



LexmarkTM

Document Distributor

Version 4.9.2

Administrator's Guide

July 2016

www.lexmark.com

Contents

Overview.....	5
Understanding the stages of a job.....	5
Understanding the Lexmark Document Distributor system.....	6
Security overview.....	10
System setup overview.....	10
Supported printers.....	11
Supported ECM software platforms.....	12
Installing Lexmark Document Distributor.....	13
System requirements.....	13
Preparing for the installation.....	15
Avoiding conflicts with other software.....	15
Ports used by the LDD system.....	15
Obtaining licenses.....	16
Understanding installation types.....	17
Installing a workgroup system.....	17
Installing an enterprise system.....	18
Antivirus policy requirements and recommendations.....	28
Installing LDD components silently.....	29
Upgrading to LDD 4.9.....	30
Configuring Kerberos authentication.....	31
Monitoring and maintaining the system.....	34
Configuring Lexmark Management Console.....	34
Finding basic information.....	43
Managing the LDD system.....	47
Managing system performance.....	52
Configuring communications.....	56
Managing licenses.....	57
Managing reports.....	57
Backup and disaster recovery.....	64
Managing solutions and cSF apps.....	69
Understanding the deployment process.....	69
Understanding solution or cSF app settings.....	69

Uploading solutions to the LDD system.....	70
Configuring global settings.....	70
Editing local settings for a deployed or assigned solution.....	71
Configuring an eSF application associated with a solution.....	71
Managing solution-related files.....	72
Removing solutions or cSF apps.....	72

Managing device groups and devices..... 74

Creating and populating device groups.....	74
Deploying solutions to a device group.....	78
Customizing the home screen for a device group.....	79
Updating policies for device groups.....	83
Scheduling policy updates.....	84
Enabling secure communication between servers and printers in a device group.....	84
Disabling validation of eSF application deployment.....	84
Configuring the Devices tab.....	85

Managing software clients..... 88

Understanding software clients and software client groups.....	88
Understanding dynamic prompting support.....	89
Understanding software client setup.....	89
Creating and populating software client groups.....	90
Assigning solutions to a software client group.....	91
Installing client software.....	91
Installing client software on a Microsoft Cluster Server.....	92
Adding LDD printers on a client workstation or print server.....	92
Configuring a Lexmark Document Server port.....	94
Increasing LDD print queue availability	94

Testing and using Lexmark Document Distributor solutions..... 95

Launching a solution from a printer.....	95
Using LDD print queues.....	95
Configuring the Microsoft Windows application software Select'N'Send.....	96
Scheduling scripts.....	99

Viewing logs..... 101

Viewing installation logs.....	101
--------------------------------	-----

Viewing the server logs.....	101
Viewing the Embedded Solutions diagnostic log.....	102
Troubleshooting.....	103
Solving LMC problems.....	103
Solving discovery problems.....	105
Solving server and printer problems.....	106
Solving client software problems.....	113
Appendix.....	116
Notices.....	119
Index.....	124

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 submit digital documents from individual computers. Some functions, such as print release, can be accessed from some single-function printers (SFPs). To view a list of supported printers, 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 native 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.
- 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 configure, use, and troubleshoot LDD.

Understanding the stages of a job

Document capture

The paper document is converted into a digital document from a Lexmark printer, or a digital document is selected on a user's computer. The user chooses from *profiles*, predefined job types that determine through scripts how the scanned document will be processed and routed. On a printer, the most commonly used profiles are often configured as buttons on the home screen.

Document processing

Document processing takes place on the LDD server after the document capture stage is complete. The document is analyzed or modified according to scripts associated with the profile selected prior to document capture.

Common tasks in document processing include reading bar codes, OCR, and image processing and manipulation.

Document routing

The main function of LDD is delivering captured documents to other systems. The LDD system uses its processing capabilities to transform paper documents into formats required by your business processes. A document can be routed to multiple destinations. When a user submits a document, LDD can automatically fax, e-mail, print, or archive it without further user intervention.

LDD can route documents to any of the following destinations:

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

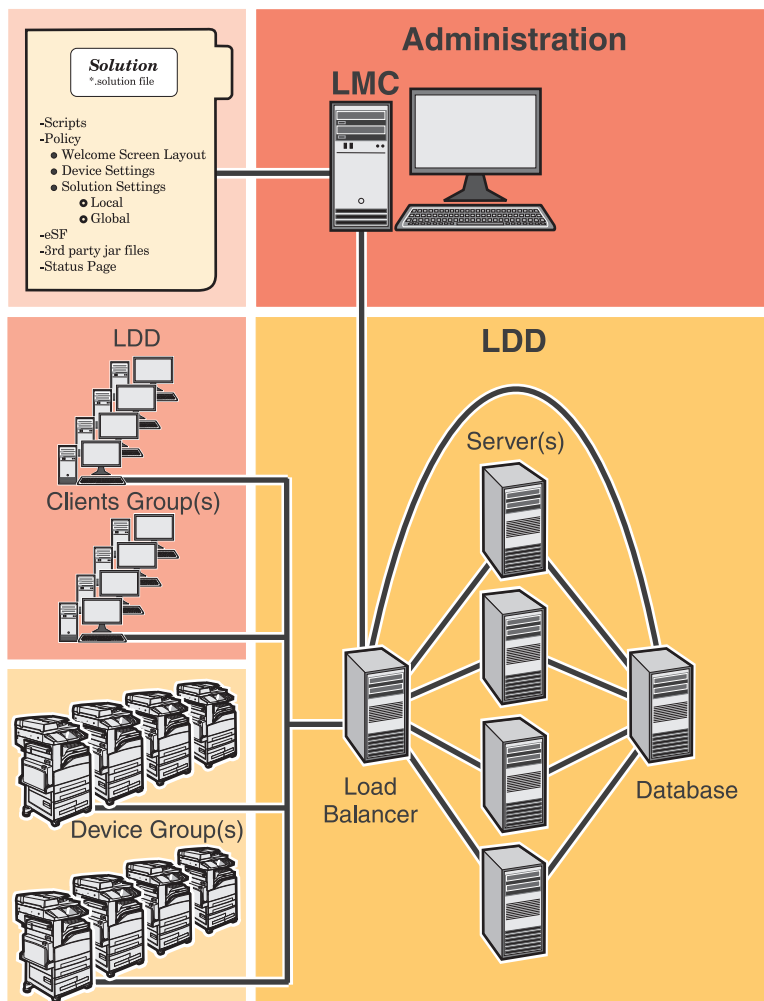
Confirmation

After document capture, processing, and routing, the user can be provided with feedback indicating success or failure. 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 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 document capture and document processing stages of a job.
- **LDD servers**—Process incoming jobs, which manage document processing and document routing stages of a job.
- **Database**—Maintains information about clients, solutions, settings, and jobs.



Reliability, scalability, and disaster recovery

The load balancer, database, and server components may be installed together on one computer or separately on individual computers, depending on the demands placed on the system. However, a one-computer setup is subject to downtime if that computer fails, and the server load will be fairly limited. Ideally, a system should have at least two server computers, connected to separate database and load balancer computers.

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

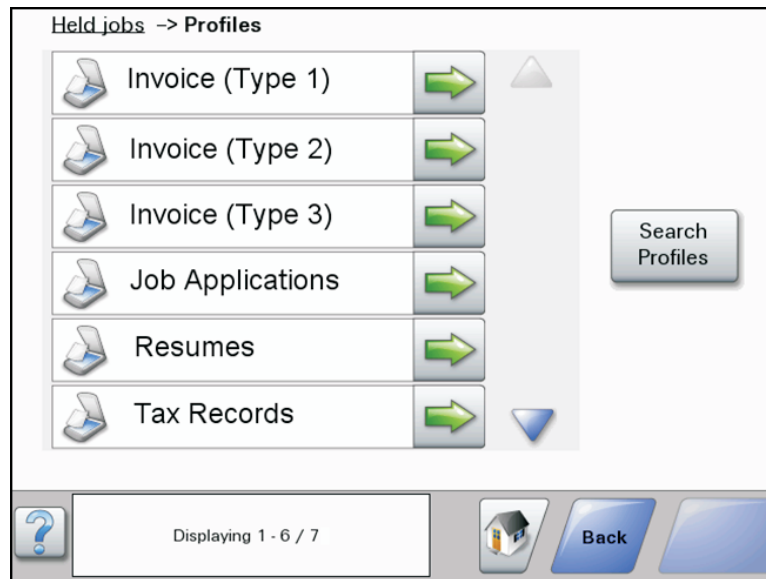
LDD uses a Tomcat Connector to manage load balancing in the system. The default balancing method is *session*, which estimates the number of sessions open by counting requests to the system that do not have a session cookie. The session count is decayed by dividing in half, once per minute by default. The server with the lowest number of estimated sessions is selected to process the request.

To further increase reliability by keeping the system online in the event of a failing load balancer or database, the load balancer and database can each be paired in a failover cluster using a *Microsoft Cluster Server (MSCS)*.

Finally, you can back up the databases and solutions from the database and load balancer to a network share. If a recovery becomes necessary, then a new load balancer and/or database can access the recovery data using a Restore Install. Existing servers are directed to the new database and/or load balancer, or new servers are installed as necessary.

Workflow solutions

In LDD, 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 solicit user input for processing and routing documents. For example, a script that processes bank loans may request 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:
 - **Device settings**—The configuration required on printers to support the jobs. This configuration typically includes profiles but can include almost any device setting.
 - **Solution settings**—Settings that allow you to 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 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 used for merging data with standard forms.
- **Custom reports**—Reports created by a solution developer that present custom data.

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.

There are 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.

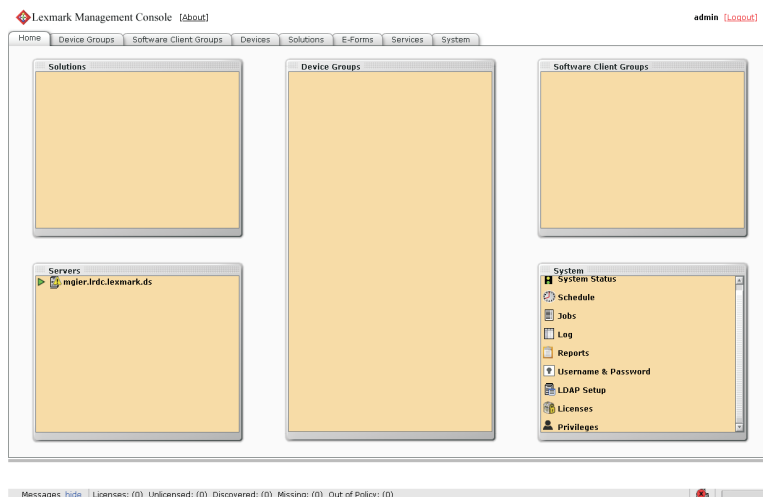
An LDD printer port can now be assigned to an LDD server system profile that prompts for user input at the time of printing. The profile or script running on the LDD server system that the LDD printer port is assigned to controls the prompting. For LDD printer port prompting, install the LDD port monitor 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 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 using a Flash® plug-in with 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 components or with any Lexmark printer that supports encryption. Encryption for communication between LDD components is accomplished using 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

Each of the following steps represents a different stage of the system setup process, covered in the chapter indicated:

- 1 Activate the appropriate licenses, and then install the database, load balancer, and servers. For more information, see [“Installing Lexmark Document Distributor” on page 13](#).
- 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 74](#) and [“Backup and disaster recovery” on page 64](#).
- 3 Deploy solutions to printers. For more information, see [“Managing solutions and cSF apps” on page 69](#).

- 4 If you are using software clients, prepare software client groups and install client software where necessary. For more information, see [“Managing software clients” on page 88](#).
- 5 Test deployed solutions on printers and software clients. For more information, see [“Testing and using Lexmark Document Distributor solutions” on page 95](#).

Supported printers

e-Task 5 printers ¹	e-Task 4 printers	e-Task 3 printers	e-Task 2+ printers	e-Task 2 printers	e-Task printers ²	X642 printers
MFPs <ul style="list-style-type: none"> CX725 CX860 CX825 CX820 SFPs <ul style="list-style-type: none"> CS720 CS725 CS820 	7- or 10-inch screen MFPs <ul style="list-style-type: none"> CX510 MX610, MX611 MX6500e MX710, MX711 MX810, MX811, MX812 MX910, MX911, MX912 4.3-inch screen MFPs <ul style="list-style-type: none"> CX410 MX410, MX510, MX511 7-inch screen SFP <ul style="list-style-type: none"> MS812de 4.3-inch screen SFPs <ul style="list-style-type: none"> CS510 MS610de MS810de MS911 	MFPs <ul style="list-style-type: none"> 6500e X548 X746, X748 X792 X925 X950, X952, X954 SFPs <ul style="list-style-type: none"> C748 C792 C925 C950 	MFPs <ul style="list-style-type: none"> X463, X464, X466 X651, X652, X654, X656, X658 X734, X736, X738 X860, X862, X864 SFP <ul style="list-style-type: none"> T656⁴ 	MFPs <ul style="list-style-type: none"> X644, X646 X772 X782 X850, X852, X854 X940, X945 SFPs <ul style="list-style-type: none"> T654⁴ W850⁴ 	MFPs <ul style="list-style-type: none"> X620³ X632, X634³ X752³ X820³ X830, X832³ X912³ SFPs <ul style="list-style-type: none"> C520, C522, C524⁴ C530, C532, C534⁴ C734, C736⁴ C780, C782⁴ C920⁴ C935⁴ E450⁴ E460, E462⁴ T640, T642, T644⁴ T650, T652⁴ W840⁴ 	X642

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

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

³ These printers may be identified as “C,” “T,” or “W” models in LMC.

⁴ These SFPs do not support all prompts supported by MFPs. For a list of supported prompts, see [“Prompts supported by single-function printers” on page 116](#).

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 116](#).

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

Category	Required	Recommended for enterprise systems
Operating system	<ul style="list-style-type: none"> 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 (x86 and x64) 	Windows Server 2012 R2 (x64) Windows Server 2008 R2 (x64)
Processor	2GHz dual-core	Dual 2.5GHz quad-core Intel Xeon or AMD Opteron™
RAM	4GB	8GB
Hard disk drive	20GB free space for each system component	Configuration 1-N, X-N, or X-Y-N: <ul style="list-style-type: none"> Database and load balancer <ul style="list-style-type: none"> 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 <ul style="list-style-type: none"> 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. <p>Note: For more information, see “Assigning servers to run LMC only or process jobs” on page 55.</p>
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
Note: Install the database on the fastest available hardware with the fastest disk I/O infrastructure.		

Category	Required	Recommended for enterprise systems
Network name resolution	Domain Name System (DNS) or Windows Internet Name Service (WINS) Notes: <ul style="list-style-type: none"> Local hosts files can be used instead of external DNS. For other network systems support, contact your Lexmark representative. 	
Static addressing	<ul style="list-style-type: none"> 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.

Category	Requirement
Browser	<ul style="list-style-type: none"> Internet Explorer® 7.0 or later Mozilla Firefox 9.0 or later Google Chrome™ Notes: <ul style="list-style-type: none"> Make sure that your browser supports Adobe® Flash® Player 10 or later. Enable cookies in the browser where the LMC address is accessed.
Video	Capable of displaying 1024 x 768 or higher resolutions.

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 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 10
- Windows 8.1
- Windows 8
- Windows 7 with SP1
- Windows Vista® with SP2

Note: 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.

Supported database servers

- Firebird® (default)
- 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.

Preparing for the installation

- 1 Download the installation package and the license files.

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

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

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

- 3 Extract the installation package, and then follow the instructions on the screen.

Avoiding conflicts with other software

- Install each system component on a computer with a new Windows operating system installation and with no other software installed.
- Avoid installing other software that includes these applications 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) may conflict with Apache HTTP Server and must not be installed.

Ports used by the LDD system

Allow communication of 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.

Component	Port	Protocol	Function
Database (Firebird)	3050	TCP	Database communications
	8001	TCP	Backup or restore agent

Component	Port	Protocol	Function
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
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 accessible to the server, and then continue with the server installation.
- For more information on licensing, contact your Lexmark representative.

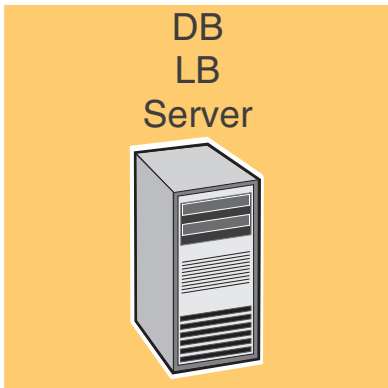
Understanding installation types

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.

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 to install LDD on the network.
- 2 Activate and download licenses.
- 3 Install LDD using a workgroup installation.
- 4 Change the administrator password, and optionally, the administrator user name.
- 5 Temporarily set servers online to test function.

Note: Because software clients are managed differently than printers, client software is installed later in the system setup process. For information about installing client software and managing software clients, see [“Managing software clients” on page 88](#).

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**.

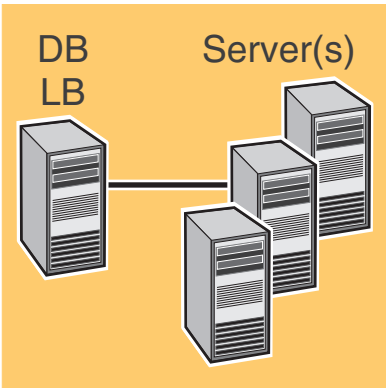
Note: You can install optional server components, such as Barcode Read, Barcode Write, and OCR, after the LDD installation.
- 7 Specify a location for the installation, and then click **Next**.
- 8 For multiple networks, select the IP address of the server that is connected to the same network as your printers, and then click **Next**.

