19 Run any of the .inf files.

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

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

22 Click **OK**.

Configuring the Devices tab

The Devices tab is generally used for specialized maintenance and troubleshooting.

Searching for devices

1 From LMC, click the **Devices** tab.

2 From the Search section, select a search criterion from the menu.

3 Enter a value that corresponds to the search criterion.

Note: Using the asterisk wildcard character (*****) to represent the sections at the end of the IP address returns all devices in that subnet. For example, typing **`10.10.*.*`** searches for all devices that have been discovered within the range 10.10.0.1–10.10.255.255.

4 Click or **Search**.

Customizing the home screen on specific devices

Accessing the home screen configuration for specific devices is helpful for the following tasks:

- Troubleshooting home screen issues on specific devices
- Customizing home screens on specific devices for which custom home screens are not configured within a device group
- Customizing home screens that include non-LDD profiles
- Removing unused buttons from the home screen

1 From LMC, click the **Devices** tab.

2 Search for printers. For more information, see “Searching for devices” on page 115.

3 From the Devices section, select one or more device names.

4 From the Tasks section, select **Home Screen**.

5 Click **Edit**, and then configure the settings.

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

  Notes:

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

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

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

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

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

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

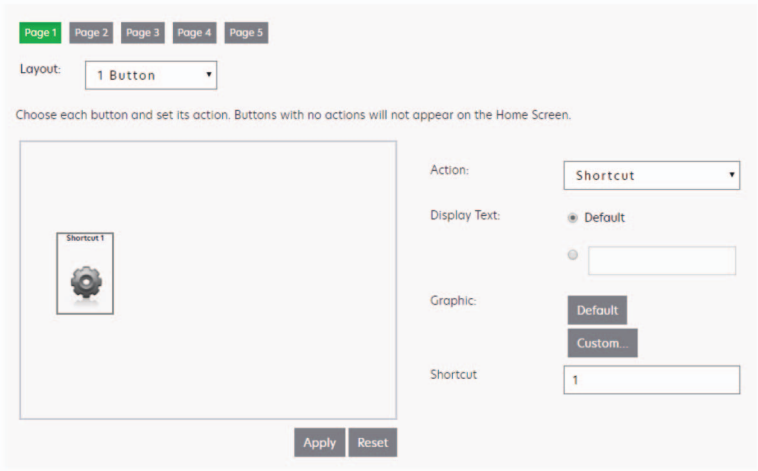
[1] Some selections may not be available in some models.

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

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

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

– If you selected **Shortcut**, then enter the number of the shortcut.

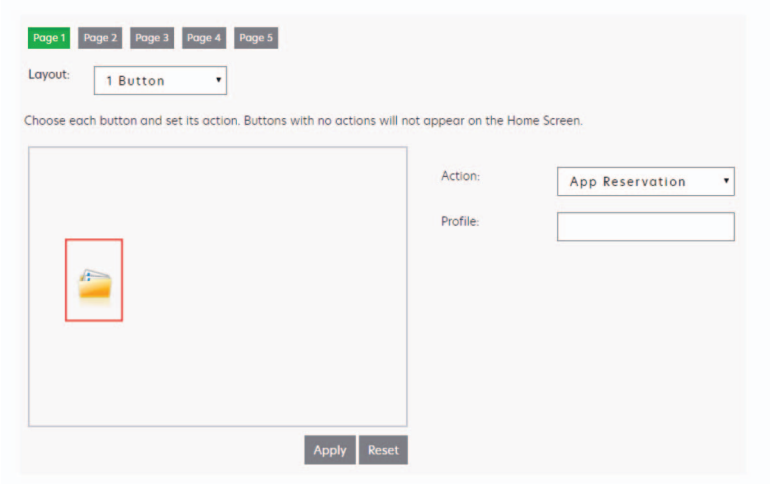


Notes:

- Shortcuts added in LMC are device-class shortcuts, and not eSF-application-specific shortcuts.
- When updating the shortcut number of a profile, make sure to match it with the shortcut number in the Home Screen settings.

– If you selected **Single Profile** or if you are overriding a standard function with a profile, then select a profile.

- If you selected **App Reservation**, then type the profile name of the eSF application that uses the button.



e If necessary, type a custom text.

Note: You cannot set a custom text for Placeholder or App Reservation.

f The graphic that appears on the button is the default graphic of the action. If you want to select a custom graphic for any action except Placeholder or App Reservation, then do the following:

1. Click **Custom**.
2. Click **Change**, and then browse to a JPEG, GIF, or PNG file for the Up and Down icons.
3. Click **Upload** > **Apply**.

Note: If you want to revert to the default graphic, then click **Default**.

The images that you selected are resized automatically to the following dimensions for each device class. For best results, resize or crop source images to the correct size before uploading.

- **e-Task 5**—140 x 140 pixels
- **e-Task 4**—172 x 254 pixels
- **e-Task 3**—172 x 254 pixels
- **e-Task 2+, e-Task 2, and SFP e-Task 2+**—120 x 75 pixels
- **e-Task**—120 x 80 pixels
- **X642**—120 x 55 pixels

Note: For a list of supported printers in each device class, see “Supported printers” on page 11.

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

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

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

Notes:

- The only action available is Single Profile. You cannot modify other menu items on a printer without a touch screen.
- To remove a button, select it in the list, and then click **Remove**.

c If necessary, type a custom text.

d Select a profile to associate with the button.

6 Configure the remaining buttons on the home screen.

7 Click **Apply**.

Notes:

- If multiple devices are selected, click **Next**, and then configure the settings of each home screen. Make sure to click **Apply** on each tab to apply the settings.
- Customizing the device group home screen after customizing the printer home screen overwrites the custom printer home screen during the next policy update.

Viewing device profiles

1 From LMC, click the **Devices** tab.

2 Search for printers. For more information, see “Searching for devices” on page 115.

3 From the Devices section, select one or more devices.

4 From the Tasks section, select **Profiles**, and then from the main section, select a profile name.

Note: If necessary, repeat these steps for other device groups.

Updating device policies

1 From LMC, click the **Devices** tab.

2 Search for printers. For more information, see “Searching for devices” on page 115.

3 From the Devices section, select one or more devices.

4 From the Tasks section, select **Policy Update**.

5 Click **Update Policy**.

Note: After updating policies, the Policy Update status shows the number of devices that failed to update. To view the error logs, click **Failed Devices Count**. To view the full set of logs, clear the Message filter.

Removing devices from the system

1 From LMC, click the **Devices** tab.

2 Search for printers. For more information, see “Searching for devices” on page 115.

3 From the Devices section, select one or more devices.

4 Click or **Remove from System** > **Yes**.

Removing a device from the system does not do the following:

- Remove profiles that are deployed to the device.
- Reset home screen modifications.
- Remove eSF applications that are installed with a solution.

To remove a device completely, remove it from the discovery profile.