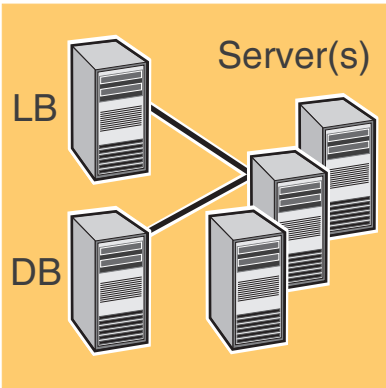
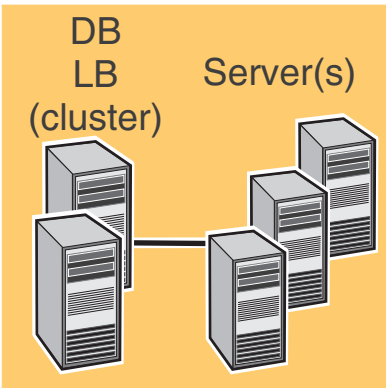
Note: If necessary, select **Allow only IP address**.
- 9 If you are installing a backup recovery system, then select **Restore Install (RI)**, specify or locate the .ri file, and then click **Next**.
- 10 Review the setup information, and then click **Next**.
- 11 Click **Install**.

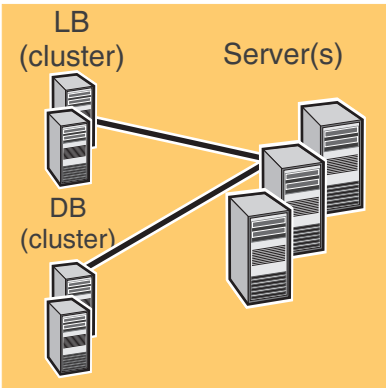
Installing an enterprise system

Configuration types for enterprise systems

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

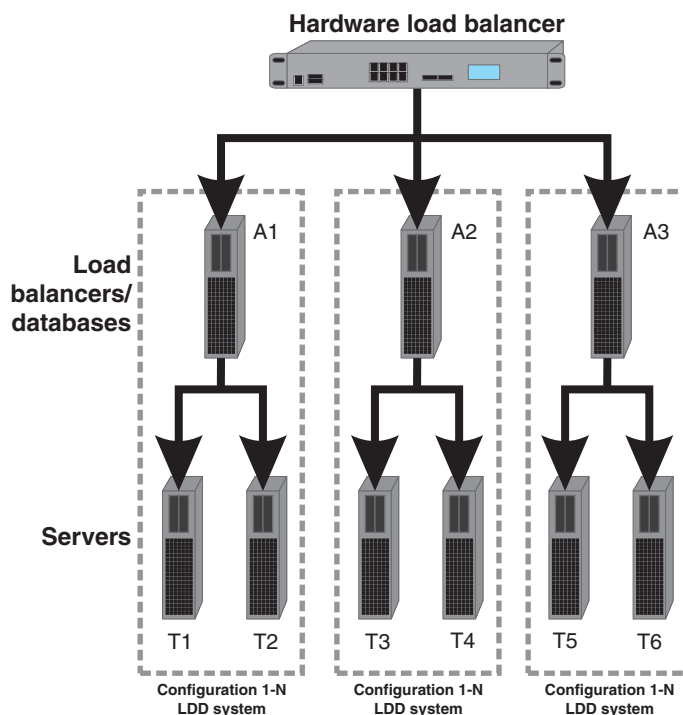
Configuration	Description	Advantages	Disadvantages
1-N	<p>The database (DB) and load balancer (LB) are on one computer, and the server is on one or more computers. This setup is the most common when failover is not used.</p> 	Improved performance	Increased hardware needs, no failover for database or load balancer

Configuration	Description	Advantages	Disadvantages
1-1-N	<p>The database (DB) and load balancer (LB) are on separate computers, and the server is on one or more computers.</p>  <p>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.</p>	Further improved performance	Further increased hardware needs, no failover for database or load balancer
X-N	<p>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.</p> 	High availability, improved performance	Increased hardware needs, cluster licensing

Configuration	Description	Advantages	Disadvantages
X-Y-N	<p>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.</p>  <p>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.</p>	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 in a group fails, then the other system in the group receives all incoming jobs until the failed system is restored.

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.
Based on tests made on hardware balancing algorithms, LDD systems work better with Round Robin than the other algorithms.

System sizing guidelines

There are two main factors for determining the number of servers required to process jobs efficiently:

- **Peak demand**—This is usually the deciding factor when the average execution time for a solution is under 30 seconds.
- **Concurrency**—This is usually the deciding factor when the average execution time for a solution is over 30 seconds.

Additionally, the database, when installed on the recommended hardware and connected using Gigabit Ethernet, can process 200,000 logged messages per hour, which is approximately 40,000 jobs per hour when using a typical solution (five logged messages per job). If this limit is reached, then it may be necessary to use multiple systems.

Peak demand

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

(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:

- Each server in your system can process 3000 jobs per hour using the solution.
- There is capacity for 300 printers in your system.
- Each printer in your system averages 100 jobs per day.

Perform the following calculations:

1 Determine the system-wide hourly job rate:

$$(300 \text{ printers}) \times (100 \text{ daily jobs/printer}) / (8 \text{ hours/day}) = \mathbf{3750 \text{ jobs/hour}}$$

2 Determine the peak demand:

$$2 \times (3750 \text{ jobs/hour}) = \mathbf{7500 \text{ jobs/hour}}$$

3 Determine the minimum number of servers:

$$(7500 \text{ jobs/hour}) / (3000 \text{ jobs/hour}) = \mathbf{2.5}$$

Rounding up, the system should include three servers to reliably handle the peak load for a solution with average execution time below 30 seconds.

The single-server throughput for a solution must be determined by the solution developer, though the following typical throughputs on a server with the recommended hardware may help determine a rough estimate:

Solution processing load	Functions used	Average single-server throughput
Typical	<ul style="list-style-type: none"> Some image processing Printing 	6000–8000 jobs per hour
Heavy	<ul style="list-style-type: none"> Extensive image processing Bar codes External processes Small to medium Document Producer (e-forms) jobs 	2000–3000 jobs per hour
Very heavy (OCR)	<ul style="list-style-type: none"> OCR Large Document Producer (e-forms) jobs 	100–200 jobs per hour

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

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

Concurrency

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

$$(\text{minimum number of servers}) = (\text{number of printers expected to submit jobs near the same time}) / 30$$

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

$$100 / 30 = \mathbf{3.33}$$

Rounding up, the system should include four servers to allow for 100 active printers for a solution with average execution time below 30 seconds.

Installation overview for an enterprise system

- 1 Select a system configuration, and then configure the appropriate hardware on the network.
- 2 Synchronize the time on all computers used in the LDD system using a Network Time Protocol (NTP) server.
- 3 Install the system components.

Note: If you are installing LDD using the default database (Firebird), then the system components can be installed in any order. However, if you are using Microsoft SQL Server database, then see [“Configuring LDD with a Microsoft SQL Server database” on page 23](#) before installing LDD.

- a Install the database.
- b Download and activate licenses on the computer where the load balancer is 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 the servers online temporarily.

Notes:

- The database requires the most system resources and disk I/O, and therefore should be installed on the fastest hardware with the fastest disk I/O infrastructure available. Second in resource usage are the servers.
- LDD components can be installed on virtual servers using VMware ESX 3.0.1 or later. However, the best performance can be achieved only by using separate physical servers.

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.

Note: To view the list of supported database servers, see [“System requirements” on page 13](#).

- LDD system components are not installed on the server running Microsoft SQL Server.
- The default database (Firebird) 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 sub-folders.

For LDD to work with Microsoft SQL Server, create seven databases before the load balancer and server are installed. To help the database administrator create these databases, do the following:

- 1 Open the *CreateDatabase.sql* file at ***installpath*\mssql\scripts\CreateDatabase.sql**, where ***installpath*** 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 *installpath*\mssql\scripts\CreateDatabase.sql -o *outputfilepath* \MyOutput.txt, where ***installpath*** is the location of the LDD installer, and ***outputfilepath*** is the location where you want to save the log file.
- 4 Confirm that the databases are installed completely.
 - a Type **sqlcmd -S .** to connect to the default instance.
 - b Type **select name from sys.databases** to show all databases.

5 Enable TCP/IP connections and port numbers.

In the SQL Server Configuration Manager, do the following:

- a From the Server Network Configuration, make sure that TCP/IP is enabled and the port number is set to 1433.

Note: To check the port numbers for the IP addresses, open the TCP/IP properties.

- b From the Native Client Configuration, make sure that TCP/IP is enabled.

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.

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 default database (Firebird) 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)**, specify or locate 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 sub-folders.
- 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 50](#).

10 If you are installing a backup recovery system, then select **Restore Install (RI)**, specify or locate 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 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 default database (Firebird) 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)**, specify or locate 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 sub-folders.
 - 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)**, specify or locate 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_WMIPProvider.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_WMIPProvider.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 sub-folders.
- 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 set the 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.

Antivirus policy requirements and recommendations

Required antivirus policies

- Do not include the following folders when performing real-time virus scanning:
 - Load balancer server or database server (or only the database server if the load balancer is installed on another server)
 - \Lexmark\solutions\firebird\data
 - \Lexmark\solutions\Apache2\logs
 - \Lexmark\solutions\Apache2\htdocs\apachewebdav
 - All Tomcat transaction servers (\Lexmark and all subfolders)

If this is not allowed, the following folders *must* be excluded:

- \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 file shares and subdirectories where solutions installed write files
- Make sure full virus scans and virus definition updates on all Lexmark servers, including load balancers or databases, application servers, and print servers are scheduled to run during off-peak hours.

Recommended antivirus policy

If you are running the system on a virtualized server environment, then make sure full virus scans and virus definition updates on all virtual machines on the same virtual machine hosts as the Lexmark virtual machine servers are scheduled to run during off-peak hours.

Installing LDD components silently

LDD components may be installed silently using the batch files 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 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 user name and 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 an SQL Server user name and 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.

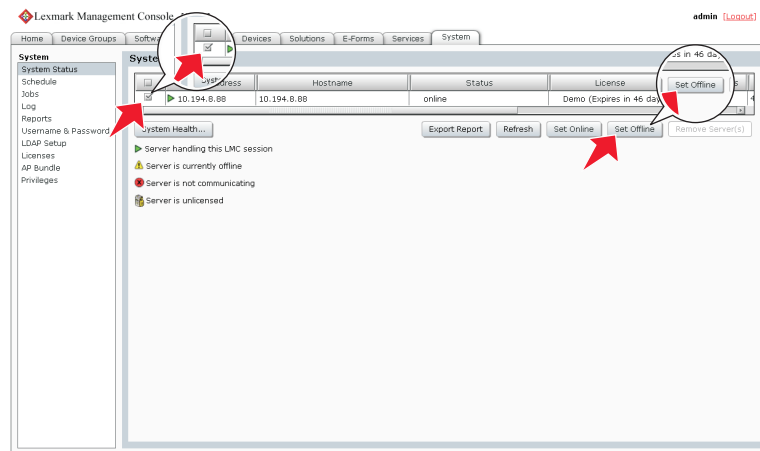
Note: For **Install_LoadBalancer_MSSQL.bat** and **Install_Server_MSSQL.bat**, make sure to allow the domain account to access the Microsoft SQL Server database by enabling integrated security when installing the database. Make sure that the domain account is granted access to the Microsoft SQL Server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

- 3 Run the batch file again using the appropriate options as shown in the usage instructions.
- 4 Follow the instructions on the screen.

Upgrading to LDD 4.9

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

- 1 From the System tab in LMC, click **Refresh**, and then set the status of all servers to offline.



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

- 2 If the database or load balancer is installed on a failover cluster, then do the following:
 - a On the primary node in each cluster, close all unnecessary applications.

Note: Make sure that no applications 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.

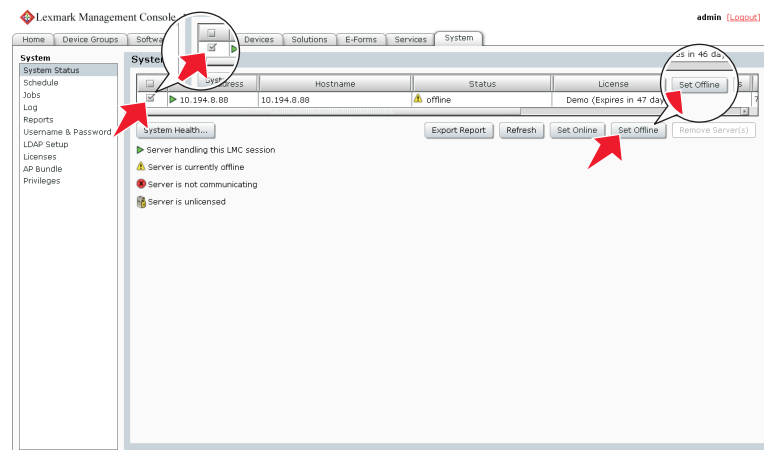
Before continuing the upgrade, wait for confirmation that the standby nodes are disabled.
 - d Set the status of all Lexmark resources to offline.
- 3 From the LDD database and load balancer servers, run the LDD installer, click **Update**, and then follow the instructions on the screen.

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 sub-folders.
- 4 If the database or load balancer is installed on a failover cluster, then do the following:
 - a From Failover Cluster Manager, set the status of all Lexmark resources to 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 a second time.
 - c Make sure that the Lexmark cluster resources are started.
 - d Start the cluster service on standby nodes.
 - 5 In all LDD servers, run the LDD installer, click **Update**, and then follow the instructions on the screen.
 - 6 Reinstall custom components on the servers.
 - 7 Reinstall all previously installed solutions, including those solutions that were automatically added during a previous installation.
 - 8 Make sure that device groups, software client groups, solutions, and all settings are correct.
 - 9 From the System tab in LMC, set all servers online.



Configuring Kerberos authentication

If a user logs in at a printer using Kerberos, then the LDD system uses the credentials to manipulate network files or 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 84.

- Make sure that the date and time on the printer, LDD server, and key distribution center (KDC) server are 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 for 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 Network Overview section or TCP/IP section of the Network/Ports menu.

2 From the Embedded Web Server, click **Settings > Security > Security Setup**.

3 In the Advanced Security Setup section, click **Kerberos 5**.

Importing a Kerberos configuration file

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 should be marked forwardable by default. For more information about configuration files, see the Kerberos documentation.

Creating a simple Kerberos configuration file

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

b In the KDC Port field, enter the number of the port (**1–88**) used by the Kerberos server. The default is **88**.

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

d Click **Submit**.

4 Add a security template:

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

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

c Select the **Kerberos Building Block** authentication setup.

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

5 Configure access controls for profiles:

a In the Advanced Security Setup section, click **Access Controls**.

b Apply the security template to all profiles or to a specific profile.

- To apply the security template to all profiles on the printer, including eSF applications, select the security template that you created beside Use Profiles.

- To apply the security template to an individual profile, do the following:

1 Determine the access control number of the profile.

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

a From the Device Groups tab in LMC, select the device group that contains the printer and the solution.

b Select the **Profiles** task.

c In the main window, select the tab that corresponds to the device class of the printer.

d Find the number beside Access Control.

Note: If **0** appears beside Access Control, then no access control number is assigned to the profile. For more information, contact your Lexmark representative.

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

c 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

When using Kerberos authentication, you may need to configure Kerberos on each LDD server in your system.

The LDD server requesting a ticket must have the KDC address and realm available in order to request a Kerberos ticket. Often, the KDC address and realm can be determined from the ticket forwarded from the printer. In this case, no configuration is 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 manually configure each LDD server for Kerberos authentication, do one of the following:

- Create a Kerberos configuration file for the server. This file may be a duplicate of the file uploaded to configure Kerberos on the printer, but we recommend a minimal configuration specifying only the KDC address and realm. The configuration file must be named `krb5.ini`, and it should be placed in the folder `\Lexmark\Solutions\Security` where LDD is installed on each LDD server. (You may have to create the Security folder.)

Note: If you need to read the Kerberos configuration file from another location, see the Apache Tomcat documentation for more information.

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

Monitoring and maintaining the system

Configuring Lexmark Management Console

Accessing Lexmark Management Console

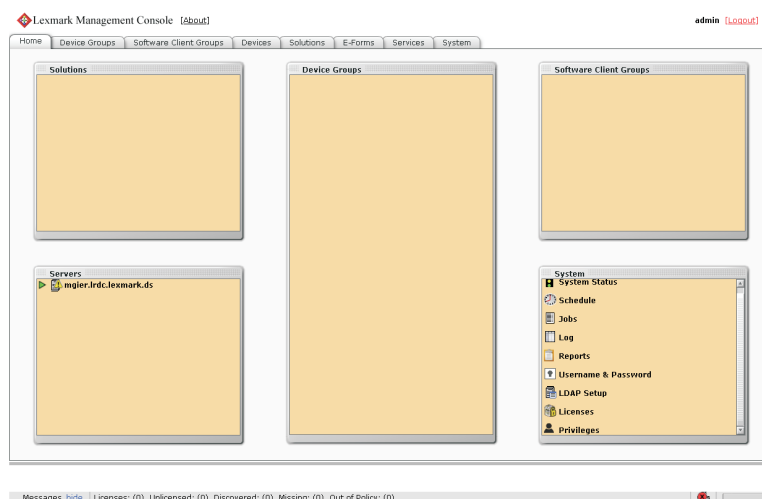
- 1 Launch LMC from your Web browser using the URL **http://loadbalancer:9780/lmc**, where **loadbalancer** is the computer where the load balancer is installed.

The load balancer selects a server to host the LMC session, indicated by a green arrow beside a server in the Servers list on the Home tab after logging in.

Notes:

- On a computer where a server is installed, you can use the desktop shortcut to access LMC.
- To access LMC on a particular server, use the URL **http://server:9788/lmc**, where **server** is the computer where the chosen server is installed.
- It may take several minutes to start all services after the system boots. If LMC cannot be accessed immediately after booting the system, wait a few minutes, and then try again.
- Cookies must be enabled on your Web browser in order to use LMC.
- Adobe Flash Player 10 or later is required. If your Web browser settings do not allow ActiveX controls to run, then you must upgrade manually by visiting the Adobe Web site.

- 2 Enter the administrator user name and password, and then click **Login**.



Notes:

- The default user name and password are both **admin**.
- If LMC is configured to connect to an LDAP server, any valid user name and password may be used.

The Home tab is displayed after a successful login.

Changing the administrator user name

- 1 In LMC, click the **System** tab.
- 2 Select **Username & Password** from the System list.
- 3 Type the new user name.
- 4 Re-type the new user name to confirm it.
- 5 Click **Apply**.

Changing the administrator password

- 1 Click the **System** tab.
- 2 Select **Username & Password** from the System list.
- 3 Type the current password.
- 4 Type the new password, and then re-type it to confirm.
- 5 Click **Apply**.

Enabling LDAP server authentication for LMC

The administrator can set up a connection with an LDAP server to authenticate users other than the administrator account.

- 1 Click the **System** tab.
- 2 From the System list, 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 used in the directory 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 should begin in the directory, 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 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 should 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 used to log in to the LDAP server, such as **uid=ldapuser,ou=Employees,o=MyOrganization**.
 - c Type the password associated with the selected user name.

10 If you want to test the connection settings, then 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 is used, then manually check them.

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

12 Click **Save Settings**.

Assigning privileges to groups

You can add access control to users accessing LMC. This feature allows you to restrict system access to authorized groups. The Privileges settings depend on the role assigned to the user.

Notes:

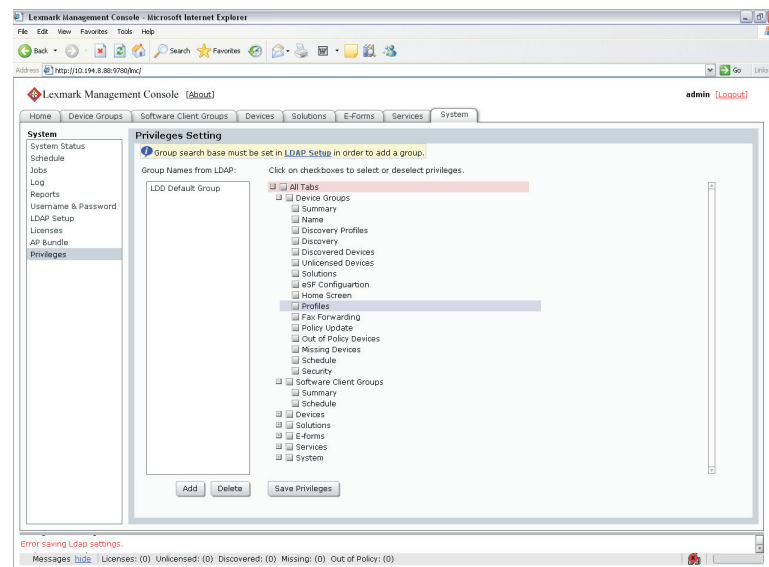
- You need to add a group first before defining privileges. By default, the Default Group is already added to the group list. This group has access to all tabs and tasks of LMC. The administrator can modify the privileges of the default group.

- If a user belongs to multiple groups, then group privileges are combined. Privileges can be modified for LDAP users only. The default administrator has access to all tabs and tasks, and these settings cannot be modified.

- 1 Select **Privileges** from the System list.
- 2 Select a group from the “Group Names from LDAP” list, or add a new group.

To add a group:

- a Click **Add**, then type the first few characters of the group name, and then click **Search**.
 - b Select a group name from the list, and then click **Add**.
- 3 Select the tabs and tasks the group is allowed to access and perform.
When assigning privileges, you can select specific tasks under each tab.



- 4 Click **Save Privileges** to save settings.

Device Groups tab tasks

Task	Operation
Summary	<p>When a device group is selected, the following information are shown:</p> <ul style="list-style-type: none"> • List of solutions deployed for the device group. • The number of Cloud Solutions Framework (cSF) apps. • The number of discovered, unlicensed, missing, and out-of-policy printers. • 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 associated with the selected group is encrypted. <p>Some of these values are linked to appropriate tasks that let you view more information or change the settings.</p> <p>When All Device Groups is selected in the Device Groups list, the following information for each device group are shown:</p> <ul style="list-style-type: none"> • List of solutions deployed • The number of cSF applications • The number of discovered, unlicensed, missing, and out-of-policy printers • Whether Secure Server Communication is enabled
Name*	Lets you change the unique name for the selected group.
Discovery Profiles*	Lets you add, edit, import, and remove discovery profiles used to discover printers.
Discovery	Finds printers on the network that match the discovery profile for each selected group. For more information, see “Discovering printers” on page 77 .
Discovered Devices	<p>Shows the following information for all printers within selected device groups:</p> <ul style="list-style-type: none"> • Address • Host name • Model • Serial number • Contact name • Contact location • Property tag • Last discovered date • Policy last applied date
Unlicensed Devices	Shows the unlicensed printers within the selected device groups. The table contains the same fields as the Discovered Devices table.
Solutions*	Lets you select solutions to deploy to the printers within the selected group. When the solutions are selected, you can edit local settings for the current device group, and the solutions are deployed using the Policy Update task.
cSF Apps*	<p>Lets you select cSF apps to deploy to the printers within the selected group.</p> <p>cSF apps are custom applications that are deployed from an application server to a supported Lexmark device. For more information, see the <i>Cloud Solutions Framework SDK Developer's Guide</i>.</p>

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

Task	Operation
eSF Configuration*	Lets you edit the settings of eSF applications associated with hybrid solutions deployed to the device group.
Security Setup Files	Lets you manage any printer security setup files within a solution.
Home Screen*	Lets you customize the layout of the home screen for the printers included in the device group. There is a tab for each supported printer class.
Profiles*	Shows the profile settings for the device group for each device class.
Fax Forwarding*	Lets you configure MFPs to forward incoming faxes to a fax number, e-mail address, FTP site, or LDSS. Based on the 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 included in selected device groups.
Out of Policy Devices	Lists all out-of-policy printers in the specified device group. The table contains the same fields as the Discovered Devices table. You can click Update Policy to apply any changes.
Missing Devices	Shows the missing printers in the selected device groups. The table contains the same fields as the Discovered Devices table.
Schedule	Lets you add, edit, and delete Discovery, Policy Update, and script tasks scheduled to run for the selected device group.
Security*	Enables or disables secure communication between the server and the printers in the device group.
* These tasks are not available when All Device Groups is selected.	

Software Client Groups tab tasks

Task	Operation
Summary	When a software client group is selected, the following information are shown: <ul style="list-style-type: none"> • Group name • List of solutions assigned to software client groups When All Software Client Groups is selected, the group names and lists of solutions of all software client groups in the system are shown.
Name*	Lets you change the unique name for the selected group.
Client Profiles*	Lets you add and remove software clients within the selected group.
Solutions*	Lets you add, edit, or delete solutions for software clients within a selected group.
Profiles*	Shows the profile settings for the software client group.
Schedule	Lets you add, edit, and delete script tasks scheduled to run for the selected software client groups.
* These tasks are not available when All Software Client Groups is selected.	

Devices tab tasks

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

Task	Description
Summary	<p>When a device is selected, the following information are shown:</p> <ul style="list-style-type: none"> • Address • Host name • List of device groups to which the device belongs • List of solutions deployed on the device • Model • Serial number • Contact name • Contact location • Property tag • Last discovered date and time • Unlicensed status <p>When multiple devices are selected, a table containing the preceding information for all devices on the network are shown. The total number is shown for Device Groups and Solutions and may be expanded to show the list for each.</p>
Profiles	<p>Shows each profile and the associated settings for a selected device.</p> <p>Note: This task shows only one device at a time. When multiple devices are selected, the first selected device is shown, and other devices may be selected by clicking Next, Previous, or individual page numbers.</p>
Policy Update	Sends policy updates to selected devices.
Missing Devices	Identifies missing devices.
Unlicensed Devices	Identifies unlicensed devices.
Home Screen	<p>Shows the layout of the home screen on a selected device and provides an interface to edit the home screen of an individual device.</p> <p>Note: This task shows only one device at a time. When multiple devices are selected, the first selected device is shown, and other devices may be selected by clicking Next, Previous, or individual page numbers.</p>
Jobs	Shows a sortable table of the jobs for selected devices.
Log	Shows a sortable table of logged messages for selected devices.

Solutions tab tasks

Task	Description
Summary	<p>When a solution is selected, the following information are shown:</p> <ul style="list-style-type: none"> • Solution name • Version number • Installation time • Update time • Lists of device groups and software client groups to which the selected solution is assigned • Lists of formsets, reports, eSF applications, and security setup files included in the solution <p>When All Solutions is selected, a table containing the preceding information for all solutions deployed on the network are shown.</p>
Configuration*	Adjusts the global settings for the selected solution. The parameters are predetermined for each solution.
EForms*	Shows a list of the formsets associated with the selected solution.
eSF*	Shows a list of eSF applications associated with the selected solution.
Jobs*	Shows a table of the jobs that use the selected solution.
Log*	Shows a table of the events and messages generated by the selected solution.
Security Setup Files*	Lets you manage any printer security setup files within a solution.
* This task is not available when All Solutions is selected.	

cSF Apps tab tasks

Task	Description
Summary	<p>When a cSF app is selected in the cSF Apps list, the following information are shown:</p> <ul style="list-style-type: none"> • Solution name • Version number • WebClient version • Installation time • Update time • List of device groups to which the selected solution is assigned <p>When All cSF Apps is selected, a table containing the preceding information for all cSF apps deployed on the network are shown.</p>

E-Forms tab tasks

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

Services tab tasks

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

System tab tasks

Task	Description
System Status	<p>Lists all servers in the system. It also shows the following information for each server:</p> <ul style="list-style-type: none"> • 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 <p>A green arrow beside the Server Address in the table indicates the server where the current LMC session is running.</p> <p>You can also set a server online or offline.</p>
Schedule	Shows all script, report, backup and restore, discovery, and policy update tasks scheduled to run on the system. It also lets you add, edit, and delete scheduled tasks.
Jobs	Shows a sortable table of all pending and completed jobs from all printers within the system.
Log	Shows a sortable table of event messages generated from all pending and completed jobs from all printers within the system.
Reports	Lets you manage and schedule built-in and custom reports.

Task	Description
Username & Password	Lets you set a new 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 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.
Advanced Prompting Bundle (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.
Privileges	Lets you add access control to users. You can assign privileges to users depending on the group to which they belong.
cSF App Certificates	Lets you upload your own security certificate for cSF apps that run on printers in an LDD system. It secures the communication between the cSF apps running on the printer and the LDD system.

Finding basic information

Understanding the Home tab

The Home tab provides shortcuts to tasks on the System tab and individual items on other tabs, as well as indicating the status of each server and device group in the system.

Home tab section	Description
Solutions	Lists all solutions available in the system. Clicking a solution in the list links to that solution on the Solutions tab.
Servers	Lists all servers connected to 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 icon appears on the icon of a device group that contains out-of-policy printers. Clicking a device group in the list links to that device group on the Device Groups tab.
Software Client Groups	Lists all groups of software clients connected to 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	Toggle the message bar by clicking show or hide .
Licenses	Shows the number of licenses available in the system.
Discovered	Shows the number of discovered printers currently stored in the database.
Unlicensed	Shows the number of discovered printers that do not have a license available in the system.
Missing	Shows the number of previously discovered printers that are no longer responding in the network.
Out of Policy	Shows the number of discovered printers known to have settings different from profiles required by solutions deployed to those printers.
System status icon	Indicates the overall status of the system.
Progress bar	Shows the progress of the current operation.

System status information on the status bar and Home tab

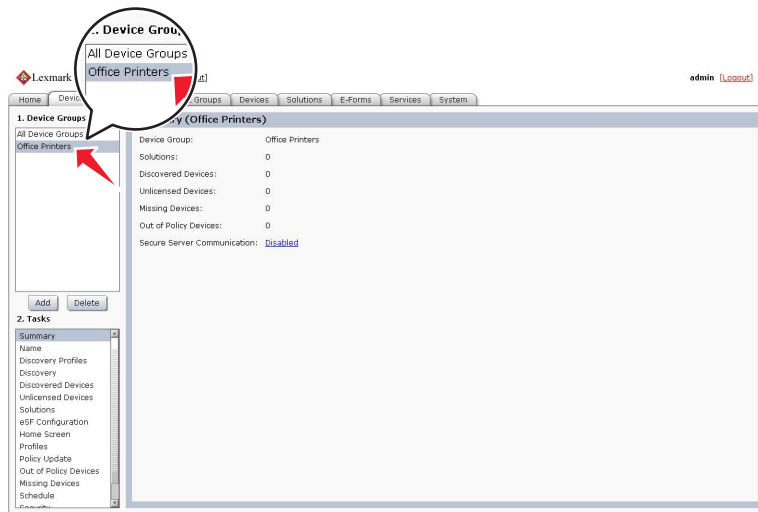
The overall system status is indicated by the icon showing three server boxes in the status bar. If any servers are offline or not communicating, then a yellow exclamation mark icon appears on the system status icon to indicate the system is operating at reduced capacity. If all servers are offline or not communicating, then a red X icon appears on the system status icon.

More detailed system status information is available through the System Status task on the System tab. Click **System Status** in the System section of the Home tab to access this information.

Viewing information summaries for LDD elements

Summaries of essential information are available for device groups, software client groups, printers, and solutions.

- 1 Click the **Device Groups**, **Software Client Groups**, **Devices**, or **Solutions** tab.
- 2 Select an item from the list, or when on the Devices tab, perform a search.



- 3 Click **Summary** from the Tasks list.

A summary of basic information about the selected element appears. The summary includes links to find more information or settings about the included information.

Viewing jobs or system logs

You can view all jobs initiated in the system, including both tasks performed in LMC and print jobs initiated using a printer or software client. Data for both jobs and logs are saved for seven days.

- 1 Click the **System** tab.
- 2 From the System list, select **Jobs** or **Logs**.

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 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 filter the list view to only jobs in progress, click **Running Tasks**.
- To stop a job, 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, set 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 are 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

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 Click the **System** tab.
- 2 Select **Jobs** or **Log**.
- 3 Click **Customize Table**.

All columns are shown by default.
- 4 From the Customize Jobs Table or Customize Log Table, adjust the columns as necessary:
 - To remove a column from view, select it in the Current Columns list, and then click **Remove**.
 - To add a column back to the Current Columns list, select it in the Available Columns list, and then click **Add**.
 - To adjust the position of a column, select it in the Current Columns list, and then click **Move Up** or **Move Down**.
 - To return all columns to view in the default order, click **Reset**.
- 5 Click **OK** to save your changes, or click **Cancel** to keep the current view.

Custom selections for columns are saved in a cookie in your browser so they are available each time you use LMC.

Viewing device group profile settings

- 1 Click the **Device Groups** tab.
- 2 Select a device group from the Device Groups list.
- 3 Select **Profiles** from the Tasks list.
- 4 In the main section, select the desired Device Class tab.
- 5 Select a profile name to display the settings.

Viewing software client group profiles

- 1 Click the **Software Client Groups** tab.
- 2 Select a software client group from the Software Client Groups list.
- 3 Select **Profiles** from the Tasks list.

Viewing forms associated with a solution

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

- 1 Click the **Solutions** tab.
- 2 Select a solution from the Solutions list.
- 3 Select **EForms** from the Tasks list.

Viewing version information

You can view version numbers for all system components, which may help you to troubleshoot problems and make sure all components are up to date.

- 1 Click the **System** tab.
- 2 Select **System Status** from the System list.
- 3 In the Components column, click **Version Info**. You may have to scroll to the right to see the Components column.

To export component version information along with system status information, click **Export Report** in the System Status window.

Managing the LDD system

To perform system tasks, such as creating reports on the overall performance of the system, setting servers offline, changing the administrative user name and password, or viewing the overall job schedule, use the System tab in LMC.

Viewing and changing server status

To view server status, click the **System** tab, and then select **System Status** from the System list.

A table is displayed 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 icon appears beside the status when the server is offline, and a red X icon appears to indicate a communication problem.

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

The server on which the current LMC session is running is indicated by a green arrow beside the Server Address.

You can perform the following tasks:

- To change the online status of a server, select the check box of a server from the table, and then click **Set Online** or **Set Offline**.
- To export all system status information and component version information, click **Export Report**.
- To remove a server that is not communicating, select the check box beside it in the table, and then click **Remove Server(s)**. If the server later reestablishes communication, it automatically reappears in the server list.

Viewing and managing scheduled tasks

To access a list of all scheduled discovery, policy update, and script tasks for all device groups and software client groups, select **Schedule** from the System list on the System tab.