Managing software clients

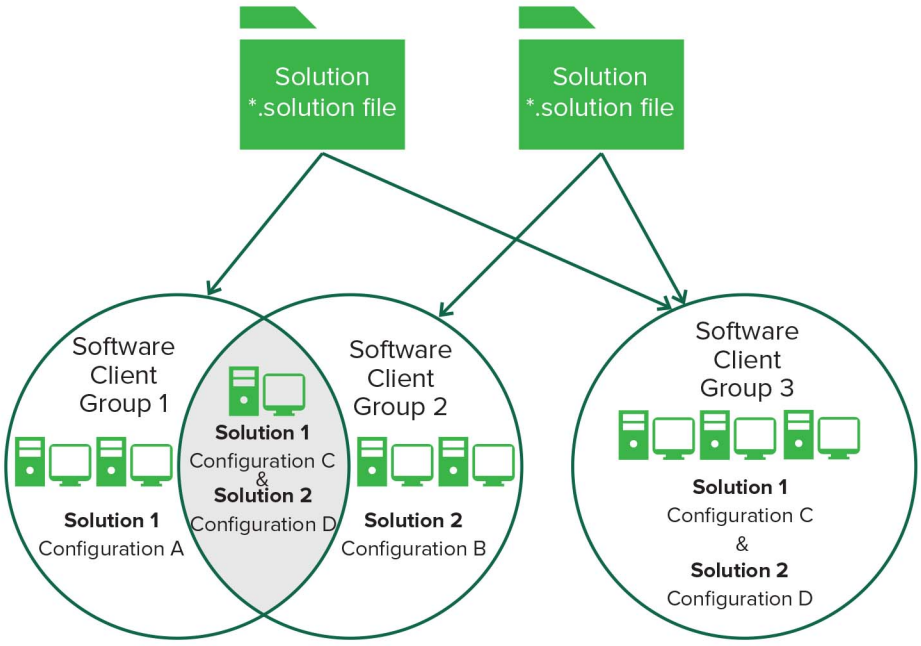
Understanding software clients and software client groups

A software client is a computer that is configured to use either of the following client software to access solutions directly:

- Microsoft Windows application software Select'N'Send
- Lexmark Document Server Printer Port

A software client group is a collection of these software clients that share one or more solutions with the same local configuration. At least one software client group must be created for solutions used with Microsoft Windows application software Select'N'Send or Lexmark Document Server Printer Port. If more than one solution is assigned to different sets of software clients, then create multiple software client groups. If one solution is assigned to different software clients with different local configurations, then create multiple software client groups as well.

Software clients can be members of more than one software client group. Solutions from each software client group to which a software client belongs is available to that software client.



Software client groups are similar to device groups, but have the following differences:

- Only solutions developed specifically for use with software clients may be made available to software clients.
- Software clients are not discovered. Adding a software client to a software client group simply enables access to the solutions in that group when the software client accesses the system.
- Policy updates are not used with software clients.
- Lexmark Document Server Printer Port supports dynamic prompting.
- The Solution Status Page cannot be associated with a software client group.

Note: Separate client licenses are required for using software clients in LDD. For more information on adding licenses to an existing system, see “Adding licenses to an existing server” on page 78.

Understanding dynamic prompting support

Many solutions involve submitting jobs that require information such as account numbers, passwords, or processing options. When a profile is selected, solutions may either prompt you for information or start a job automatically.

The Job Submission Web Service provides prompting capability to Lexmark Document Server Printer Port clients. The following prompts are supported:

- **`MessagePrompt`**
- **`BooleanPrompt`**
- **`IntegerPrompt`**
- **`ListPrompt`**
- **`ArrayPrompt`**
- **`PasswordPrompt`**
- **`ScanPrompt`**
- **`MessagePrompt`**
- **`EndPrompt`**

The timeout period for the prompt wizard is 30 seconds.

Prompting depends on whether there are more required information or documents to process. If there are more, then select whether to continue or not. On the last prompt, a summary dialog box of the answers appears.

Notes:

- Canceling the job does not undo the processing of the job.
- LDD 4.6.3.x printer ports on a clustered print server are not supported.

Software client setup overview

Preparing software clients for use with LDD solutions requires a slightly different process than the setup and solution deployment for printers.

After installing other LDD system components, do the following:

1. Upload a solution to LDD. For more information, see “Uploading solutions to the LDD system” on page 98.
2. If necessary, install client software licenses on the LDD system. For more information, see “Adding licenses to an existing server” on page 78.
3. Create a software client group to contain software clients to which a particular solution must be available. For more information, see “Creating a software client group” on page 123.
4. Add IP addresses to the software client group for the computers where you want to install the client software and solution.

5 Add the solution to the new software client group.

Note: Only solutions developed for use with client software (instead of, or in addition to, printers) may be made available to software client groups.

6 Install the client software on each of the client computers. For more information, see “Installing client software” on page 125.

Note: To install the client software successfully, set servers online.

7 Run Windows Update.

8 When using Lexmark Document Server Printer Ports, add print queues that are assigned to the appropriate client software on each client computer or print server.

Note: LDD printer port prompting is not supported on print servers. If it is configured on a print server, then the spooler stops responding and may crash when print jobs start going into the print server. Prompting profiles must be used only on client computers.

9 Test all print queues that use Lexmark Document Server Printer Ports. For more information, see “Printing documents by using LDD print queues” on page 130.

10 Use test jobs to complete the setup of the Microsoft Windows application software Select'N'Send from each client. For more information, see “Configuring the GUI of the Microsoft Windows application software Select'N'Send” on page 131.

Creating and populating software client groups

Creating a software client group

1 From LMC, click the **Software Client Groups** tab.

2 From the Software Client Groups section, click ✚ or **Add**.

3 Type a unique name for the software client group.

4 Click **Save** or **Add**.

Adding software clients to a software client group

1 From LMC, click the **Software Client Groups** tab.

2 From the Software Client Groups section, select a software client group.

3 From the Tasks section, select **Client Profiles**.

4 In the Address field, type one of the following:

- IP address (For example, **`10.10.2.100`**)
- IP address range (For example, **`10.10.2.1-10.10.2.127`**)
- Subnet (For example, **`10.10.2.*`**)
- FQDN (For example, **`client-hostname.domain-name`**)

Note: Using the asterisk wildcard character (*****) to represent the sections at the end of the IP address returns all devices in that subnet. For example, typing **`10.10.*.*`** searches for all devices that have been discovered within the range 10.10.0.1–10.10.255.255.

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

When adding a software client on an MSCS, add the following information:

- IP address of the logical host
- IP addresses of all the physical nodes in the cluster

For more information, see "Installing client software on a Microsoft Cluster Server" on page 126.

Note: Software client groups manage software clients by IP address and do not require discovery.

Importing software clients to a software client group

Software clients can be imported from an XML, TXT, or CSV file.

1 Click the **Software Client Groups** tab.

2 From the Software Client Groups section, select a software client group.

3 From the Tasks section, select **Client Profiles**.

4 Click **Import**, and then browse to the file.

Note: To prevent overwriting existing files, clear **Overwrite if file already exists**.

5 Click **Upload**.

The entries in the file are added to the list of software clients.

In a CSV and TXT file, each line must contain a single IP address of a software client. The following is an example of an XML file structure:

```
<?xml version="1.0" encoding="UTF-8" ?>
<filters>
  <filter>
    <address>10.10.2.200</address>
  </filter>
  <filter>
    <address>10.10.2.150</address>
  </filter>
</filters>
```

Assigning solutions to a software client group

Assigning a solution to a software client group allows the software clients in the group access to the solution on the server.

1 From LMC, click the **Software Client Groups** tab.

2 From the Software Client Groups section, select a software client group.

3 From the Tasks section, select **Solutions**.

4 From the main section, click ✚ or **Add**.

5 Select a solution, and then click **Next**.

6 Configure the local settings of the solution for the current software client group.

7 Click **Finish**.

Installing client software

On a client computer or print server, do the following:

1 From the LDD installation package, run **Setup.exe**.

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

3 From the LDD Setup window, click **Next**.

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

5 Accept the license agreement, and then click **Next**.

6 From the list of components, select **Client Software**.

Note: Do not install the Microsoft Windows application software Select'N'Send on a print server.

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

8 Review the setup information, and then click **Next**.

9 Click **Install**.

Installing client software with secure print support

On a client computer or print server, do the following:

1 From the LDD installation package, run **Setup.exe**.

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

3 From the LDD Setup window, click **Next**.

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

5 Accept the license agreement, and then click **Next**.

6 From the list of components, select **Client Software**, and click **Next**.

Note: Do not install the Microsoft Windows application software Select'N'Send on a print server.

7 From the Device Support Update window, click **Next**.

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

9 From the Select Client Software window, select **Client Software with Secure Print Support**.

10 In the Loadbalancer IP/Hostname field, type the IP address or the host name of the server.

11 From the Profile Name menu, select the client profile.

Notes:

- The Profile Name menu lists all the fetched client software profiles.
- If no client software profiles are fetched, then type the name of the profile. In this scenario, the default name is PrintSubmit.