From this list, you can perform the following actions:

- **Add a new task**—Click **Add**.
- **Edit an existing task**—Select the existing scheduled task you want to edit, and then click **Edit**.
Note: You cannot change the task type for an existing task.
- **Delete an existing task**—Select the existing scheduled task you want to delete, and then click **Delete**.

Do the following when adding or editing a task:

- 1 If you are adding a new task, then select a task to schedule.
- 2 Edit the description of the task, and then click **Next**.
- 3 If you are adding or editing a script task, then select whether to associate the scheduled script with a device group or software client group to access the local solution settings of that group:
 - To associate the script with a device group, click **DeviceGroup**, and then click **Next**.
 - To associate the script with a software client group, click **SftClientGroup**, and then click **Next**.
 - To schedule the script without associating it with a device group or software client group, click **None**, and then click **Next**.
- 4 Continue configuring the selected task:
 - If you are adding or editing a discovery or policy update task, then select the device groups for which the task is performed, and then click **Next**.
 - If you are adding or editing a script task, then do the following:
 - a Select the device group or software client group for which the task is performed, and then click **Next**.
Note: You can only select one device group or software client group for a script task.
 - b Select the solution that contains the script you want to run.
 - c Select the script to run, and then click **Next**.
 - If you are adding or editing a report task, then select and configure the report to run, and then click **Next**.
 - If you are adding or editing a backup and restore task, then type the Backup Share Path and the credentials required to access the specified share, and then click **Next**.
- 5 Configure the date, time, and frequency information for the task.
- 6 Click **Finish**.

Configuring the confirmation page

When a job is completed, a confirmation is automatically delivered through a printout or e-mail message unless it is disabled within a particular solution. These settings determine the type of confirmation, how it appears, and, if it is an e-mail message, to whom it is sent.

- 1 Click the **Services** tab.
- 2 Select **Confirm** from the Services list.

- 3 Select **Parameters** from the Tasks list.
 - 4 Select the lowest level of messages to include in confirmations:
 - **debug**—This includes detailed messages used to diagnose problems, as well as other lower message levels than this level.
 - **info**—This includes messages that indicate successful job activities, as well as other lower message levels than this level.
 - **warn**—This includes messages that indicate potential problems, as well as other lower message levels than this level.
 - **error**—This includes messages that indicate unsuccessful job activities, as well as other lower message levels than this level.
 - **fatal**—This includes only messages that indicate complete failure of jobs.
 - 5 Select a task from the “Task used to deliver confirmation page” list:
 - **confirm.printPS**—This prints a confirmation page in PostScript format.
 - **confirm.printPDF**—This prints a confirmation page in PDF format.
 - **confirm.emailAdmin**—This sends a message to the administrator e-mail address with a PDF confirmation page attached.
 - **confirm.emailAdminTextOnly**—This sends a message containing the confirmation information to the administrator e-mail address with no attachments.
- Note:** The e-mail service must be correctly configured to use `confirm.emailAdmin` or `confirm.emailAdminTextOnly`.
- 6 If you are using e-mail confirmations, then type the address where e-mail confirmations are sent in the “Admin email address” field.
 - 7 Type a page title to appear on the confirmation page or message.
 - 8 Edit the remaining parameters to determine the font settings for the title and page text.
 - 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 already has solutions, the solutions and all associated settings are added to the new server. However, any third-party services used with existing solutions must be installed manually. If the new server is left without the same services as existing servers, any jobs that use the solution that is missing services on the new server will fail.

- 1 Add the computer where the server will be installed on the network, and make sure the time is synchronized using an NTP server.
- 2 Install the server. For more information, see [“Installing servers” on page 27](#).
- 3 Install any third-party services required by existing solutions on the new server.
- 4 From the System tab in LMC, set the new server online. For more information, see [“Viewing and changing server status” on page 47](#).

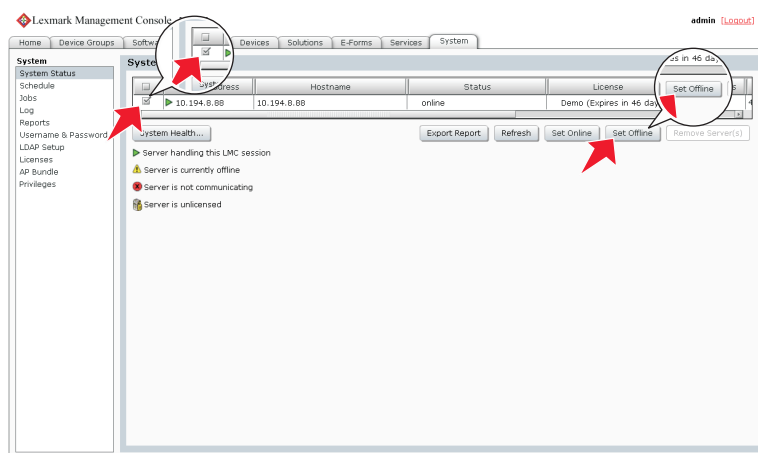
Changing the IP address on a configuration 1 system

If an incorrect IP address or fully qualified domain name is used when installing a configuration 1 system, or the IP address of the computer on which the components of a configuration 1 system are installed changes for any reason, then the IP address of the components can be changed without reinstallation.

- 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. (The default is C:\Program Files\Lexmark\Solutions\InstallHelper.)
- 2 Type **update-addr.bat -hostname** to use the fully qualified domain name of the local computer, and then press **Enter**
or
Type **update-addr.bat -ip** to use the IP address of the local computer, and then press **Enter**.
- 3 The desktop shortcut must be changed to the new address manually:
 - a On the desktop of the computer where the components are installed, right click the **Lexmark Management Console (LMC)** icon, and then click **Properties**.
 - b Click **Find Target**.
 - c In the folder that appears, right click the shortcut **lmc**, and then click **Properties**.
 - d Change the IP address or host name part of the URL to the new IP address or host name of the local computer. The complete URL should be **http://hostname:9780/lmc/**, where *hostname* is the host name or IP address of the computer where the components are installed.

Rebooting the LDD system

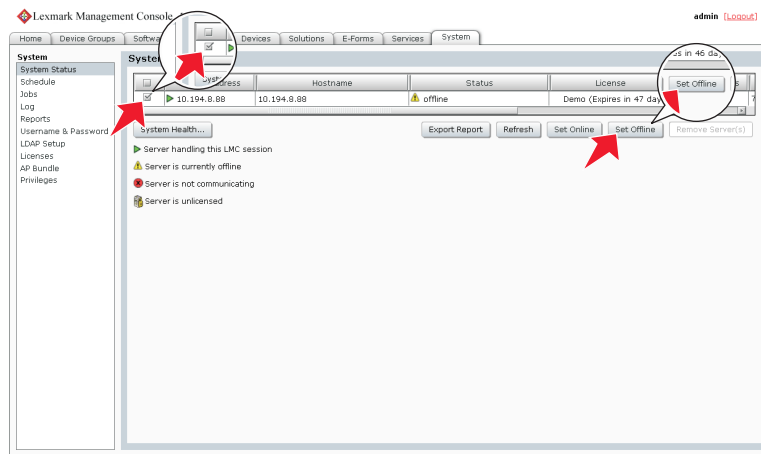
- 1 Click the **System** tab.
- 2 Set all servers offline. For more information, see [“Viewing and changing server status” on page 47](#).



- 3 Shut down all server computers, load balancer computers, and database computers.
- 4 Boot the database computers, load balancer computers, and server computers.

Note: You can boot the server components in any order.

- 5 From the System tab in LMC, set all servers online. For more information, see [“Viewing and changing server status” on page 47](#).



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

Restarting the Lexmark Solutions Application Server

If you install a workflow solution that includes a component, then you may need to restart the Lexmark Solutions Application Server for the solution to fully function.

Before restarting the Lexmark Solutions Application Server, set the server offline on the System tab in LMC. Make sure the server is offline before proceeding. Click **Refresh**, and then make sure **offline** is reported in the Status column for the server.

You can restart the Lexmark Solutions Application Server from the Windows Services control panel.

Note: When you restart the Lexmark Solutions Application Server service, any solution-related file in the \Lexmark\Solutions\apps\wf-ldss\ or \Lexmark\Solutions\apps\wf-ldss\solutions folders, such as a property file for a solution, is reverted to the version stored with the solution package as it was initially installed or upgraded, and any manual changes are lost.

Uninstalling LDD components

- 1 Click the **System** tab.
- 2 From the System list, select **System Status**.
- 3 Set all servers offline. For more information, see [“Viewing and changing server status” on page 47](#).

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 in each cluster, close all unnecessary applications. Make sure that no applications 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, in the Start menu or Apps list, open the Lexmark folder, and then launch **Uninstall Lexmark Document Distributor**.

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 e-Task 5, e-Task 4, e-Task 3, e-Task 2+, and e-Task 2 MFPs and SFPs, and X642 printers. 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 Click the **System** tab.
- 2 From the System list, select **AP Bundle**.
- 3 Beside AP Bundle Application File, click **Browse**, and then locate the file ap-x.x.x.x.flc.
- 4 Beside AP Bundle Descriptor File, click **Browse**, and then locate the file ap-x.x.x.x_desc.xml.

Notes:

- To update the AP Bundle, the descriptor file is required.
- You can change the default settings of the AP Bundle on e-Task 2+ printers by editing the value attributes of the property elements in the descriptor file. Adding or removing settings in the descriptor file does not affect the application.

- 5 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.

Managing system performance

Accessing the System Health dashboard

- 1 Click the **System** tab.
- 2 Select **System Status** from the System list, and then click **System Health**.

Monitoring system health

The overall system health is shown on the top section of the page by the following indicators:

- **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.

- **Tasks / 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, in 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 / hour**—Shows the hourly rate of overload events. An overload event occurs when the number of tasks exceed the configured design load and ends when the number of tasks reaches the configured recover load.

Note: For more information about design load and recover load, see [“Tuning the load balancer for unequal servers” on page 54](#).

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 / hour**—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 zoom in any of the performance graphs in the Server Health section, click the graph. Click the graph again to return to the view of all graphs.

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 slider controls at the bottom of the page are used to tune system performance. For more information, see [“Tuning the load balancer for unequal servers” on page 54](#) and [“Adjusting limits on concurrent jobs” on page 53](#).

Adjusting limits on concurrent jobs

A server that meets recommended requirements is tested to 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 Click the **System** tab.
- 2 From the System list, select **System Status**.

3 Click **System Health**.

4 In the Server Health section, select a server address.

5 Adjust the Concurrently Running Task Limit slider to the preferred limit for the server.

6 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

When all servers in the system are approximately equal, server loads should be optimal without manually tuning the load balancer. If servers are unequal, then the least powerful machine determines the overall throughput unless you compensate by manually assigning a load balancing factor to each server. Because more powerful machines run and complete each concurrent job in less time, routing more traffic to them increases the overall job capacity of the system.

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.

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

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

The ideal job distribution depends on the hardware, network environment, and the solution being run. The optimal proportions for load balancing factors can be found by running 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 Click the **System** tab.

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

3 Click **System Health**.

4 In the Server Health section, select a server address.

5 Adjust the Load Factor slider to the preferred load balancing factor for the server.

6 Click **Apply**.

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

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 all servers are separated in this manner, assigning only one server to run LMC is adequate.

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

- Install the server component on the RAID 1 array where the operating system is installed on the load balancer computer, and configure it to run LMC only.
 - Configure the servers installed on dedicated computers to only process jobs.
- 1** From your web browser, launch JK Status Manager using the URL **`http://loadbalancer:9780/status/?opt=454`**, where **`loadbalancer`** is the computer where your 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 should only process jobs, stop the associated worker on the adminloadbalancer load balancing worker, which balances requests to LMC:
 - a** In the “Worker Status for adminloadbalancer” section, click **E** beside the server name.
 - b** For Activation, select **Stopped**.
 - c** Click **Update Worker**.
 - 3** For each server that should run LMC only, stop the associated worker on the clientloadbalancer and adaptorloadbalancer load balancing workers, which balance job requests:
 - a** In the “Worker Status for clientloadbalancer” section, click **E** beside the server name.
 - b** For Activation, select **Stopped**.
 - c** Click **Update Worker**.
 - d** Repeat these steps for the same server in the “Worker Status for adaptorbalancer” section.

Notes:

- Make sure that at least one server is assigned to run LMC and at least one server is assigned to process jobs.
- Changing other load balancer and server properties is not recommended.

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** Click the **Services** tab.
- 2** Select **General** from the Services list.
- 3** Select **Parameters** from the Tasks list.
- 4** In the ChunkSize field, type a new value. When using three or more servers, a value as low as **2** may be appropriate.
- 5** Click **Apply**.

Configuring communications

Configuring connection to an SMTP server

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

Configuring NPA device communication

Though the default port is usually used for NPA device communication, the timeout periods between retries can be changed to improve reliability during device discovery.

- 1 Click the **Services** tab.
- 2 Select **NPA** from the Services list.
- 3 Select **Parameters** from the Tasks list.
- 4 Type the port number used for NPA on your network in the Unsecure Port field. The default setting is 9300.
- 5 Type a timeout period in milliseconds for each retry in sequence, separating each by a space in the NPANT Timeout field. The default settings are 1000 and 5000.
- 6 Click **Apply**.

Configuring SNMP for discovering printers

- 1 Click the **Services** tab.
- 2 Select **SNMP** from the Services list.
- 3 Select **Parameters** from the Tasks list.
- 4 In the Port field, type the port number used for SNMP on your network. The default is 161.
- 5 In the Write Community Name field, type the write community string for printers on your network.
- 6 In the Timeouts/Retries field, type a timeout period in milliseconds for each retry in sequence, separating each by a space.
- 7 In the Read Community Name field, type the read community string for printers on your network.
- 8 Click **Apply**.

Configuring device security

To enable communication with Basic Security template–enabled devices, make sure the Basic Security template matches the authentication type and the password or PIN configured in LMC. Only authentication through password or PIN is supported.

- 1 Click the **Services** tab.
- 2 Select **DeviceSecurity** from the Services list.
- 3 Select **Parameters** from the Tasks list.
- 4 Select the type of authentication for the device, and then type the password or PIN.
- 5 Click **Apply**.

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 Click the **System** tab.
- 2 From the System list, select **Licenses**.
- 3 Click **Add License**.
- 4 Browse to the license file, and then click **Upload**.

Note: Uploading license files copies them to the program folder. You can safely move the license files from the temporary location where you saved them.

Managing reports



Running a report

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

- 1 Click the **System** tab.
- 2 From the System list, select **Reports**.
- 3 From the Available Reports list, select a report.
- 4 Specify the reporting period.
- 5 From the Output Format drop-down menu, select an output format.

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

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

- To save the report, do the following:
 - a** Select **Save To**.
 - b** Click  beside the Save To field.
 - c** Type a destination folder path using either a local drive letter or a UNC path for a shared folder.
 - d** If the folder is on a shared folder that requires authentication, then type your shared folder credentials.
 - e** Click **OK**.
- To send the report in an e-mail, do the following:
 - a** Select **Email To**.
 - b** Click  beside the Email To field.
 - c** If necessary, edit the e-mail, and then click **OK**.

7 If other query parameters are available for the selected report, then click **Additional Parameters** to specify values for those parameters. If there are no other available parameters, then the button is disabled.

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*.

8 Click **Run Report**.

The report is shown in a new window and may be saved to a file or sent in an e-mail.

Notes:

- Only summary reports are supported. Even if a custom report has a detail section defined, the section is not shown. 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** Click the **System** tab.
- 2** From the System list, select **Schedule**.
- 3** Click **Add > Report**.

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 the developer of your solution.

- 4** Type a description for the task, and then click **Next**.
- 5** Select and configure the scheduled report. Do the following:
 - a** From the Available Reports list, select a report.
 - b** Select a reporting period.
 - c** From the Output Format drop-down menu, select an output format.

Note: Each report has a default Output Format. For more information about a custom report, contact the designer of your custom report.

d Save the report or send it in an e-mail:

- To save the report, do the following:
 - 1** Select **Save To**.
 - 2** Click  beside the Save To field.
 - 3** Type a destination folder path using either a local drive letter or a UNC path for a shared folder.
 - 4** If the folder is on a shared folder that requires authentication, then type your shared folder credentials.
 - 5** Click **OK**.
- To send the report in an e-mail:
 - 1** Select **Save To**.
 - 2** Click  beside the Email To field.
 - 3** If necessary, edit the e-mail, and then click **OK**.

e If other query parameters are available for the selected report, then click **Additional Parameters** to specify values for those parameters. If there are no other available parameters, then the button is disabled.

6 Click **Next**.

7 Enter a start date and a start time.

8 Configure the frequency of the scheduled event, and then click **Finish**.

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. Even if a custom report has a detail section defined, the section will not be displayed. If a custom report does not have a summary section, then any reports generated from the custom report will be blank.

- 1 Click the **System** tab.
 - 2 Click **Reports** in the System list.
 - 3 Upload the report files:
 - a Click **Upload Report Files > Browse**.
 - b Select a .jasper compiled report file, as well as any of the following:
 - .jasper compiled report files used as subreports
 - .jpg or .png graphics included in the report
 - .jrxml report source files (optional)
 - c Click **Open**.
 - d Existing files are overwritten by default. If you do not want to overwrite existing files, then clear the **Overwrite if file already exists** check box.
 - e Click **Upload**.