12 From the Secured Print Settings section, do the following:
   a Select **Enable Secured Print Support**.
   b Select **Allow Unencrypted print job submission**.
13 Review the setup information, and then click **Next**.
14 Click **Install**.
15 Click **Finish**.

Note: For more information on configuring the print queue, see "Configuring the print queue" on page 114.

Installing client software on a Microsoft Cluster Server

1 Set any print spooler resource offline.
2 Install the Lexmark Document Server Printer Port only on each physical node in the cluster.
3 Run Windows Update on each node.
4 If necessary, configure the print spooler resource and the LDD Client Service for the cluster.

   Note: To enable the failover to initiate simultaneously, make sure that the print spooler resource and the LDD Client Service are in the same cluster resource pool.
5 Create print queues on the cluster, and then set **Lexmark Document Server Port - Enterprise** as the port.

   Notes:

   - For more information on creating print queues, see "Configuring a Lexmark Document Server port" on page 128.
   - For more information on the latest LDD port monitor support, see the *Readme* file.

Configuring client software ports

1 From your computer, navigate to the **clientsoftware** installation folder, and then make sure that the **clientsoftware.properties** file is added.
2 Open the **clientsoftware.properties** file.
3 Configure the LB ports and secure mode.

Adding LDD printers on a client workstation or print server

After installing the client software, do the following:

- Create a separate Lexmark Document Server Printer Port for each profile that you want to use on an LDD server.
- Create a print queue that is assigned to that port.

1. Install the print driver for the Lexmark Document Server Printer Port.

   Note: If you do not have a specific print driver, then use the PCL® or PostScript Lexmark Universal Print Driver that is appropriate for your operating system. You can download it at **support.lexmark.com**.

2. From LMC, click the **System** tab.
3. From the System section, select **System Status**.
4. Set at least one server online. For more information, see "Viewing and changing server status" on page 64.
5. From the Windows "Devices and Printers" control panel, add a printer. For more information on adding a printer, see "Configuring a Lexmark Document Server port" on page 128.
6. When prompted, select a local printer, and do not allow Windows to search for plug-and-play printers.
7. When prompted to select a printer port, create a port of Lexmark Document Server Port - Enterprise type.
8. Type a unique name for the port, and then click **Next**. The port name must be 75 characters or fewer.
9. Select a document server.

   If the client software is newly installed, then the list is empty.

   To add a server, do the following:

   a. Click **Manage List**.
   b. From the Server Setup window, click **Add**.
   c. Type the IP address or FQDN of the load balancer, and then click **OK**.
   d. Exit the Server Setup window, and then select the new server from the list.

10. Click **Next**.
11. Select a profile on the server to use with the new port, and then click **Next**.

    Notes:

    - LDD printer port prompting is not supported on print servers. If it is configured on a print server, then the spooler stops responding and may crash when print jobs start going into the print server. Prompting profiles must be used only on client computers.
    - Only profiles associated with solutions that are created for software clients are available.
    - Profiles used with the Lexmark Document Server port must have a name with 14 characters or fewer. For more information on setting the name of a profile, see the *Lexmark Document Distributor SDK Guide*.
    - If the server is running multiple jobs, then profiles on the server may not appear in the list. Wait until the server is not busy, and then try adding the port again.

12. Click **Finish**.
13. Select an existing print driver, and then click **Next**. For more information, see the documentation that came with the printer or print driver.
14. When prompted to keep the existing driver, select **Keep existing driver (recommended)**, and then click **Next**.
15. Type a unique printer name that describes the profile used with the new printer.

    If necessary, select whether to use the new print queue as the default, and then click **Next**.

16 Select whether to share the new print queue. If you are installing the print queue on a server, then select **Share name**.

17 Type a unique name for the print queue on the network, and then click **Next**.

18 To skip printing a test page, select **No**.

19 Confirm the settings, and then click **Finish**.

20 From the Windows "Devices and Printers" control panel, right-click the new printer, and then click **Properties**.

21 Click the **Advanced** tab.

22 Select **Spool print documents so program finishes printing faster** and **Start printing after last page is spooled**.

Note: These settings are required to report an accurate page count to the LDD system. If a large job needs significant time to spool, then smaller jobs can still be completed.

23 Click **OK**.

Configuring a Lexmark Document Server port

Note: Make sure to log in as an administrator.

1 From your computer, in the Windows "Devices and Printers" control panel, right-click the printer, and then click **Properties**.

Note: If the printer that you want to configure is not listed, then add it.

2 Click the **Ports** tab, and then click **Change Port Settings**.

3 Configure a Lexmark Document Server port.

4 Click **Finish**.

Increasing LDD print queue availability

Printer pooling provides a single print queue to several users and can prevent backups when large jobs are submitted.

1 From your computer, in the Windows "Devices and Printers" control panel, right-click the printer, and then click **Properties**.

2 Click the **Ports** tab, and then click **Change Port Settings**.

3 Select **Enable printer pooling**, and then add a Lexmark Document Server port.

4 Select the Lexmark Document Server port that is created for the selected printer, and then click **Next**.

5 Select the profile used for the port that is created for the selected printer, and then click **Next**.

Notes:

- LDD printer port prompting is not supported on print servers. If it is configured on a print server, then the spooler stops responding and may crash when print jobs start going into the print server. Prompting profiles must be used only on client computers.

- If the server is running multiple jobs, then profiles on the server may not appear in the list. Wait until the server is not busy, and then try adding the port again.

6 Follow the instructions on the screen.

Note: You can add more Lexmark Document Server ports, and then add them to the same profile.

7 Click **Finish**.

Testing and using Lexmark Document Distributor solutions

Launching a solution from a printer

After a solution is deployed to a printer, a profile is available on the home screen that lets users access the solution. To launch it, touch the icon for the profile.

If the profile does not appear on the home screen, then do the following:

1. From the printer home screen, do either of the following:
   - For e-Task 5 printers, touch **App Profiles**.
   - For e-Task 4, e-Task 3, or e-Task 2+ printers, touch **Held Jobs** > **Profiles**.
2. Touch the profile.

   The profile launches the associated script on the server. Documents are scanned, and any prompts that are included in the script are presented to the user.

Note: When using a solution that reads a bar code, set the resolution at 300 dpi, and other quality settings at the highest value. For more information, see the documentation that came with your printer or print driver.

Printing documents by using LDD print queues

1. From your computer, open a document, and then click **File** > **Print**.
2. Select the printer that is associated with the Lexmark Document Server port and the profile that you want to use.
3. If necessary, configure the print settings.

   Note: When using a solution that reads a bar code, set the resolution at 300 dpi, and other quality settings at the highest value. For more information, see the documentation that came with your printer or print driver.
4. Close any printer software dialog boxes.
5. Click **OK** or **Print**.

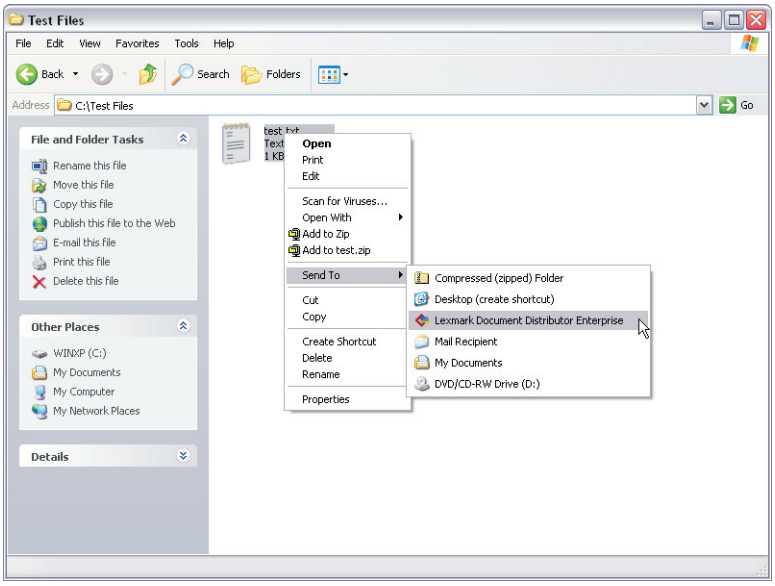
   The document is sent to the LDD system using the profile specified in the Lexmark Document Server port that is associated with the printer. The output of the print driver determines the file type, and each solution script determines the accepted file types.

Configuring the Microsoft Windows application software Select'N'Send

Configuring the GUI of the Microsoft Windows application software Select'N'Send

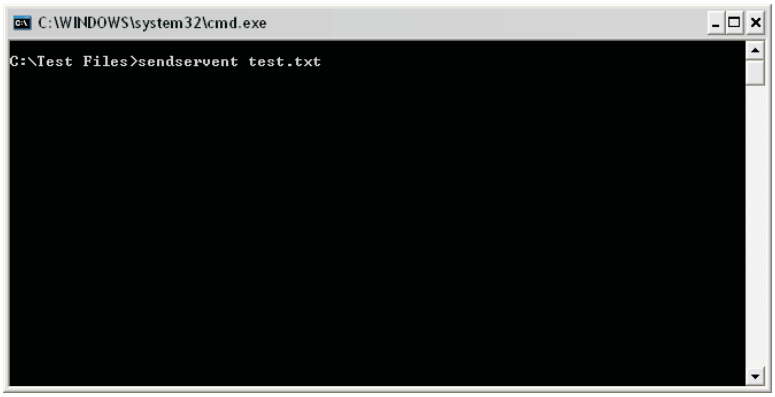
The GUI version of the Microsoft Windows application software Select'N'Send lets users access a selection of LDD profiles. It also submits various documents and document types to the LDD system. Selected files are submitted to the system in their current formats. Each solution script determines the accepted file types. For more information, contact your solution developer.

1. From your computer, launch the GUI of the Microsoft Windows application software Select'N'Send. Do one of the following:
   - Right-click the file that you want to submit to LDD, and then click **Send To** > **Lexmark Document Distributor Enterprise**.

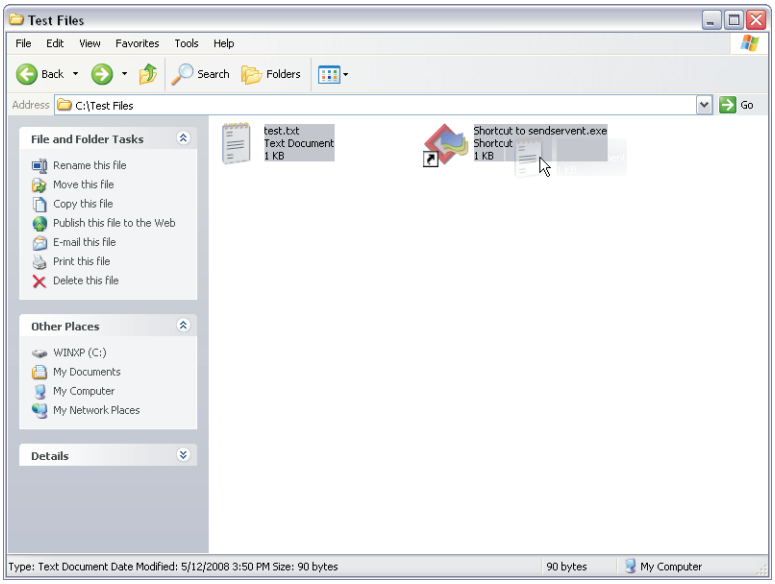


   - From the command line, type **`sendservent filename`**, where ***`filename`*** is the file that you want to submit to LDD, and then press **Enter**. For more information, see "Running the Microsoft Windows application software Select'N'Send from the command line" on page 133.

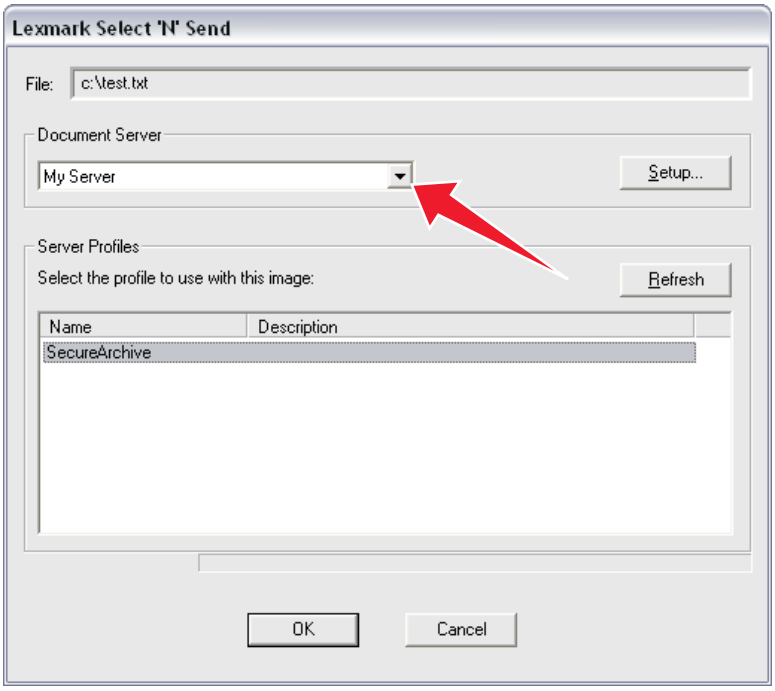
     Note: The program folder of the Microsoft Windows application software Select'N'Send is added to the system path during installation. This configuration enables the software to be accessed from any folder at the command line.



- Drag the file that you want to submit to LDD onto the sendservent.exe file or to a shortcut pointing to that file.



2 From the Lexmark Select'N'Send window, select a document server.



If the client software is newly installed, then the list is empty.

To add a server, do the following:

a Click **Setup**.

b From the Server Setup window, click **Add**.

c Type the IP address or FQDN of the server, and then click **OK**.

d Exit the Server Setup window, and then select the new server from the list.

3 Click **Next**.

4 From the Server Profiles list, select a profile.

5 Click **OK**.

Running the Microsoft Windows application software Select'N'Send from the command line

The command-line version of the Microsoft Windows application software Select'N'Send is useful for the following:

- Automated processes
- Accessing LDD profiles from other software, such as Windows Small Business Server operating systems
- Creating batch files that help users submit specific files by using specific profiles

To run the command-line version of the Microsoft Windows application software Select'N'Send, type the following command:

sendservent -s *server* -p *profile* -f *filename* [-u *userdatafile* -t *timeout* -i *interval*]

where:

- ***server*** is the IP address or FQDN of the load balancer.
- ***profile*** is the profile to run on the LDD server.
- ***filename*** is the name of the file to be submitted to the LDD system.

  Note: The specified file is submitted to the system in its current format. Each solution script determines the accepted file types. For more information, contact your solution developer.
- ***userdatafile*** is the name of the file containing user information for the job.

  Note: If a user data file is not specified or if expected data is missing from a specified file, then a script that expects user data fails.
- ***timeout*** is the time in seconds the LDD system waits for confirmation before aborting the operation with an error. The default value is **0**, which specifies no timeout. This setting is optional.
- ***interval*** is the time in seconds the LDD system waits between each instance of polling for confirmation. The default value is **0.5**. This setting is optional.

Note: Any option that contains a space must be enclosed in double quotation marks (**"**).

Installing the Lexmark Job Router Service

Lexmark Job Router Service is a Windows service that submits print jobs to the Lexmark Print Management (LPM) database directly. The service uses standard TCP/IP ports on port number 9100.

1. From the computer, run the CD, and then navigate to the **\tools\LxkJobRouter** folder.
2. Run the **JobRouterSetup.exe** file, and then click **Next**.
3. Type the LPM site ID.
4. In the Database IP field, type the IP address of the LPM database.
5. Select the database type.
6. Type the location where print jobs are saved.