Selected files are copied to the folder \Lexmark\Solutions\apps\wf-Idss\WEB-INF\reports\ where the system is installed on each server.
 - 4 Below the Available Reports list, click **Add**.
 - 5 Type a descriptive report name.
 - 6 Select the Jasper report file name for the compiled report you uploaded.
 - 7 Select the database the report was designed to access from the Datasource drop-down menu. Commonly used databases include:
 - **MONITOR**—This is used by reports that access the jobs list and the log.
 - **SOLUTIONINFO**—This is used by some solutions to store custom data.
- For more information about a custom report, contact the designer of your custom report.

- 8 Select the default output format.

Note: Each report has a default selection for output format, which may be the format that the report was specifically designed to use. For more information about a custom report, contact the designer of your custom report.

- 9 Click **Save**.

Editing report settings

- 1 Click the **System** tab.
- 2 Click **Reports** in the System list.
- 3 Select a report from the Available Reports list, and then click **Edit**.

- 4 Edit the report settings as necessary:

- Type a descriptive report name.
- Select the Jasper report file name for a compiled report that has been uploaded to the system.
- Select the data source.
- Select the default output format.

Note: Each report has a default selection for output format, which may be the format the report was specifically designed to use. For more information about a custom report, contact the designer of your custom report.

- 5 Click **Save**.

Removing a report

To remove a report, from the Available Reports list, select a report, and then click **Delete**.

Note: Removing a report automatically removes any associated scheduled report tasks. However, any scheduled script tasks that use the report are not detected and must be removed 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 where LDD is installed on each server.

Configuring default report options

You can configure default report options, such as default e-mail or file destination and default reporting period.

Select the **Reports** service from the Services tab.

Clicking **Refresh Defaults** while configuring a report returns settings to defaults.

Creating custom reports

LDD uses JasperReports for custom reports. You can create custom reports using the open-source application iReport 3.5.2, available from jasperforge.org/ireport. For more information about overall report design, see the documentation for iReport.

Note: Only summary reports are supported. Even if a custom report has a detail section defined, the section is not shown. If a custom report does not have a summary section, then the finished report is blank.

Using special LDD parameters

You can add the following parameters to the report design in order to use the specified information in other parts of the report:

- **start_date**—This retrieves the start date for report data, as specified in a script or by the administrator when the report is run.
- **end_date**—This retrieves the end date for report data, as specified in a script or by the administrator when the report is run.
- **SUBREPORT_DIR**—This retrieves the reports folder, located at \Lexmark\Solutions\apps\wf-ldss\WEB-INF\reports\ where LDD is installed on each server, from the LDD installation in order to locate subreport files.

Note: Additional parameters can only be added when a report is developed and uploaded with a solution using the SDK. 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 as follows:

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

Information that appears in the log is available from the TASK_LOG table in the MONITOR database. It contains the following fields:

- **ID**—A unique ID number assigned to each entry in the log.
- **LOG_TIME**—The time when an entry was 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 assigned to a task. Each entry recorded from the same task has the same TASK_ID.

Information from the Jobs list is available from the TASK_INFO table in the MONITOR database. It contains the following fields:

- **TASK_ID**—The unique ID number assigned to the task.
- **HOST_NAME**—The host name of the server where the job was run.
- **TASK_NAME**—The name of the task.
- **SOLUTION_NAME**—The name of the solution where the task was run.

- **STATUS**—The status reported when the job was completed or abandoned.
- **START_TIME**—The time when the job was received.
- **END_TIME**—The time when the job was completed or abandoned.
- **PERCENT_COMPLETE**—The progress reported by the job when it was completed or abandoned.
- **USER_ID**—The user who submitted the job (if applicable).
- **PRINTER**—The address of the printer or software client that submitted the job (if applicable).
- **ADDRESS**—The unique ID number of a printer.
- **SCHEDULE_ID**—The ID for the scheduled task that ran (if applicable).
- **PARENT_ID**—The task ID of the previous task that started the listed task (if applicable).
- **THREAD_NAME**—The name of the thread 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 included subreports may be useful in developing custom reports. Because these files are included with the installation, uploading them is not necessary before adding a form that includes any of the subreports.

When using a subreport in a custom report, pass the **start_date**, **end_date**, and **SUBREPORT_DIR** to the subreport using the Parameters property of the subreport element.

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 no data was found within the selected period. Note: By default, iReport does not generate a report if no data is found. To use a No Data node, change the setting for when no data is found in the report from No Pages selection to No Data Section.
_landscape_no_data_message.jasper	Landscape	
_Printers_Least_Used	Either	Shows the printers least used to submit jobs.
_Printer_Models_Most_Used	Either	Shows the printer models most used to submit jobs.
_Printers_Most_Used	Either	Shows the printers most used to submit jobs.
_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 should be run.

File name	Page orientation	Description
_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 are most run by scheduled tasks.
_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 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. In the event a recovery is necessary, a new system can access the recovery data 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 validates backup database files on the network folder. The system also sends an e-mail message that indicates success or failure to the address specified for the “Admin email address” setting of the Confirm service. Failures are also recorded in the system log.

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

- 1 Click the **System** tab.
- 2 From the System list, 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 should be backed up.
For example, `\\myserver\myshare\`.
Note: When storing backup data from multiple LDD systems, make sure to 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 from 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 Enter a start date and a start time.
- 11 Configure the frequency of the scheduled event, and then 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:
 - If a workgroup system has failed, then perform a workgroup installation.
 - If both the database and load balancer or only the database has failed in an enterprise system, then install the database.
 - If only the load balancer has failed in an enterprise system, then install the load balancer.
- 2 Before proceeding to the final step of each installation, select **Restore Install (RI)**, and then specify or locate the .ri file.
- 3 Follow the instructions on the screen.
- 4 If you are using an enterprise system and you 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 66](#).
 - If you are using existing servers, then see [“Connecting existing servers during recovery” on page 66](#).

- 6 If a new IP address or fully qualified domain name 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 an address change” on page 67](#).
 - b Change settings for any associated eSF applications that specify the load balancer address using the eSF Configuration task on the Device Groups tab in LMC. For more information, see [“Configuring an eSF application associated with a solution” on page 71](#).

Installing new servers during recovery

- 1 On computers where you want to install servers, make sure the time is synchronized with existing system components using an NTP server.
- 2 Perform server installations using the new database and/or load balancer. For more information, see [“Installing servers” on page 27](#).
- 3 Install any third-party services required by installed solutions on each new server.
- 4 Perform policy updates as necessary:
 - If the new database and load balancer are identified by the same IP address(es) and fully qualified domain name(s) as the failed database and/or load balancer, then perform a policy update for any device groups that contain e-Task printers, making sure to clear the **Only update those devices which are Out of Policy** check box.
 - If the backup database or load balancer is identified by a new IP address or fully qualified domain name, then perform a policy update for all device groups, making sure to clear the **Only update those devices which are Out of Policy** check box.
- 5 From the System tab in LMC, set the new servers online. For more information, see [“Viewing and changing server status” on page 47](#).
- 6 If new servers are identified by different addresses than the failed servers, then the failed servers remain in the system and appear as non-communicating on the System Status page. To avoid affecting system performance, remove these servers from the System tab in LMC.

Connecting existing servers during recovery

Do the following after the database or load balancer is recovered:

- If the new database and load balancer are identified by the same IP address(es) and fully qualified domain name(s) as the failed database and/or load balancer, then do the following:
 - 1 Make sure the time is synchronized among all system components using an NTP server.
 - 2 Restart the Lexmark Solutions Application Server service from the Windows Services control panel on each server.
 - 3 Perform a policy update for any device groups that contain e-Task printers, making sure to clear the **Only update those devices which are Out of Policy** check box.
 - 4 From the System tab in LMC, set the servers online. For more information, see [“Viewing and changing server status” on page 47](#).
- If the new database or load balancer is identified by a new IP address or fully qualified domain name, then do the following on each server:
 - 1 Make sure the time is synchronized among all system components using an NTP server.
 - 2 From the Services control panel, stop the Lexmark Solutions Application Server service.

- 3 In the file \Lexmark\Solutions\apps\wf-ldss\WEB-INF\classes\adaptor.properties where the server is installed, change each of the properties **adaptor.address** and **adaptor.canonicalhostname** to the IP address or fully qualified domain name of the new load balancer.

Note: If the setting is currently an IP address, then use the IP address of the load balancer. Likewise, if the setting is currently a fully qualified domain name, then use the fully qualified domain name of the load balancer.

- 4 Change the URL for the desktop shortcut to LMC on the server:
 - a In the folder \Lexmark\Solutions\apps\wf-ldss\, right click the shortcut **lmc**, and then click **Properties**.
 - b Change the IP address or host name part of the URL to the new IP address or host name of the new load balancer. The complete URL should be **http://hostname:9780/lmc/**, where *hostname* is the host name or IP address of the new load balancer.
- 5 If you are using a new database, then locate the file \Lexmark\Solutions\apps\wf-ldss\WEB-INF\classes\database.properties where the server is installed, and then change the property **database.hostname** to the fully qualified domain name of the new database.

Note: If you are using an IP address for this setting because the network does not have a reliable DNS, then you can use the IP address of the new database.
- 6 From the Services control panel, start the Lexmark Solutions Application Server service.
- 7 Perform a policy update for all device groups, making sure to clear the **Only update those devices which are Out of Policy** check box.
- 8 From the System tab in LMC, set the servers online. For more information, see [“Viewing and changing server status” on page 47](#).

Recreating LDD printer ports after an address change

If the new load balancer is identified by a new IP address or fully qualified domain name after a recovery, then you must recreate any LDD printer ports on software clients.

- 1 In the printers control panel in Windows, right-click an LDD print queue, and then click **Properties**.

Note: For more information about accessing the properties for the Lexmark Document Server port, see [“Configuring a Lexmark Document Server port” on page 94](#).
- 2 Click the **Ports** tab > **Add Port** > **Lexmark Document Server Port - Enterprise** > **New Port**.

Note: The port name must be 75 characters or fewer.
- 3 Add the new Lexmark Document Server:
 - a Click **Manage List**.
 - b From the Server Setup dialog, click **Add**.
 - c Type the fully qualified domain name or IP address of the load balancer, and then click **OK**.
 - d Select the old load balancer from the list, then click **Remove**, and then click **Yes** to confirm removal.
 - e Click **OK** to exit the Server Setup dialog.
- 4 Make sure the new server is selected from the Document Server list, and then click **Next**.
- 5 Select a profile on the server to use with the new port, and then click **Next**.

Note: If the server is currently running a large number of jobs, then profiles on the server may not appear in the list. Wait until the server is not as busy, and then try adding the port again.

- 6 Click **Finish** to add the new port.
- 7 If you are using pooled ports, then add additional ports using the same server and profile.
- 8 If the Printer Ports dialog is still open, then click **Close**.
- 9 Make sure only newly created ports are selected, and then click **Apply**.
- 10 Do the following for each port associated with the failed load balancer:
 - a Select the port from the list.
 - b Click **Delete**, and then click **Yes** to confirm deletion.

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

Manually backing up databases

You can back up the LDD databases 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, should be included in the backup:

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

The user name for each database is **framework**, and the password is **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, which uses the extension **.fbk**.

Managing solutions and cSF apps

Understanding the deployment process

- 1 Set servers offline to prevent execution of profiles before configuration is complete. For more information, see [“Viewing and changing server status” on page 47](#).
- 2 Upload the solution or cSF app to the system and adjust global settings for the solution.
- 3 Create a device group to contain printers where the solution or cSF app will be deployed.
Note: Multifunction and single-function printers are known as *devices* in LMC.
- 4 Create discovery profiles to add printers to the device group.
- 5 Discover printers in the device group according to the discovery profiles.
- 6 Add the solution or cSF app to the device group and adjust local settings, if necessary.
- 7 Configure home screens for the device group to use the deployed solution or cSF app.
- 8 Update the device policies for the printers in the device group.
- 9 Set servers online. For more information, see [“Viewing and changing server status” on page 47](#).

Each step is covered in more detail in the following sections.

Note: Some solutions or cSF apps may automatically complete any or all of steps 3 through 8 if the creator of the solution or cSF apps included auto-configure. For more information, see the documentation associated with a specific solution.

Understanding solution or cSF app settings

Setting type	Location in LMC		Initial configuration	Scope
	Solution	cSF app		
Global	Configuration task on the Solutions tab	<ol style="list-style-type: none"> 1 Click the cSF App tab. 2 Click the checkbox by every cSF app. 3 Click Config Service, and then click Yes. 	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
Local	Solutions task on the Device Groups or Software Client Groups tab (Select a solution, and then click Edit .)	N/A	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 Click the **Solutions** tab.
- 2 From the Solutions list, select **All Solutions**.
- 3 Click **Install/Upgrade**.
- 4 Type the path to the solution file, or browse to the solution file.
- 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 policy updates for the associated device groups. For more information, see [“Viewing and changing server status” on page 47](#).
- If you install a workflow solution that includes a component, then restart the Lexmark Solutions Application Server service for the solution to function.
- Remove all solutions from home screens, device groups, and software client groups before removing them from the system. For more information, see [“Removing solutions or cSF apps” on page 72](#).
- You can upload a solution to the LDD system directly from the Eclipse software by adding the solution to the LDD 4.x System list. For more information, see the *Lexmark Document Distributor SDK Guide*.

Configuring global settings

Configuring global solution settings

- 1 Click the **Solutions** tab.
- 2 Select a solution name from the list.
- 3 Select **Configuration** from the Tasks list.
- 4 Adjust the settings for the solution as needed. For more information, see the documentation that came with the solution.

Note: When updating the shortcut number of a profile, make sure to match it with the shortcut number in the Home Screen settings. For more information on configuring the home screen, see [“Customizing the home screen for a device group” on page 79](#).

- 5 Click **Apply**.

Configuring global cSF app settings

- 1 Click the **cSF Apps** tab.
- 2 Select **All cSF Apps**, and then check the checkbox next to the cSF app that you want to configure.

- 3 Click **Config Service**, and then click **Yes**.
- 4 Adjust the settings for the cSF app as needed.

Note: When updating the shortcut number of a profile, make sure to match it with the shortcut number in the Home Screen settings. For more information on configuring the home screen, see [“Customizing the home screen for a device group” on page 79](#).

Editing local settings for a deployed or assigned solution

Local settings are configured during deployment or assignment of a solution.

- 1 Select a group:
 - a Click the **Device Groups** tab.
 - b Select a device group from the Device Groups list.or
 - a Click the **Software Client Groups** tab.
 - b Select a software client group from the Software Client Groups list.
- 2 Select **Solutions** from the Tasks list.
- 3 Select a solution from the list in the main section, and then click **Edit**.
- 4 Configure the deployment settings of the solution for the current device group, and then click **Finish**.

Note: A policy update is required after changing settings that affect a device group. For more information see [“Updating policies for device groups” on page 83](#).

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 applications, which are similar to local solution settings.

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

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

Note: If you are configuring advanced prompt, then make sure to select **ALL** to install the AP Bundle in all printers running the LDD solution.

- 7 Configure the settings.
- 8 Click **Save Settings**.

Note: A policy update is required after changing the eSF application settings for a device group. For more information, see [“Updating policies for device groups” on page 83](#).

Managing solution-related files

Some solutions may include properties files or other associated files.

Files associated with only a single solution are located in the \Lexmark\Solutions\apps\wf-Idss\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-Idss\ folder where each server is installed.

For more information, contact the developer of your solution.

Note: If you restart the Lexmark Solutions Application Server service, then any solution-related file is reverted to the version stored with the solution package as it was initially installed or upgraded, and any manual changes are lost.

Removing solutions or cSF apps

Removing home screen buttons for the solution or cSF app

- 1 Click the **Device Groups** tab.
- 2 From the Device Groups list, select a device group where a home screen button is assigned to the solution or cSF app.
- 3 From the Tasks list, select **Home Screen**.
- 4 Click the tab for each device class with a button assigned to the solution or cSF app, and then do the following:
 - a In the Layout menu, select a button.
 - b From the Action list, select **None**.
 - c Click **Apply**.

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

Deleting the solution or cSF app from device groups or software client groups

- 1 Click the **Device Groups** tab.
- 2 From the Device Groups list, select a device group where the solution or cSF app has been deployed.
- 3 From the Tasks list, select **Solutions** or **cSF Apps**.
- 4 Select the solution or cSF app.
- 5 Click **Delete**.

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

Removing the solution or cSF app from the system

- 1** Click the **Solutions** or **cSF Apps** tab.
- 2** From the Solutions list or cSF Apps list, select **All Solutions** or **All cSF Apps**.
- 3** From the summary list, select the solution or cSF app.
- 4** Click **Remove**.

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

Notes:

- Forms may be shared among solutions, and removing forms that are used by any remaining solutions stops those solutions from working correctly.
- Removing a solution removes any associated scheduled tasks automatically.