   Note: This setting must be the same as the LPM location configuration.
7. If the location is a shared network folder, then type your credentials.
8. If the LPM database is Microsoft SQL Server, then click **Next**, and then configure the database settings.
9. Click **Finish**.
10. Create a TCP/IP print port for port number 9100 and the IP address of the computer where Lexmark Job Router Service is running.
11. Create a print queue using port number 9100.

Limitations

- The Lexmark Job Router Service extracts metadata by parsing the PRN file from the print queue and shows only the data in the PRN file.
- The service shows the client login user ID as the owner of the print job depending on the following:
  - The client-side rendering is on the print driver.
  - The workstation login user ID and the print server login user ID are different.

- In a multiple-domain environment, the service does not show the domain name as part of the user name.
- The service may show a different page size name for a print job.

Note: If the service is running on a machine that is not in the LDD or LPM server, then it is configured with a **\\IP\lexmark\printrelease** network path. When submitting print jobs to the LPM table, the service writes the network path in the PR_JOBS table. If an error occurs, then in the LPM configuration, enter the network credentials for the "Directory for print jobs" setting.

Installing the Lexmark Job Router Service silently

Lexmark Keep Job Router Service can also be installed silently.

1. Navigate to **<LDD Installation directory>\install\Silent_Install_Script_Examples**.
2. Run the command prompt as an administrator.
3. Run the **Install_JobRouter.bat** batch file.

   Note: For help information, at the command prompt, type **Install_JobRouter.bat /?**.

Installing the Lexmark Job Router Service for secure print

Lexmark Job Router Service is a Windows service that submits print jobs to the Lexmark Print Management (LPM) database directly. The service uses standard TCP/IP ports on port number 9100.

1. From the computer, run the CD, and then navigate to the **\tools\LxkJobRouter** folder.
2. Run the **JobRouterSetup.exe** file, and then click **Next**.
3. Type the LPM site ID.
4. In the Database IP field, type the IP address of the LPM database.
5. Select the database type.
6. From the Secured Print Settings section, do the following:
   a. Select **Enable Secured Print Support**.
   b. Select **Allow Unencrypted print job submission**.
   c. If the database is different for LDD and LPM, then select **Different DB for LDD and LPM**.

      Note: If the database is different for LDD and LPM, then LoadBalancer IP Address is also required.
7. Type the location where print jobs are saved.

   Note: This setting must be the same as the LPM location configuration.
8. If the location is a shared network folder, then type your credentials.
9. If the LPM database is Microsoft SQL Server, then click **Next**, and then configure the database settings.
10. Click **Finish**.

Note: For more information on configuring the print queue, see “Configuring the print queue” on page 114.

Viewing logs

Viewing the installation logs

1. From the computer where LDD is installed, open the Windows Run dialog box, and then type **"%ALLUSERSPROFILE%\Lexmark\LDD4x"**.
2. Using a text editor, open the installation logs.

Viewing the server logs

In LDD 4.9.1, log data is recorded in the cdcl_wrapper.log file in the **Lexmark\Solutions\tomcat\logs** folder. This log file contains device communication data for all device discoveries and policy deployments to e-Task 5 printers. For a list of supported printers in each device class, see "Supported printers" on page 11.

To change the logging level of the cdcl_wrapper.log to **"debug"**, do the following:

1. Using a text editor, open the **Lexmark\Solutions\apps\cdcl-rest-wrapper\WEB-INF\classes\log4j.properties** file.
2. Change **log4j.rootLogger=WARN,perflog** to **log4j.rootLogger=DEBUG,perflog**.
3. Save and close the file.
4. From the Windows Services control panel on the server computer, restart the Lexmark Solutions Application Server. For more information, see "Restarting the Lexmark Solutions Application Server" on page 69.

All server activity at the selected message priority is recorded in the lsas.log file in the **Lexmark\Solutions\tomcat\logs** folder where the server is installed. To view the logs, using a text editor, open the file.

The default message priority for recording is **"warn"**. When troubleshooting a problem, change the message priority to **"debug"** to capture all available messages.

1. From LMC, click the **System** tab.
2. From the System section, click **System Status**.
3. Set the server for which you are changing the message priority offline. For more information, see "Viewing and changing server status" on page 64.

   Note: Make sure that the server is offline before proceeding. Click **Refresh**, and then make sure that **offline** is reported in the Status column for the server.
4. Using a text editor, open the **log4j-lsas.xml** file from the **Lexmark\Solutions\apps\wf-ldss\WEB-INF\classes** folder where the server is installed.
5. In the following lines, change **"warn"** to **"debug"**:

   ```
   <!-- Root Logger. -->
   <root>
     <priority value="warn" />
   ```
6. Save and close the file.

7 From the Windows Services control panel on the server computer, restart the Lexmark Solutions Application Server. For more information, see "Restarting the Lexmark Solutions Application Server" on page 69.

8 Set the server for which you changed the message priority online. For more information, see "Viewing and changing server status" on page 64.

Note: To save disk space, after recording the data, change the message priority to **"warn"**.

Viewing the Embedded Solutions diagnostic log

All activity for solutions and eSF applications is recorded in the Embedded Solutions diagnostic log of each printer.

1 Open a web browser, and then type **http://*IP*/se**, where ***IP*** is the printer IP address or host name.

2 Click **Embedded Solutions** > **Log File**.

By default, debugging messages are not recorded. When troubleshooting a problem, enable debugging entries in the log to capture all available messages.

1 Open a web browser, and then type **http://*IP*/se**, where ***IP*** is the printer IP address or host name.

2 Click **Embedded Solutions** > **Set Logging Level** > **Yes** > **Submit**.

Note: After recording the data, set the logging level to **No**.

Troubleshooting

Solving LMC problems

A certificate error appears when accessing LMC

Try one or more of the following:

Add the LDD self-signed certificate to your certificate store

Replace the LDD self-signed certificate with another trusted certificate

Contact your Lexmark representative

The browser shows a 5yy error when accessing LMC

Try one or more of the following:

Make sure that the system has been running long enough for all services to start

It may take several minutes to start all services when the system is first booted. If the system is recently booted, or the load balancer is overloaded, then wait a few minutes, and then try again.

Make sure that the load balancer is not processing a heavy load

Uninstall and reinstall the server that is not communicating

1. On each computer where a server is installed, launch LMC by using the URL **`http://server:9788/lmc`**. ***`Server`*** is the IP address of the computer where the server is installed.
2. Click the **System** tab.
3. From the System section, select **System Status**.
4. From the main section, uninstall the server that is not communicating.

   Note: If the entry remains in the servers list in LMC after uninstalling the server, then remove the server that is not communicating. For more information, see "Viewing and changing server status" on page 64.
5. Reinstall the server.

   Note: Make sure that the correct IP address or FQDN is used for the database and load balancer when installing servers. If the server is installed on the same computer as the database and the load balancer, then use the FQDN of the computer.
6. Launch LMC by using the **`http://loadbalancer:9780/lmc`** URL, where ***`loadbalancer`*** is the IP address of the computer where the load balancer is installed.

Uninstall and reinstall all LDD components

Make sure that the correct IP address or FQDN is used for the database and load balancer when installing servers. If the server is installed on the same computer as the database and the load balancer, then use the FQDN of the computer.

Contact your Lexmark representative

LMC responds very slowly

Try one or more of the following:

Remove servers that are not communicating

1. On each computer where a server is installed, launch LMC by using the URL **`http://server:9788/lmc`**. ***`Server`*** is the IP address of the computer where the server is installed.
2. From LMC, click the **System** tab.
3. From the System section, select **System Status**.
4. From the main section, select any servers that are not communicating, and then click **Remove Server(s)**.
5. Launch LMC by using the URL **`http://loadbalancer:9788/lmc`**, where ***`loadbalancer`*** is the IP address of the computer where the load balancer is installed.