Managing device groups and devices

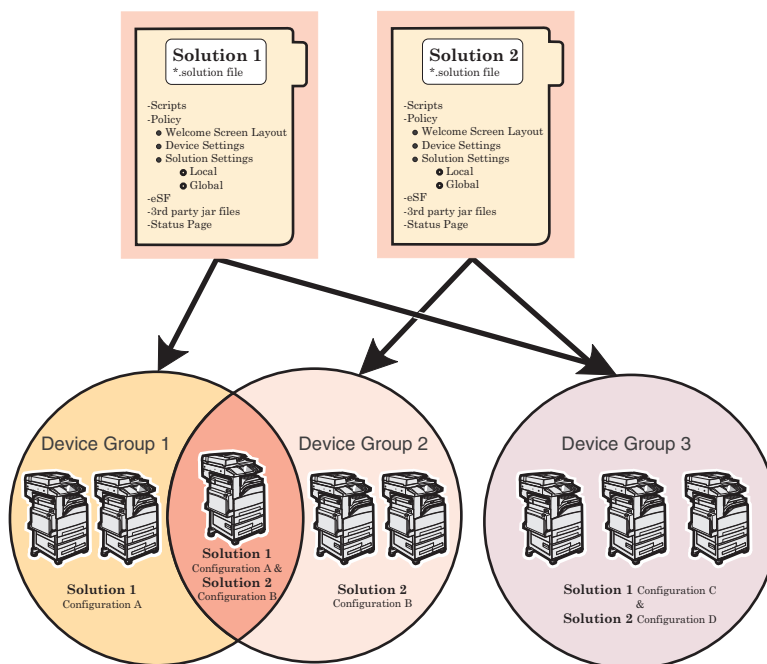
Creating and populating device groups

Understanding device groups

A *device group* is a collection of printers that share one or more solution deployments with the same local configuration. At least one device group must be created to deploy solutions. Multiple device groups should be created if either more than one solution is deployed to different sets of printers or one solution is deployed with different local configurations for different printers.

Note: Printers are known as devices in LMC.

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



Creating a device group

- 1 Click the **Device Groups** tab.
- 2 Under the Device Groups list, click the **Add** button.
- 3 Type a unique name for the device group, and then click **Add**.

Creating a device group from an existing device group

- 1 Click the **Device Groups** tab.
- 2 Under the Device Groups list, click **Add**.

- 3 Type a unique name for the new device group.
- 4 Select the existing group to copy, and then click **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 Click the **Services** tab.
- 2 Select **PolicyUpdate** from the Services list.
- 3 If necessary, select **Parameters** from the Tasks list.
- 4 Type a timeout period in seconds for each device during a policy update.

The timeout setting for the PolicyUpdate service determines how long the system waits for a printer to respond after it is initially connected during a policy update.

Note: If a large eSF application or several eSF applications are included with a hybrid solution, then you may need to increase the default timeout for policy updates in order to allow enough time for policy updates that include eSF application deployments to complete.

- 5 Select the **Overwrite all function overrides on the device** check box.

Note: If there are eSF applications installed on the device that can override the device function, then clear the **Overwrite all function overrides on the device** check box. Otherwise, this setting should be selected at all times.

- 6 Click **Apply**.

Creating a new discovery profile

- 1 Click the **Device Groups** tab.
- 2 Select a device group from the Device Groups list.
- 3 Select **Discovery Profiles** from the Tasks list.
- 4 Type the IP address, address range, subnet, host name, or fully qualified domain name in the Address field.

Address format	Example
IP address	10.10.2.100
IP address range	10.10.2.1-10.10.2.127
Subnet	10.10.2.*
Host name	printer-host-name

Address format	Example
Fully qualified domain name	printer-host-name.domain-name

5 Type information in the remaining fields for any optional filters.

6 Click **Add** in the main section to save the discovery profile.

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 Click the **Device Groups** tab

2 Select a device group from the Device Groups list.

3 Select **Discovery Profiles** from the Tasks list.

4 Click **Import**.

5 Type the path of the file, or click **Browse**, and then locate the file.

6 Click **Upload**.

The entries in the file are added to the list of discovery profiles. Perform a device discovery to search for the imported printers.

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. Each line may contain a single IP address or fully qualified domain name, or the following fields may be used:

IP address or fully qualified domain name, SNMP read name, SNMP write name, device class, device model, serial number, contact name, contact location, property tag

As with any CSV file, you must still include a comma for a blank field followed by populated fields.

An XML file is structured like the following example:

```
<?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>
```

</filter>
</filters>

Discovering printers

Before a solution can be deployed to a printer, the printer must be discovered as part of a device group. Printers may be manually discovered or automatically discovered on a schedule. This section covers manual discovery, which is used during initial setup of the system. For more information about scheduled discovery, see [“Scheduling a discovery task” on page 78](#).

- 1 Click the **Device Groups** tab.
- 2 If necessary, create a new discovery profile.
- 3 Select a device group from the Device Groups list, or select **All Device Groups** to discover printers in multiple device groups.
- 4 Select **Discovery** from the Tasks list.
- 5 If you are discovering printers in a device group or groups where you have previously discovered printers, and you want to skip any IP address where a printer has been discovered (including currently missing devices), then select **Discover new devices only**. This results in a faster discovery when adding subsequent discovery profiles.

If you are discovering printers from multiple device groups, then select the device groups for the discovery task in the main section. The list does not appear if a specific device group is selected in the Device Groups list.

- 6 If necessary, click **Edit** to edit the discovery configuration.

Note: For more information about adjusting timeout periods for device discovery, see [“Configuring NPA device communication” on page 56](#).

- 7 Click **Discover**.

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

Notes:

- If you stop the discovery process, then it may take a few minutes for the discovery task to completely stop.
- After a printer has been discovered, removing the related device group or discovery profile does not remove the printer from the system. For information about removing printers from the system, see [“Removing devices from the system” on page 87](#).
- After the discovery process, the number of missing devices appears, if applicable. Click **Missing Devices Count** to launch the Missing Devices task. For more information, see [“Discovering missing printers” on page 77](#).

Discovering missing printers

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

- 1 Click the **Device Groups** tab.
- 2 Select a device group from the Device Groups list, or select **All Device Groups** to discover missing printers in multiple device groups.

- 3 Select **Missing Devices** from the Tasks list.
- 4 If you are discovering missing printers in multiple device groups, then select the device groups for the discovery task in the main section. The list does not appear if a specific device group is selected in the Device Groups list.
- 5 If necessary, edit the discovery parameters.
- 6 Click **Discover**.

Viewing all printers with outdated policies

- 1 Click the **Device Groups** tab.
- 2 Select **All Device Groups** from the Device Groups list.
- 3 Select **Out of Policy Devices** from the Tasks list.

Scheduling a discovery task

- 1 Click the **Device Groups** tab.
- 2 Select a device group from the Device Groups list, or select **All Device Groups** to discover devices in multiple device groups.
Note: Make sure discovery profiles exist for device groups to be included in the operation.
- 3 Select **Schedule** from the Tasks list.
- 4 Click **Add > Discovery**.
- 5 Type a description for the task, and then click **Next**.
- 6 If you are discovering devices from multiple device groups, then select the device groups for the discovery task, and then click **Next**. The list does not appear if a specific device group is selected in the Device Groups list.
- 7 Enter a start date and a start time.
- 8 Configure the frequency of the scheduled event, and then click **Finish**.

Deploying solutions to a device group

Deploying a solution to a device group creates profiles on the printers in the group that allow users to execute jobs using the solution.

Note: It is recommended to set servers offline before deploying solutions to device groups to prevent execution of associated profiles before you have completed configuration. For more information, see [“Viewing and changing server status” on page 47](#).

- 1 Click the **Device Groups** tab.
- 2 Select a device group from the Device Groups list.
- 3 Select **Solutions** from the Tasks list.
- 4 In the main section, click **Add**.

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

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

Note: A policy update is required to complete the deployment of the solution. For more information see [“Updating policies for device groups” on page 83](#).

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 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, 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 device classes, 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.

- 1** Click the **Device Groups** tab.
- 2** From the Device Groups list, select a device group.
- 3** From the Tasks list, select **Home Screen**.
- 4** Click the tab for the class of printers that you want to configure.
- 5** Select **Use this home screen as part of the device groups policy**.
- 6** Configure a button on the home screen:
 - For touch-screen printers, do the following:
 - a** From the Layout menu, select the number of buttons to include.
 - b** If necessary, click a page, and then click the button to configure.
 - c** 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.	<ul style="list-style-type: none"> – 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/Supplies – USB Drive
Show a list of profiles.	<ul style="list-style-type: none"> – App Profiles – Profiles
Execute a specific profile.	Single Profile

¹ Not all selections are available for all 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
Override a standard function with a profile. ²	<ul style="list-style-type: none"> – Copy + Profile – Email + Profile – Fax + Profile – FTP + Profile
Execute a printer shortcut.	<ul style="list-style-type: none"> – Shortcut
Provide a placeholder for an eSF application icon. ³	<ul style="list-style-type: none"> – App Reservation – Placeholder
Leave a blank space.	None

¹ Not all selections are available for all 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:

- If you selected **Shortcut**, then enter the number of the shortcut.

☒ Use this home screen as part of the device group's policy.

[Page 1](#) [Page 2](#) [Page 3](#) [Page 4](#)

Layout: 1 Button

Choose each button and set its action. Buttons with no actions will not appear on the Home Screen.

Shortcut 1

Action: Shortcut

Display: ☒ Default

Text:

Graphic: Default Custom...

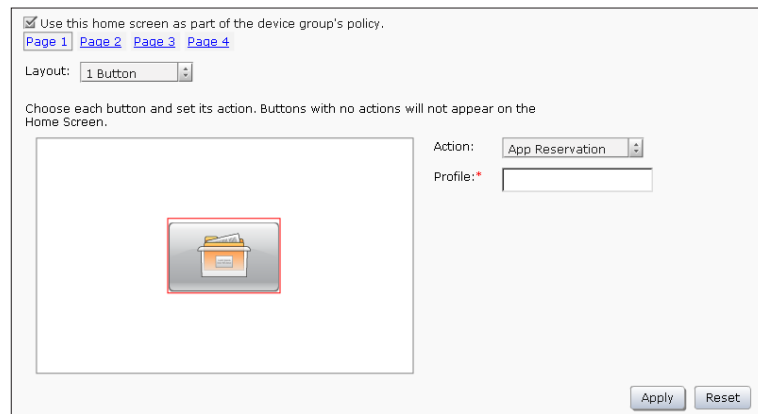
Shortcut:* 1

Apply Reset

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 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 select a JPEG, GIF, or PNG file for the Up and Down icons.
- 3 Click **Apply**.

Note: If you want to revert to the default graphic, then click **Default**.

Selected images are resized to the following dimensions for each device class. For best results, resize or crop source images to the correct size before use.

- **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](#).

- f To apply custom text to any button except Placeholder or App Reservation, select **Text**, and then type your custom text. You can also select the Text option and leave it blank to show only the icon.
- For non-touch-screen printers:
 - a From 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 To apply custom text to the button, select the option for the custom text field beside Display Text, and then type your custom text.
- d Select a profile to associate with the button.

7 Configure the rest of the buttons on the home screen.

8 Apply the changes.

Note: Before changing tabs during configuration, make sure to click **Apply** on each tab to apply the settings.

Updating policies for device groups

When solutions are deployed, home screens are configured, or settings are changed for a device group, the printers in the group are marked as “Out of Policy,” and a policy update is required to apply the changes to the printers. Changes are not automatically pushed to printers, so you can schedule policy updates during times of off-peak usage to avoid negatively affecting system performance.

Additionally, because the system cannot monitor changes that occur outside of the system that affect the policy conformance of a printer, it is a good idea to schedule policy updates after a system is set up. For more information, see [“Scheduling policy updates” on page 84](#).

Policy updates include deployment of eSF applications to e-Task 2 printers when necessary. This includes deployment of the Advanced Prompting Bundle the first time policies are updated on e-Task 2 printers, first-time deployment of eSF applications associated with hybrid solutions, and any policy updates immediately after the Advanced Prompting Bundle or other eSF applications are updated. Validation that occurs during deployment of eSF applications causes policy updates that include eSF deployments to take significantly longer than those that do not.

If a large eSF application or several eSF applications are included with a hybrid solution, then you may need to increase the default timeout for policy updates using the PolicyUpdate service on the Services tab in order to allow enough time for the policy update to complete. If you do not want to validate eSF application deployment on each printer, then see [“Disabling validation of eSF application deployment” on page 84](#).

1 Click the **Device Groups** tab.

2 Select a device group from the Device Groups list, or select **All Device Groups** to update policies for printers in multiple device groups.

3 Select **Policy Update** from the Tasks list.

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:

- To update only out-of-policy printers, select the **Only update those devices which are Out Of Policy** check box.
- To update all printers, regardless of current policy conformance, clear the **Only update those devices which are Out Of Policy** check box.

5 If you are updating policies for printers in multiple device groups, then select the device groups for the policy update task in the main section. The list does not appear if a specific device group is selected in the Device Groups list.

6 Click **Update Policy** to deploy the solutions to the printers in the device group.

Note: After updating policies, the Policy Update status appears showing the number of devices that failed to update, if applicable. Click **Failed Devices Count** to view the error logs for this task. To view the full set of logs for this task, clear the Message filter.

Scheduling policy updates

- 1 Click the **Device Groups** tab.
- 2 Select a device group from the Device Groups list, or select **All Device Groups** to update policies for printers in multiple device groups.
- 3 Select **Schedule** from the Tasks list.
- 4 Click **Add > Policy Update**.
- 5 Type a description for the task, and then click **Next**.
- 6 If you are updating policies for printers in multiple device groups, then select the device groups for the policy update task in the main section. The list does not appear if a specific device group is selected in the Device Groups list.
- 7 Enter a start date and a start time.
- 8 Configure the frequency of the scheduled event, and then 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 Click the **Device Groups** tab.
- 2 Select a device group from the Device Groups list.
- 3 Select **Security** from the Tasks list.
- 4 Enable secure communication, and then click **Apply**:
 - To secure only the credentials such as user name and password of the session, select the **Enabled for Credentials** option.
This option is faster than a communication that is set to “Enabled for Session.”
 - To completely secure the session, select the **Enabled for Session** option.

Disabling validation of eSF application deployment

Validation that occurs during deployment of eSF applications causes policy updates that include eSF deployments to take significantly longer than those that do not. If you do not want to validate eSF application deployment on each printer, then do the following:

Note: eSF settings configured using the eSF configuration task are not deployed when validation of eSF application deployment is disabled.

- 1 Click the **Device Groups** tab.
- 2 Select an appropriate device group from the list.
- 3 Select the **eSF Configuration** task.

- 4 Clear the **Verify eSF application deployment and deploy these eSF settings** check box, and then click **Save Settings**.
- 5 Repeat steps 2 through 4 for any other appropriate device groups.

Configuring the Devices tab

The Devices tab is generally used for specialized maintenance and troubleshooting.

Searching for devices

Before performing device-specific tasks, previously discovered devices must be selected by searching for matching values of certain criteria, selected from the following:

- Address
- Hostname
- Device Model
- Serial Number
- Contact Name
- Contact Location
- Property Tag

- 1 Click the **Devices** tab.
- 2 Select a search criterion.
- 3 Enter a value to search.
- 4 Click **Search**.

Note: Using the asterisk wildcard character (*) to represent the sections at the end of the IP address will return all devices in that subnet. For example, type **10.10.*.*** to find all devices that have been discovered within the range 10.10.0.1–10.10.255.255. Also, a range of IP addresses can be used as a search criterion by entering the first and last addresses, separated by a hyphen.

Editing the home screen layout on specific devices

The Home Screen task on the Devices tab accesses the home screen and available profiles of selected printers directly, unlike the corresponding task on the Device Groups tab, which lets you configure a common home screen to be deployed during a policy update and only provides access to LDD profiles.

Accessing the home screen configuration for specific devices may be helpful for the following tasks:

- Troubleshooting home screen issues on specific devices
- Configuring home screens on specific devices for which custom home screens are not configured within a device group
- Configuring home screens that include non-LDD profiles
- Removing orphan buttons from the home screen

Notes:

- If a custom home screen is configured for a device group that contains the printer, then any changes made will be overwritten during the next policy update.
- LMC cannot access eSF application icons directly. Use placeholders to provide locations for eSF application icons in the default order, and then use App Reservation to designate a location for the icon of a specific eSF application identified by name. If no placeholders or App Reservations are provided, then any installed eSF applications appear on the first page after the pages defined in the custom home screen.

1 Click the **Devices** tab.

2 Search for printers.

3 Select device names in the Devices list.

4 Select **Home Screen** from the Tasks list.

5 To edit an individual home screen, click **Edit**.

Make any necessary changes to the layout of the home screen, and then click **Apply**. To cancel editing, click **Reset**.

6 If multiple devices are selected, click **Next** to view the home screen of the next device on the list.

Viewing device profiles

1 Click the **Devices** tab.

2 Search for device(s).

3 Select the device name(s) in the Devices list.

4 Select **Profiles** from the Tasks list.

5 Select a profile name from the list to view the profile settings.

6 If multiple devices are selected, then click **Next** to view the next device on the list.

Updating device policies

1 Click the **Devices** tab.

2 Search for the device or devices.

3 Select the device names in the Devices list.

4 Select **Policy Update** from the Tasks list.

5 Click **Update Policy**.

Note: After policies are updated, the Policy Update status appears and shows the number of devices that failed to update, if applicable. Click **Failed Devices Count** to view the logs, and then select the task ID in the Jobs page to view the details.

Removing devices from the system

- 1 Click the **Devices** tab.
- 2 Search for one or more devices.
- 3 Select one or more device names in the Devices list.
- 4 Click **Remove from System** > **Yes**.

Notes:

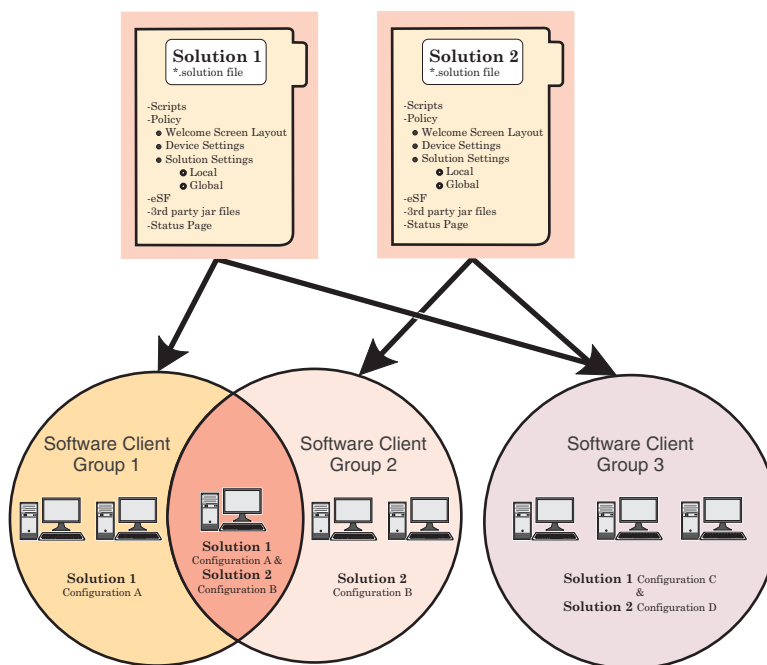
- Removing a device from the system does not remove profiles that have been deployed to the device, reverse any home screen modifications, or remove eSF applications installed with any solution.
- If a removed device is still included in a discovery profile, then it will be rediscovered during the next discovery task using that discovery profile.

Managing software clients

Understanding software clients and software client groups

A software client is a computer that is configured to use Microsoft Windows application software Select'N'Send or Lexmark Document Server Printer Port to access solutions directly. 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 57](#).

Understanding dynamic prompting support

When a profile is selected, solutions usually either prompt you for information or start a job. Many solutions involve submitting jobs with related information (such as account numbers, passwords, or processing options) that is obtained through prompting. Where possible, prompting should occur before submitting the job. This gives you the opportunity to cancel jobs when prompted for information they don't have at the moment.

The Job Submission Web Service provides prompting capability to Lexmark Document Server Printer Port clients. From the port monitor, the following prompts are supported:

- **MessagePrompt**
- **BooleanPrompt**
- **IntegerPrompt**
- **ListPrompt**
- **ArrayPrompt**
- **PasswordPrompt**
- **ScanPrompt**
- **MessagePrompt**
- **EndPrompt**

When the prompt wizard appears on the client screen, you can respond to the prompt within 30 seconds before it times out. Prompting depends on whether or not there are any more required information or documents to process. If there are more, then the end user is asked whether to continue or not. When the user reaches the last prompt, a summary dialog of the answers appears. The user can then choose to send or cancel the job.

You can cancel the job at any time, although cancelling the job cannot undo the job application processing that has already taken place.

Note: LDD 4.6.3.x printer ports on a clustered print server is not supported.

Understanding software client setup

Preparing software clients for use with LDD solutions requires a slightly different process than 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 70](#).
- 2 If necessary, install client software licenses on the LDD system. For more information, see [“Adding licenses to an existing server” on page 57](#).
- 3 Create a software client group to contain software clients to which a particular solution should be available.
- 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 client software on each of the client computers. For more information, see [“Installing client software” on page 91](#).
Note: Servers must be set online to install the client software successfully.
- 7 Run Windows Update to make sure the latest updates for the .NET framework are installed.
- 8 When using Lexmark Document Server Printer Ports, add print queues assigned to the appropriate Lexmark Document Server Printer Port on each client computer or print server.
Note: Do *not* configure an LDD printer port on a print server to use a profile or script that prompts.
- 9 Test all print queues that use Lexmark Document Server Printer Ports. For more information, see [“Using LDD print queues” on page 95](#).
- 10 Use test jobs to complete 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 96](#).

Creating and populating software client groups

Creating a software client group

- 1 Click the **Software Client Groups** tab.
- 2 Click **Add** from the Software Client Groups list.
- 3 Type a unique name for the new software client group, and then click **Add**.

Adding software clients to a software client group

- 1 Click the **Software Client Groups** tab.
- 2 Select a software client group from the Software Client Groups list.
- 3 Select **Client Profiles** from the Tasks list.
- 4 Type an IP address, address range, subnet, or fully qualified domain name in the Address field.

Address format	Example
IP address	10.10.2.100
IP address range	10.10.2.1-10.10.2.127
Subnet	10.10.2.*
Fully qualified domain name	client-hostname.domain-name

- 5 Click **Add**.

Notes:

- Software client groups manage software clients by IP address and do not require discovery.
- When adding a software client that will be installed on a Microsoft Cluster Server, add the IP address of the logical host, as well as the IP addresses of all physical nodes in the cluster.

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 list, select a software client group.
- 3 From the Tasks list, select **Client Profiles**.
- 4 Click **Import**.
- 5 Type the path of the file, or click **Browse**, and then locate the file.
- 6 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 grants the software clients in the group access to the solution on the server, which allows users of these software clients to execute jobs using the solution.

- 1 Click the **Software Client Groups** tab.
- 2 Select a software client group from the Software Client Groups list.
- 3 Select **Solutions** from the Tasks list.
- 4 In the main section, click **Add**.
- 5 Select the solution from the list, and then click **Next**.
- 6 Configure the local settings of the solution for the current software client group, and then 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 on a Microsoft Cluster Server

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

- 1 Set any online Print Spooler resource offline to avoid initiating a failover during installation.
- 2 Install *only* the Lexmark Document Server Printer Port on each physical node in the cluster.
- 3 Run Windows Update on each node to make sure the latest updates for the .NET framework are installed.
- 4 If necessary, configure the spooler resource and the LDD Client Service for the cluster.

Note: Make sure the spooler resource and the LDD Client Service are in the same cluster resource pool so that failover is initiated together.
- 5 Create print queues on the cluster, selecting **Lexmark Document Server Port - Enterprise** as the port.

Note: For more information on creating print queues, see [“Configuring a Lexmark Document Server port” on page 94](#).

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 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 the System tab in LMC, set at least one server online. For more information, see [“Viewing and changing server status” on page 47](#).
 - 3 From the Printers or Devices control panel in Windows, add a printer. For more information on adding a printer, see [“Configuring a Lexmark Document Server port” on page 94](#).
 - 4 When prompted, select a local printer, and do not allow Windows to search for plug-and-play printers.
 - 5 When prompted to select a printer port, create a port of Lexmark Document Server Port - Enterprise type.
 - 6 Type a name for the new port, and then click **Next**. The port name must be 75 characters or fewer.
 - 7 Select a Lexmark 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 fully qualified domain name or IP address of the load balancer, and then click **OK**.
- d** To exit the Server Setup window, click **OK**.
- e** Select the new server from the list.

8 Click **Next**.

9 Select a profile on the server to use with the new port, and then click **Next**.

Notes:

- Do not configure an LDD port on a print server to use a profile that prompts. Prompting profiles should be used only on client computers.
- Only profiles associated with solutions 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 on the list. Wait until the server is not busy, and then try adding the port again.

10 Click **Finish**.

11 Select an existing print driver, and then click **Next**. For more information, see the documentation that came with the printer or print driver.

12 If you are asked whether to keep the existing driver, then select **Keep existing driver (recommended)**, and then click **Next**.

13 Type a 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**.

14 Select whether to share the new print queue. If you are installing the print queue on a server, then select **Share name**.

15 Type a name for the print queue on the network.

16 Click **Next**.

17 To skip printing a test page, select **No**.

18 Confirm the settings, and then click **Finish**.

19 In the Printers control panel, right-click the new printer, and then click **Properties**.

20 Click the **Advanced** tab.

21 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 complete while the large job is spooling.

22 Click **OK**.

Configuring a Lexmark Document Server port

Note: Make sure to log in as an administrator.

Creating a print queue

- 1 Open the printers folder, and then add your printer.
- 2 Follow the instructions on the computer screen.

Configuring an existing print queue

- 1 Open the printers folder, and then select your printer.
- 2 Open the printer properties.
- 3 From the Ports tab, configure or add a Lexmark Document Server port.

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 the print queue, open the printer properties.
- 2 From the Ports tab, select **Enable printer pooling**, and then add a Lexmark Document Server port.
- 3 Select the Lexmark Document Server port created for the selected printer, and then click **Next**.
- 4 Select the profile used for the port created for the selected printer, and then click **Next**.

Notes:

- Do not select a profile that prompts.
- If the server is running many jobs, then profiles on the server may not appear in the list. Wait until the server is ready, and then try adding the port again.

- 5 Follow the instructions on the screen.

Note: You can add more Lexmark Document Server ports, and then add them to the same profile.

- 6 Apply the changes.

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 display that allows users to access the solution.

If the profile that you want appears on the home screen, then touch the icon for the profile.

If the profile that you want 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 that you want to appear on the home screen.

The profile launches the associated script on the server. Documents are scanned as necessary, and any prompts included in the script are presented to the user.

Note: When using a solution that reads a bar code, scan at 300 dpi for best results. Depending on the documents being scanned, using a higher setting for Darkness may also provide better results.

Using LDD print queues

- 1 With a document open in Windows, click **File > Print**.
- 2 Select the printer associated with the Lexmark Document Server port and the profile you want to use.
- 3 To configure print options, click **Properties**, **Preferences**, **Options**, or **Setup**.

See the documentation that came with the printer or print driver for more information about print options.

Note: When using a solution that reads a bar code, print at 300 dpi, with any other quality settings at the highest levels for best results.
- 4 Click **OK** to close any printer software dialogs.
- 5 Click **OK** or **Print**.

The document is sent to the LDD system using the profile specified in the configuration of the Lexmark Document Server port associated with the selected printer. The file type is determined by the output of the print driver, and each solution determines the accepted file types.

Configuring the Microsoft Windows application software Select'N'Send

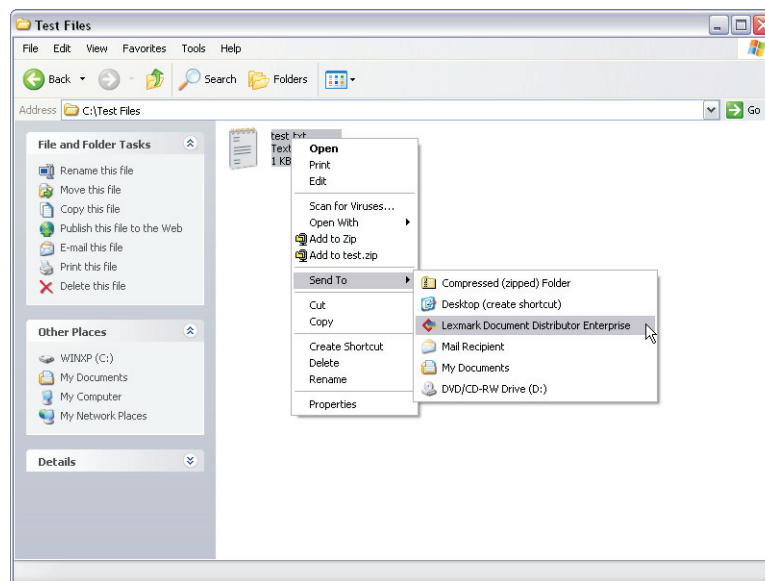
Configuring the GUI of the Microsoft Windows application software Select'N'Send

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 which file types are acceptable. For more information, contact the developer of your solution.

1 Launch the GUI of the Microsoft Windows application software Select'N'Send.

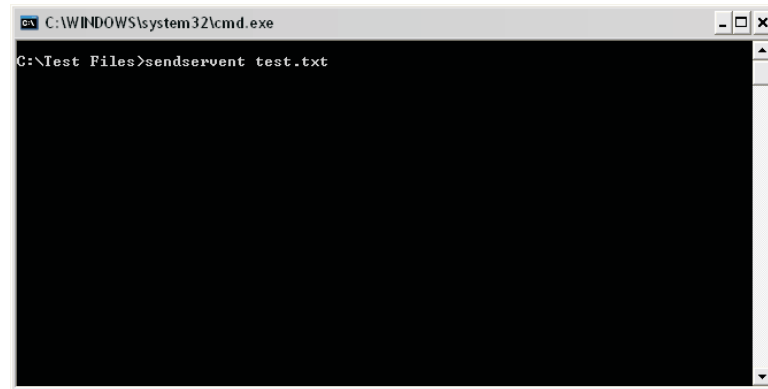
Do one of the following:

- From Windows Explorer, right-click the file that you want to submit to LDD, and then click **Send To > Lexmark Document Distributor Enterprise**.

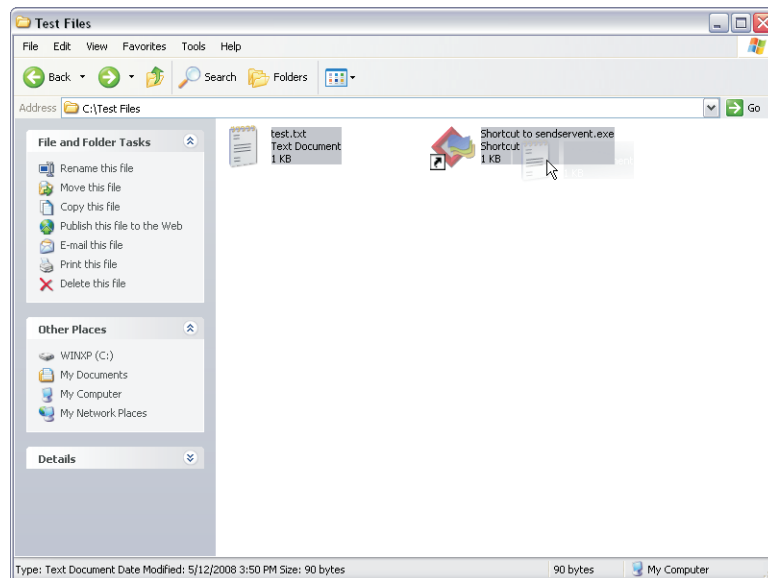


- From the command line, type **sendservent filename**, where **filename** is the file that you want to submit to LDD, and then press **Enter**.

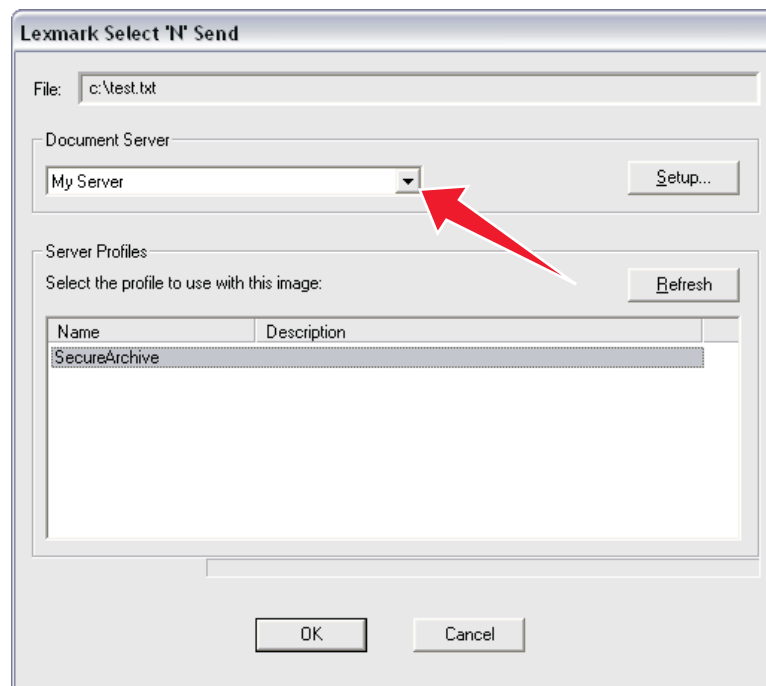
Note: The program folder of the Microsoft Windows application software Select'N'Send is added to the system path during installation. This configuration enables the software to be accessed from any folder at the command line.



- Drag the file that you want to submit to LDD onto the *sendserver.exe* file or to a shortcut pointing to that file.



2 From the Lexmark Select'N'Send window, select a Lexmark 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 fully qualified domain name or IP address of the server, and then click **OK**.
- d** To exit the Server Setup window, click **OK**.
- e** If necessary, select the new server from the list.

3 From the Server Profiles list, select a profile.

4 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 using specific profiles

Use this command to run the command-line version of the Microsoft Windows application software Select'N'Send:

```
sendservent -s server -p profile -f filename [-u userdatafile -t timeout -i interval]
```

where:

- **server** is the IP address or fully qualified domain name of the load balancer LDD system.
- **profile** is the profile to run on the LDD server.
- **filename** is the path 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 which file types are acceptable. For more information, contact the developer of your solution.

- **userdatafile** is the path of a file containing user information for the job.

Note: If no user data file is 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 to wait for confirmation from the LDD system before aborting the operation with an error. The default is **0**, which specifies no timeout. This setting is optional.
- **interval** is the time in seconds to wait between each instance of polling the LDD system for confirmation. The default is **0.5**. This setting is optional.

Note: Any option that contains a space must be enclosed in double quotation marks (").

Scheduling scripts

Some solutions include scripts that can be set to run on a schedule. Additionally, some scripts can be associated with a device group or software client group in order to use local settings associated with that group.