Contact your Lexmark representative

LMC does not finish loading or data is missing

Try one or more of the following:

Make sure that your web browser allows cookies for the IP address where you access LMC

Contact your Lexmark representative

Cannot upload a formset

Contact your Lexmark representative

Reports are not showing

Try one or more of the following:

Make sure that pop-ups are allowed for LMC in your web browser

Make sure that Adobe Reader is installed when running a PDF report

Contact your Lexmark representative

Cannot access tasks in LMC

Try one or more of the following:

Make sure that the group to which the user belongs to has access to tasks

Contact your Lexmark representative

Tasks are still accessible after privileges are removed

Try one or more of the following:

Make sure that the privileges of all the groups to which the user belongs to are configured correctly

For more information, see “Assigning privileges to groups” on page 55.

Contact your Lexmark representative

The Solutions tab and the eSF Configuration task for device groups do not function

Try one or more of the following:

Make sure that the descriptor file of an eSF application that is included with a solution does not contain colons

For more information, contact your solution developer.

Uninstall and reinstall the solution that caused the problem

For more information, contact your Lexmark representative.

Contact your Lexmark representative

Jobs are not responding

Try one or more of the following:

Stop the failed task

If an error occurs while a job is being processed, then stop the task. This action terminates the job that is not responding but is still marked as running in LMC.

1. From LMC, click the **System** tab.
2. From the System section, select **Jobs**.
3. Select the tasks that are not responding.
4. Click **Stop Task**.

Contact your Lexmark representative

Apache 2.4 service stopped and LMC cannot be opened

Make sure that the app server name is less than 60 characters long. For more information, see the **Apache Tomcat Connectors documentation**.

Solving discovery problems

Discovery and policy updates are running slowly

Try one or more of the following:

Make sure that communication is allowed among all system components

Check the proxy, firewall, and other network settings across the LDD system.

Make sure that the network bandwidth is sufficient during discovery and policy updates

Reduce the chunk size of multiple servers

For more information, see “Configuring chunk size for device discovery and policy updates” on page 75.

Increase the timeout period of devices during policy updates

This configuration allows sufficient time for policy updates that include the deployment of eSF applications to complete. For more information, see “Configuring policy updates” on page 103.

Discover only new devices

For more information, see “Manually discovering printers” on page 105.

Contact your Lexmark representative

Discoveries frequently time out

Try one or more of the following:

Make sure that communication is allowed among all system components

Check the proxy, firewall, and other network settings across the LDD system.

Make sure that the network bandwidth is sufficient during discovery and policy updates

Increase the NPANT timeout period

For more information, see “Configuring NPA device communication” on page 75.

Contact your Lexmark representative

Cannot discover some printers on the network

Try one or more of the following:

Make sure that communication is allowed among all system components

Check the proxy, firewall, and other network settings across the LDD system.

Make sure that all printers in the LDD system have the same read community name and write community name

For more information, see “Configuring SNMP for discovering devices” on page 76.

Make sure that the SNMP v3 read and write credentials are the same as the SNMP v3 credentials of the printer

For more information, see “Configuring SNMP for discovering devices” on page 76.

Make sure that the discovery profile is configured correctly

For more information, see “Creating a discovery profile” on page 103.

Enable the printer mDNS

1. From the Embedded Web Server, click **Settings** > **Network/Ports** > **TCP/IP**.

   Note: For a list of supported printers in each device class, see “Supported printers” on page 11.
2. Select **Enable mDNS**.
3. Click **Save** or **Submit**.

Make sure that the "Secure mode active" setting is disabled

Disable the setting for the following printer models:

- X642
- X644
- X646dte
- X646ef
- X772e
- X782
- X850
- X852
- X854
- X940
- X940e
- X945e

Contact your Lexmark representative

Solving server and printer problems

Cannot connect to the Microsoft SQL Server database by using integrated security

Try one or more of the following:

Make sure that the domain account has full control privileges to the LDD installation path on the application servers and all its subfolders

Make sure that all communication is allowed among components

Check the proxy, firewall, and other network settings across the LDD system.

Make sure that the Log On properties are configured correctly

The Log On properties of the following must be set to the domain account that has access to the Microsoft SQL Server database:

- Lexmark Apache Agent service
- Lexmark Solutions Application Server

Restart the Lexmark Apache Agent service and Lexmark Solutions Application Server

Contact your Lexmark representative

Connection times out

Try one or more of the following:

Make sure that the dbProduct.properties file in the \apps\wf-ldss\WEB-INF\classes folder is pointing to the availability group listener

Contact your Lexmark representative

Cannot update the DNS

Try one or more of the following:

Enter the DNS in the DNS server

Contact your Lexmark representative

One or more servers cannot be set online

Try one or more of the following:

Make sure that a license is installed for each server during installation

For more information on obtaining licenses, see “Obtaining licenses” on page 26. For more information on adding licenses after installation, see “Adding licenses to an existing server” on page 78.

Make sure that all communication is allowed among components

Check the proxy, firewall, and other network settings across the LDD system.

Remove servers that are not communicating

Multiple non-communicating servers may affect system performance. If you do not expect a non-communicating server to reestablish communication quickly, then remove it.

1. On each computer where a server is installed, launch LMC by using the **`http://server:9788/lmc`** URL. ***`Server`*** is the IP address of the computer where the server is installed.
2. Remove the server that is not communicating. For more information, see “Viewing and changing server status” on page 64.
3. Launch LMC by using the **`http://loadbalancer:9780/lmc`** URL, where ***`loadbalancer`*** is the IP address of the computer where the load balancer is installed.

Uninstall and reinstall the server that is not communicating

1. On each computer where a server is installed, launch LMC by using the **`http://server:9788/lmc`** URL. ***`Server`*** is the IP address of the computer where the server is installed.
2. Click the **System** tab.
3. From the System section, select **System Status**.
4. From the main section, uninstall the server that is not communicating.

   Note: If the entry remains in the servers list in LMC after uninstalling the server, then remove the server that is not communicating. For more information, see “Viewing and changing server status” on page 64.
5. Reinstall the server.

   Note: Make sure that the correct IP address or FQDN is used for the database and load balancer when installing servers. If the server is installed on the same computer as the database and the load balancer, then use the FQDN of the computer.
6. Launch LMC by using the **`http://loadbalancer:9780/lmc`** URL, where ***`loadbalancer`*** is the IP address of the computer where the load balancer is installed.

Make sure that the correct IP address or FQDN is used for the database when installing the load balancer

If the load balancer is installed on the same computer as the database, then use the FQDN of the computer. If the IP address or FQDN is incorrect, then uninstall and reinstall the load balancer and all the servers.

Contact your Lexmark representative

One or more servers cannot be set offline

Try one or more of the following:

Make sure that the Lexmark Apache Agent service is running in the Windows Services control panel

Contact your Lexmark representative

Cannot import a license

Try one or more of the following:

Make sure that the correct IP address or FQDN is used for the database and load balancer when installing servers

If the server is installed on the same computer as the database and the load balancer, then use the FQDN of the computer. If the IP address or FQDN is incorrect, then uninstall and reinstall the applicable servers.

Make sure that the correct IP address or FQDN is used for the database when installing the load balancer

If the load balancer is installed on the same computer as the database, then use the FQDN of the computer. If the IP address or FQDN is incorrect, then uninstall and reinstall the load balancer and all the servers.

Contact your Lexmark representative

A clustered service is unresponsive

Try one or more of the following:

Use custom scripts or add-on management packs that monitor applications

1. From the command prompt shell, type the following:

   ```
   C:\> cscript .\NLBMon_LDD.vbs -n 192.168.122.202 -v 192.168.122.200 -s Apache2.4 -f index.html
   ```

   Where:

   - The **-n** argument is the node that the script must connect to. This argument can be the address of the remote node.
   - The **-v** argument is the cluster virtual IP address.
   - The **-s** argument is the Windows service that must be monitored.
   - The **-f** argument is the file that must be called from the URL specified in the script.

   Note: Using the virtual IP address, the script checks all the member nodes.

2. Using Windows Task Scheduler, run the custom script regularly on all cluster nodes that run the LDD load balancer component.
   a. From Task Scheduler, click **Create Basic Task**.
   b. Configure the settings.
   c. Click **Actions** > **New**.

d In the Action menu, select **Start a program**.

e In the "Program/script" field, type **"%SystemRoot%\System32\cscript.exe"**.

f In the "Add arguments" field, enter the same argument from the command prompt shell. The following is a sample argument:

NLBMon_LDD.vbs -n *192.168.122.202* -v *192.168.122.200* -s *Apache2.4* -f *index.html*

g In the "Start in" field, type **C\scripts**.

h Click **OK**.

Contact your Lexmark representative

An “LDSS Server is unavailable” message appears on the printer control panel

Try one or more of the following:

Make sure that the system has been running long enough for all services to start

It may take several minutes to start all services when the system is first booted. If the system is recently booted, or the load balancer is overloaded, then wait a few minutes, and then try again.

Make sure that the LDD system and all servers are online

For more information, see “Viewing and changing server status” on page 64.

Make sure that all communication is allowed among components

Check the proxy, firewall, and other network settings across the LDD system.

Make sure that the solution is deployed to the device group

1 From LMC, click the **Solutions** tab.

2 Select the solution that you are trying to access from the printer.

If the solution does not appear, then install the solution. For more information, see “Uploading solutions to the LDD system” on page 98.

3 From the Tasks section, select **Summary**.

4 From the Summary section, in the Device Groups column, check that the device group that contains the printer appears.

If the device group does not appear, then make sure that the printer is added to the device group.

5 Check that the solution has been deployed to the device group. For more information, see “Deploying solutions to a device group” on page 107.

6 Perform a policy update. For more information, see “Updating policies for device groups” on page 112.

Make sure that the printer can resolve the server host name

For more information, see “Viewing the Embedded Solutions diagnostic log” on page 137.

Make sure that the correct version of the AP Bundle is installed

1. From the Embedded Web Server, do one of the following:
   - For e-Task 5 printers, click **Apps**, and then click **AP Bundle**.
   - For e-Task 4 printers, click **Settings** > **Apps** > **Apps Management**.
   - For e-Task 3 printers, click **Settings** > **Device Solutions** > **Solutions (eSF)**.
   - For e-Task 2+, e-Task 2, or e-Task printers, click **Settings** > **Embedded Solutions**.

   Note: For a list of supported printers in each device class, see "Supported printers" on page 11.
2. Make sure that the first two segments of the version number for AP Bundle match the version number of the LDD system. For version 4.6, the version of the AP Bundle must be 4.6.*x*.

Perform a policy update

For more information, see "Updating policies for device groups" on page 112.

Install the AP Bundle

1. From the Embedded Web Server, do one of the following:
   - For e-Task 5 printers, click **Apps**, and then click **AP Bundle**.
   - For e-Task 4 printers, click **Settings** > **Apps** > **Apps Management**.
   - For e-Task 3 printers, click **Settings** > **Device Solutions** > **Solutions (eSF)**.
   - For e-Task 2+, e-Task 2, or e-Task printers, click **Settings** > **Embedded Solutions**.

   Note: For a list of supported printers in each device class, see "Supported printers" on page 11.
2. Browse to the ap.fls file in the **\Lexmark\Solutions\apps\wf-ldss\firmware** folder where an LDD server is installed.
3. Click **Install** or **Start Install**.

Contact your Lexmark representative

LDSS system busy message appears on device

Sometimes, Advanced Prompt bundle communication fails because connection to the LDD load balancer is set to secure. (first HTTPS call between the device and the LDD load balancer).

Make sure that secure connection to the load balancer is disabled

1. From the Embedded Web Server, click **Apps** > **Advanced Prompt** > **Configure**.
2. Clear **Secure connection to load balancer**.

The server log contains Quartz errors

Try one or more of the following:

Make sure that the time is synchronized on all computers before installing the LDD components

If the time is not synchronized, then do the following:

1. Uninstall all components.
2. Using an NTP server, synchronize the time on all computers that are used in the LDD system.
3. Reinstall all components.

Contact your Lexmark representative

Kerberos authentication is not working

Try one or more of the following:

Make sure that the date and time are correct and synchronized on the printers, LDD servers, and KDC server

Edit the Windows registry key of the Apache Software Foundation

To log Kerberos debug messages from the Java Virtual Machine on each server, add the **`-Dsun.security.krb5.debug=true`** line to the **HKEY_LOCAL_MACHINE\SOFTWARE\Apache Software Foundation\Procrun 2.0\Tomcat7\Parameters\Java\Options** Windows registry path.

If you are using a 64-bit Windows operating system such as Windows Server 2008 R2 x64, then **HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\Tomcat7\Parameters\Java\Options** is the Windows registry path.

Note: Do not delete the existing contents of the registry key.

Warning—Potential Damage: Incorrectly editing the Windows registry may damage your Windows installation and result in an unusable system. Make sure that you understand how to make the required changes. We recommend backing up the registry before making any changes.

Debug messages are logged in the tomcat7-stdout.*yyyy-mm-dd*.log file in the **\Lexmark\Solutions\tomcat\logs** folder where the LDD server is installed.

Contact your Lexmark representative

The solution or profile icon does not appear on the home screen

Try one or more of the following:

Make sure to navigate to the last page on the printer home screen

Refresh the printer home screen

From the printer home screen, navigate to another screen and then return to the home screen.

Make sure that the printer home screen is customized correctly

For more information on customizing the home screen for a device group, see "Customizing the home screen for a device group" on page 107. For more information on customizing the home screen on specific devices, see "Customizing the home screen on specific devices" on page 115.

Make sure that the solution is deployed properly

For more information, see "Deploying solutions to a device group" on page 107.

Perform a policy update

For more information, see "Updating policies for device groups" on page 112.

Make sure that the missing icon is enabled in the printer settings

1. From the Embedded Web Server, do either of the following:
   - For e-Task 5 printers, click **Settings** > **Device** > **Visible Home Screen Icons**.
   - For e-Task 4, e-Task 3, or e-Task 2+ printers, click **Settings** > **General Settings** > **Home screen customization**.

   Note: For a list of supported printers in each device class, see "Supported printers" on page 11.
2. Select the item that corresponds to the missing icon.
3. Click **Save** or **Submit**.

Make sure that the printer access controls are not preventing policy updates from working correctly

1. From the Embedded Web Server, configure the printer access controls.
   - For e-Task 5 printers, do the following:
     a. Click **Settings** > **Security** > **Login Methods**.
     b. From the Public section, click **Manage Permissions**.
     c. Expand **Function Access** and **Device Management**, and then select **Create Profiles** and **Remote Management**, respectively.
   - For e-Task 4, e-Task 3, e-Task 2+, e-Task 2, or e-Task printers, do the following:
     a. Click **Settings** > **Security** > **Security Setup** > **Access Controls**.
     b. Expand **Management** and **Function Access**, and then set Remote Management and Create Profiles or Use Profiles to **No Security**, respectively.

   Note: For a list of supported printers in each device class, see "Supported printers" on page 11.
2. Click **Submit**.
3. From LMC, perform a policy update. For more information, see "Updating policies for device groups" on page 112.

Make sure that your printer has the latest firmware updates

For more information, contact your Lexmark representative.

Contact your Lexmark representative

Policy updates failed for a printer

Try one or more of the following:

Make sure that the device security for the printer is configured correctly

For more information, see “Configuring printer security” on page 77.

Make sure that the printer access controls are not preventing policy updates from working correctly

1. From the Embedded Web Server, configure the printer access controls.
   - For e-Task 5 printers, do the following:
     a. Click **Settings** > **Security** > **Login Methods**.
     b. From the Public section, click **Manage Permissions**.
     c. Expand **Function Access** and **Device Management**, and then select **Create Profiles** and **Remote Management**, respectively.
   - For e-Task 4, e-Task 3, e-Task 2+, e-Task 2, or e-Task printers, do the following:
     a. Click **Settings** > **Security** > **Security Setup** > **Access Controls**.
     b. Expand **Management** and **Function Access**, and then set Remote Management and Create Profiles or Use Profiles to **No Security**, respectively.

   Note: For a list of supported printers in each device class, see “Supported printers” on page 11.
2. Click **Submit**.
3. From LMC, perform a policy update. For more information, see “Updating policies for device groups” on page 112.

Contact your Lexmark representative

The printer returns to the home screen only after attempting to execute an LDD profile

Try one or more of the following:

Make sure that the AP Bundle is running

1. From the Embedded Web Server, do one of the following:
   - For e-Task 5 printers, click **Apps**, and then click **AP Bundle**.
   - For e-Task 4 printers, click **Settings** > **Apps** > **Apps Management**.
   - For e-Task 3 printers, click **Settings** > **Device Solutions** > **Solutions (eSF)**.
   - For e-Task 2+, e-Task 2, or e-Task printers, click **Settings** > **Embedded Solutions**.

   Note: For a list of supported printers in each device class, see “Supported printers” on page 11.
2. Check if the AP Bundle is enabled.

Make sure that the device security for the printer is configured correctly

For more information, see “Configuring printer security” on page 77.

Make sure that the printer access controls are not preventing policy updates from working correctly

1. From the Embedded Web Server, configure the printer access controls.
   - For e-Task 5 printers, do the following:
     a. Click **Settings** > **Security** > **Login Methods**.
     b. From the Public section, click **Manage Permissions**.
     c. Expand **Function Access** and **Device Management**, and then select **Create Profiles** and **Remote Management**, respectively.
   - For e-Task 4, e-Task 3, e-Task 2+, e-Task 2, or e-Task printers, do the following:
     a. Click **Settings** > **Security** > **Security Setup** > **Access Controls**.
     b. Expand **Management** and **Function Access**, and then set Remote Management and Create Profiles or Use Profiles to **No Security**, respectively.

   Note: For a list of supported printers in each device class, see "Supported printers" on page 11.
2. Click **Submit**.
3. From LMC, perform a policy update. For more information, see "Updating policies for device groups" on page 112.

Perform a policy update

For more information, see "Updating policies for device groups" on page 112.

Install the AP Bundle

1. From the Embedded Web Server, do one of the following:
   - For e-Task 5 printers, click **Apps**, and then click **AP Bundle**.
   - For e-Task 4 printers, click **Settings** > **Apps** > **Apps Management**.
   - For e-Task 3 printers, click **Settings** > **Device Solutions** > **Solutions (eSF)**.
   - For e-Task 2+, e-Task 2, or e-Task printers, click **Settings** > **Embedded Solutions**.

   Note: For a list of supported printers in each device class, see "Supported printers" on page 11.
2. Browse to the ap.fls file in the **\Lexmark\Solutions\apps\wf-ldss\firmware** folder where an LDD server is installed.
3. Click **Install** or **Start Install**.

Contact your Lexmark representative

The solution stops responding

Try one or more of the following:

Wait a few minutes to see if the network connection returns

Restart the printer

Make sure that the network cable is connected correctly

Check the printer network settings and the status of the network

For more information, see the documentation that came with the printer.

Contact your system administrator

The solution cannot connect to the network

Try one or more of the following:

Make sure that the local network domain can bypass the proxy server

Add the local network domain as an exception in the proxy server settings of the printer.

Contact your Lexmark representative

The LDSS profile cannot forward incoming faxes on e-Task 5 printers

Try one or more of the following:

Make sure that the "Forward to" shortcut number fields of the printer Fax settings is empty

From the Embedded Web Server, click **Settings** > **Fax** > **Analog Fax Setup** > **Fax Receive Settings** > **Admin Controls**.

Contact your system administrator

The server log shows an incorrect user name or password when accessing network files

Try one or more of the following:

Add the user name in LMC

From LMC, add the user name by using the ***y\yy*** format, where ***y*** is the domain name and ***yy*** is the user name or host name.

Contact your Lexmark representative

Solving client software problems

Cannot create a Lexmark Document Server port

Try one or more of the following:

Make sure that the Lexmark Document Server port is configured with administrative privileges

Make sure that the Lexmark Document Server port is configured correctly

For more information, see “Configuring a Lexmark Document Server port” on page 128.

Make sure that at least one server is online

For more information, see “Viewing and changing server status” on page 64.

Make sure that a license is installed for the software clients, and is not expired

For more information, see “Adding licenses to an existing server” on page 78.

Make sure that the software client group is configured correctly

For more information, see “Adding software clients to a software client group” on page 123.

Make sure that all communication is allowed for the load balancer

Check the proxy, firewall, and other network settings on the client computer.

Contact your Lexmark representative

System processes terminate unexpectedly when creating a Lexmark Document Server port

Try one or more of the following:

Make sure that the profile that is assigned to the Lexmark Document Server port has a name of 14 characters or fewer

Make sure that the port name has 75 characters or fewer

Restart the computer where you added the port

Contact your Lexmark representative

LDD printers cannot send jobs to the LDD system

Try one or more of the following:

Make sure that a Lexmark Document Server port is created and assigned a print queue by using an existing print driver

For more information, see “Adding LDD printers on a client workstation or print server” on page 126.

Make sure that a license is installed for the software clients, and is not expired

For more information, see “Adding licenses to an existing server” on page 78.

Make sure that a solution is deployed correctly to a software client group that is containing the software client

For more information, see “Assigning solutions to a software client group” on page 124.

Make sure that all communication is allowed for the load balancer

Check the proxy, firewall, and other network settings on the client computer.

Run Windows Update

Updating the Windows system ensures that the latest updates for the .NET framework are installed.

Contact your Lexmark representative

Cannot send files to the LDD system by using Microsoft Windows application software Select'N'Send

Try one or more of the following:

Make sure that a license is installed for the software clients, and is not expired

For more information, see “Adding licenses to an existing server” on page 78.

Make sure that a solution is deployed correctly to a software client group that is containing the software client

For more information, see “Assigning solutions to a software client group” on page 124.

Make sure that all communication is allowed for the load balancer

Check the proxy, firewall, and other network settings on the client computer.

Contact your Lexmark representative

Solutions are receiving inaccurate page counts

Try one or more of the following:

Make sure that jobs are not sent until they are finished spooling

1. From your computer, in the Windows “Devices and Printers” control panel, right-click the printer, and then click **Properties**.
2. Click the **Advanced** tab.
3. Select **Spool print documents so program finishes printing faster** and **Start printing after last page is spooled**.
4. Click **OK**.

Make sure that you have the latest Office service pack installed

If you are using Microsoft Word, then see the Microsoft Knowledge Base article KB919736 (**support.microsoft.com/kb/919736**).

Contact your Lexmark representative

LDAP table field length is not increased in Microsoft SQL Server database

This error may occur after upgrading to LDD version 5.1. Try one or more of the following:

Increase the field length in the LDAP table manually

Contact your Lexmark representative

Notices

Edition notice

March 2022

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**.

Trademarks

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

Adobe, Flash, Flash Player, and Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Firebird is a registered trademark of the Firebird Foundation.

Google Chrome is a trademark of Google LLC.

Java is a registered trademark of Oracle and/or its affiliates.

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.

The Apache Software License, Version 1.1

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The end-user documentation included with the redistribution, if any, must include the following acknowledgment:

   "This product includes software developed by the Apache Software Foundation (http://www.apache.org/)."

   Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.
4. The names "Apache" and "Apache Software Foundation", "Jakarta-Oro" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact apache@apache.org.
5. Products derived from this software may not be called "Apache" or "Jakarta-Oro", nor may "Apache" or "Jakarta-Oro" appear in their name, without prior written permission of the Apache Software Foundation.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

==========

This software consists of voluntary contributions made by many individuals on behalf of the Apache Software Foundation. For more information on the Apache Software Foundation, please see **http://www.apache.org/**

Apache License Version 2.0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

   "License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

   "Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2 Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3 Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4 Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

- **a** (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and
- **b** (b) You must cause any modified files to carry prominent notices stating that You changed the files; and

c (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

d (d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5 Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6 Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7 Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8 Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9 Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

Index

D

E

F

M

N

O

P

R

S

T

U

V

W