- 1 Click the **System** tab.
- 2 Select **Schedule** from the System list.
- 3 Click **Add > Script**.
- 4 Type a description for the task, and then click **Next**.
- 5 Select whether to associate the scheduled script with a device group or software client group:
 - To associate the script with a device group:
 - a Click **DeviceGroup**, and then click **Next**.
 - b Select the device group to associate the script with, and then click **Next**.
 - To associate the script with a software client group:
 - a Click **SftClientGroup**, and then click **Next**.
 - b Select the software client group to associate the script with, and then click **Next**.
 - To schedule the script without associating it with a device group or software client group, click **None**, and then click **Next**.
A script that is not associated with a device group or software client group can access only global solution settings.
- 6 Select a solution, and then select a script.
- 7 If the script applies to individual servers rather than the system as a whole, such as a script that deletes certain files from a server, or a script that runs a report with server-specific information, then click **Run on All Servers**.
- 8 If the script uses information supplied in the Additional Options field, then type the necessary information. For more information, contact the developer of the solution.
- 9 Click **Next**.

10 Enter a start date and a start time.

11 Configure the frequency of the scheduled event, and then click **Finish**.

Viewing logs

Viewing installation logs

- 1 From the computer where LDD is installed, open the Windows Run dialog box, and then type **"%ALLUSERSPROFILE%\Lexmark\LDD4x"**.
- 2 Open the log files in a text editor.

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 e-Task 5 printers, see ["Supported printers" on page 11](#).

To change the logging level of the `cdcl_wrapper.log` to **"debug"**, do the following:

- 1 Open the "Lexmark\Solutions\apps\cdcl-rest-wrapper\WEB-INF\classes\log4j.properties" file in a text editor.
- 2 Change **log4j.rootLogger=WARN,perfllog** to **log4j.rootLogger=DEBUG,perfllog**.
- 3 Save and close the file.
- 4 From the Windows Services control panel on the server computer, restart the Lexmark Solutions Application Server service.

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, open the file in a text editor.

The default message priority for recording is **warn**. When troubleshooting a problem, the message priority can be changed to **debug** to capture all available messages.

- 1 Click the **System** tab.
- 2 From the System list, click **System Status**.
- 3 Set the server for which you are changing the message priority offline. 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 In a text editor, open the **log4j-lsas.xml** file from the "Lexmark\Solutions\apps\wf-lsds\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 service.
- 8 From the System tab, set the server online. For more information, see ["Viewing and changing server status" on page 47](#).

Note: To save disk space, after recording the necessary 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, you can 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 necessary data, set the logging level to **No**.

Troubleshooting

Solving LMC problems

The browser shows a 5yy error when accessing LMC

When the system is under a heavy processing load, your web browser may show a 5yy error when you try to access 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.
- If the load balancer is under a heavy processing load, then try again when the system is processing fewer jobs.
- Determine whether a problematic server installation is causing LMC to be inaccessible through the load balancer:
 - 1 Access LMC directly on each server using the URL **http://server:9788/lmc**, where **server** is the computer where the server is installed.
 - 2 Click the **System** tab.
 - 3 From the System list, select **System Status**, and then determine whether any of the servers in the system are not communicating.
 - 4 If any server is not communicating, then uninstall it from the computer where it is installed.
Note: If the entry remains after uninstalling the server, then select the non-communicating servers in LMC, and then click **Remove Server(s)**.
 - 5 Access LMC using the load balancer address.
- Uninstall and reinstall all components. Make sure to enter the correct addresses for the database and load balancer.

LMC responds very slowly

Several servers that are not communicating may cause LMC to respond very slowly.

Determine whether non-communicating servers appear in LMC:

- 1 Access LMC directly on an active server using the URL **http://server:9788/lmc**, where **server** is the computer where the server is installed.
- 2 Use the System Status task on the System tab to determine whether any of the servers in the system are not communicating.
- 3 If any servers are not communicating, then select them from the list, and then click **Remove Server(s)**.
- 4 Access LMC using the load balancer address.

LMC does not finish loading or data is missing

If cookies are not enabled, then LMC may continue to display **Loading** for an extended period after logging in, or data may be missing or incorrect on some screens.

Try one or more of the following:

- Make sure cookies are allowed for the address where you access LMC. Cookies must be enabled on your Web browser in order to use LMC.
- Make sure you have Adobe Flash Player 10 or later installed. If your Web browser settings do not allow ActiveX controls to run, then you must upgrade manually by visiting the Adobe Web site.

An error occurs when uploading a formset

Make sure you have Adobe Flash Player 10 or later installed. If your Web browser settings do not allow ActiveX controls to run, then you must upgrade manually on the Adobe Web site.

Reports are not displayed when run

- 1 Make sure pop-ups are allowed for LMC in your Web browser.
- 2 If you are running a PDF report, then make sure Adobe Reader is installed.

User cannot access some tasks in LMC

Check with the administrator if the group to which the user belongs has limited access to that task.

User can still access tasks even after privileges are removed

Check the Privileges settings of all the groups to which the user belongs. For more information, see [“Assigning privileges to groups” on page 36](#).

The Solutions tab and the eSF Configuration task for device groups do not function

A descriptor file for an eSF application included with a solution may have contained tag names that have colons. Multiple errors may have occurred while uploading the solution.

Try one or more of the following:

- Remove colons from descriptor files for associated eSF applications. For more information, contact the developer of the solution.
- Manually remove the solution that caused the problem. For more information, contact your Lexmark representative.
- Reinstall the solution.

Jobs do not respond after an error occurred

If an error occurred while a job is being processed, then stop the specific job. This terminates the job that is no longer responding but is still marked as running in LMC.

- 1 Click the **System** tab.
- 2 Select **Jobs** from the System list.
- 3 Select the tasks that do not respond, and then click **Stop Task**.

Solving discovery problems

Discovery and policy updates running slowly

- 1 Check your proxy, firewall, and other network settings on system components to make sure all necessary communication is allowed.
- 2 Make sure other network traffic is not reducing bandwidth during discoveries and policy updates.
- 3 If you have three or more servers in your system, then try reducing the chunk size using the **General** service on the **Services** tab. A value as low as **2** may improve performance.
- 4 To reduce the time waiting for non-responsive printers during policy updates, reduce the timeout per device using the **PolicyUpdate** service on the **Services** tab.
Note: If you are deploying solutions that include large eSF applications or several eSF applications, then a lower setting may not allow enough time to successfully validate eSF application deployment.
- 5 If you are discovering printers for subsequently added discovery profiles in a device group or groups in which you have previously discovered printers, then select **Discover new devices only** to skip any IP address where a printer has been discovered.

Discoveries frequently time out

- 1 Check your proxy, firewall, and other network settings on system components to make sure all necessary communication is allowed.
- 2 Make sure other network traffic is not reducing bandwidth during discoveries and policy updates.
- 3 If you have three or more servers in your system, then try increasing the initial timeout and retry times using the **NPA** service on the **Services** tab. Type a timeout period in milliseconds for each retry in sequence, separating each by a space in the NPANT Timeout field.

Some printers on the network cannot be discovered

- 1 Check your proxy, firewall, and other network settings on system components to make sure all necessary communication is allowed.
- 2 From the Services tab, make sure the read community name and write community name for the SNMP service match the printers on the network. All printers used in the system must use the same read community name and write community name.

- 3 From the Device Groups tab, make sure the discovery profile settings of the discovery profile are correct. For more information, see [“Discovering printers” on page 77](#).

Solving server and printer problems

Cannot connect to the Microsoft SQL Server database using integrated security

Try one or more of the following:

- Make sure that the domain account is granted access to the Microsoft SQL Server database.
- Make sure that the domain account has full control privileges to the LDD installation path on the application servers and all its sub-folders.
- If you have a remote Microsoft SQL Server database, then make sure that the domain account is able to communicate with the server.
- Make sure that the Log On properties of the following are set to the domain account that has access to the Microsoft SQL Server database:
 - Lexmark Apache Agent service
 - Lexmark Solutions Application Server
- Make sure that the Lexmark Apache Agent service and Lexmark Solutions Application Server is restarted.

One or more servers cannot be set online

Try one or more of the following:

- Make sure a license is installed for each server during installation. For more information about activating licenses, see [“Obtaining licenses” on page 16](#). For more information about adding licenses after installation, see [“Adding licenses to an existing server” on page 57](#).
- Check your proxy, firewall, and other network settings across the LDD system to make sure communication is allowed among components.
- Uninstall and reinstall the problem server making sure to enter correct addresses for the database and load balancer. Note that when the server is installed on the same computer as the database and the load balancer, the fully qualified domain name of the computer must still be used, not localhost or the loopback address (**127.0.0.1**).
- Make sure the correct address is used for the database when installing the load balancer. Note that when the load balancer is installed on the same computer as the database, the fully qualified domain name of the computer must still be used, not localhost or the loopback address (**127.0.0.1**). If the address is specified incorrectly, then uninstall and reinstall the load balancer and all servers.

Note: Multiple non-communicating servers may impact system performance. If you do not expect a non-communicating server to quickly reestablish communication, then you should remove it. To remove a server that is not communicating, select the check box beside it in the table, and then click **Remove Server(s)**.

One or more servers cannot be set offline

From the Windows Services control panel, make sure the Lexmark Solutions Apache Agent service is running.

Error in importing a license

Try one or more of the following:

- Make sure the correct address is used for the database and load balancer when installing servers. Note that when the server is installed on the same computer as the database and the load balancer, the fully qualified domain name of the computer must still be used, not localhost or the loopback address (**127.0.0.1**). If the address is specified incorrectly, then uninstall and reinstall the applicable servers.
- Make sure the correct address is used for the database when installing the load balancer. Note that when the load balancer is installed on the same computer as the database, the fully qualified domain name of the computer must still be used, not localhost or the loopback address (**127.0.0.1**). If the address is specified incorrectly, then uninstall and reinstall the load balancer and all servers.

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 LDD system is first booted. If the system was recently booted, then wait a few minutes, and then try again.
- Make sure that the LDD system and all servers are online.
 - 1 Log in to LMC.
 - 2 Click the **System** tab.
 - 3 If necessary, from the System list, select **System Status**.
 - 4 In the Status column, look for offline servers, and then set servers online as necessary. For more information, see [“Viewing and changing server status” on page 47](#).
- Make sure that the solution you are attempting to access exists in the system and has been properly deployed to a device group containing the printer.
 - 1 Log in to LMC.
 - 2 Click the **Solutions** tab.
 - 3 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 70](#).
 - 4 If necessary, select the **Summary** task.
 - 5 Make sure that a device group that contains the printer appears beside Device Groups in the Summary section.

If no device group containing the printer appears, then make sure that the printer is added to a device group. Deploy the solution to that device group. For more information, see [“Deploying solutions to a device group” on page 78](#).
 - 6 Perform a policy update. For more information, see [“Updating policies for device groups” on page 83](#).

- Make sure that the correct version of the AP Bundle is installed.
 - 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, do one of the following:
 - For e-Task 5 printers, click **Apps**.
 - For e-Task 4 printers, click **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**.
 - 4 Make sure that the first two segments of the version number beside 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.
 - 5 If the version numbers do not match, then do the following:
 - a Make sure that the printer access controls are not preventing policy updates from working correctly.
 - 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, do either of the following:
 - For e-Task 5 printers, click **Settings > Security > Login Methods**. From the Public section, click **Manage Permissions**. Expand **Device Management**, and then select **Firmware Updates**.
 - For e-Task 4, e-Task 3, e-Task 2+, e-Task 2, or e-Task printers, click **Settings > Security > Security Setup > Access Controls > Management**. Set Firmware Updates to **No Security**.
 - b Click **Submit**.
 - c In LMC, do either of the following:
 - Perform a policy update. For more information, see [“Updating policies for device groups” on page 83](#).
 - Install the AP Bundle manually.
- 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, do one of the following:
 - For e-Task 5 printers, click **Apps > Installed Apps > Install an app**.
 - For e-Task 4 printers, click **Settings > Apps > Apps Management > Install a New App**.

- For e-Task 3 printers, click **Settings > Device Solutions > Solutions (eSF) > Install**.
 - For e-Task 2+, e-Task 2, or e-Task printers, click **Settings > Embedded Solutions > Install**.
- 4** Locate and select the **ap.flis** file in the “\Lexmark\Solutions\apps\wf-ldss\firmware\” folder where an LDD server is installed, and then click **Open**. Depending on your printer model, click either **Install** or **Start Install**.
- Review the Embedded Solutions diagnostic log to make sure that the printer can resolve the server host name. For more information, see [“Viewing the Embedded Solutions diagnostic log” on page 102](#).
 - Check your proxy, firewall, and other network settings on LDD components to make sure that all necessary communication is allowed.

The server log contains Quartz errors

Make sure to synchronize the time on all computers used in the LDD system before installing LDD components.

If the time is not synchronized, then do the following:

- 1** Uninstall all components.
- 2** Synchronize the time on all computers using an NTP server.
- 3** Reinstall all components.

Kerberos authentication is not working

Make sure that the date and time on the printer, LDD server, and KDC server are correct and synchronized.

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 key.

For 64-bit Windows operating systems such as Windows Server 2008 R2 x64, "HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\Tomcat7\Parameters\Java\Options" is the 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.

The solution or profile icon does not appear on the home screen

Try one or more of the following:

- From the printer control panel, refresh the home screen by moving to another screen and then returning to the home screen.
- If the home screen has multiple pages available, then make sure that the icon does not appear on other pages.

- If the profile is available in the App Profiles menu or the Held Jobs menu and its icon is missing, then customize the home screen correctly.
 - 1 From LMC, click the **Device Groups** tab.
 - 2 From the Device Groups list, select a device group.
 - 3 From the Tasks list, select **Home Screen**.
 - 4 Click the device class tab that matches the device class of the printer.
For more information on device classes, see [“Supported printers” on page 11](#).
 - 5 Select **Use this home screen as part of the device groups policy**.
 - 6 Select a layout other than the default, and make sure that the profile has been assigned to a button.
For more information on customizing the home screen, see [“Customizing the home screen for a device group” on page 79](#).
- If the profile does not appear in the App Profiles menu or the Held Jobs menu, then configure the device groups correctly and update the policies.
 - 1 Make sure that the solution has been deployed properly to a device group containing the printer.
For more information, see [“Deploying solutions to a device group” on page 78](#).
 - 2 Perform a policy update. For more information, see [“Updating policies for device groups” on page 83](#).
- For e-Task 5, e-Task 4, e-Task 3, and e-Task 2+ printers, make sure that the missing icon is enabled in the printer settings.

Note: For a list of printers, see [“Supported printers” on page 11](#).

 - 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, 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**.
 - 4 Select the item that corresponds to the missing icon, and then click **Save** or **Submit**.
- Make sure that the printer access controls are not preventing policy updates from working correctly.
 - 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, do either of the following:

- For e-Task 5 printers, click **Settings > Security > Login Methods**.
From the Public section, click **Manage Permissions**. Expand **Function Access** and **Device Management**, and then select **Create Profiles** and **Remote Management**.
- For e-Task 4, e-Task 3, e-Task 2+, e-Task 2, or e-Task printers, click **Settings > Security > Security Setup > Access Controls**.
Expand **Management** and **Function Access**, and then set Remote Management and Create Profiles or Use Profiles to **No Security**.

4 Click **Submit**.

5 In LMC, perform a policy update. For more information, see [“Updating policies for device groups” on page 83](#).

- If you are using custom icons, then use smaller files.
- Make sure that your printer has the latest firmware updates. For more information, contact your Lexmark representative.

Policy updates failed for a printer

After a policy update, the printer remains marked “Out of Policy,” and the system log contains the message **Policy not deployed to xxx.xxx.xxx.xxx**.

Try one or more of the following:

- If the printer uses a basic security template with a password or PIN, then configure the device security service for the printer. For more information, see [“Configuring device security” on page 57](#).
- Make sure that the printer access controls are not preventing policy updates from working correctly.

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, do either of the following:

- For e-Task 5 printers, click **Settings > Security > Login Methods**.
From the Public section, click **Manage Permissions**. Expand **Function Access** and **Device Management**, and then select **Create Profiles** and **Remote Management**.
- For e-Task 4, e-Task 3, e-Task 2+, e-Task 2, or e-Task printers, click **Settings > Security > Security Setup > Access Controls**.
Expand **Management** and **Function Access**, and then set Remote Management and Create Profiles or Use Profiles to **No Security**.

4 Click **Submit**.

5 In LMC, perform a policy update. For information, see [“Updating policies for device groups” on page 83](#).

The printer returns to the home screen only after attempting to execute an LDD profile

If the AP Bundle is not installed or running, then the printer appears to be in policy after a policy update. The printer may return to the home screen only when you attempt to execute an LDD profile.

Try one or more of the following:

- Determine whether the AP Bundle is installed correctly:
 - 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, do one of the following:
 - For e-Task 5 printers, click **Apps**.
 - For e-Task 4 printers, click **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**.
 - 4** If the AP Bundle does not appear in the list of installed solutions, then continue with the troubleshooting procedure.
- Note:** If the AP Bundle is already installed, then make sure that it is in a running state. Otherwise, the problem may be with the solution itself. Contact your Lexmark representative.
- If the printer uses a basic security template with a password or PIN, then configure the device security service for the printer. For more information, see [“Configuring device security” on page 57](#).
 - Make sure that the printer access controls are not preventing policy updates from working correctly:
 - 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, do either of the following:
 - For e-Task 5 printers, click **Settings > Security > Login Methods**. From the Public section, click **Manage Permissions**. Expand **Device Management**, and then select **Firmware Updates**.
 - For e-Task 4, e-Task 3, e-Task 2+, e-Task 2, or e-Task printers, click **Settings > Security > Security Setup > Access Controls > Management**. Set Firmware Updates to **No Security**.
 - 4** Click **Submit**.
 - In LMC, do either of the following:
 - Perform a policy update. For more information, see [“Updating policies for device groups” on page 83](#).
 - Install the AP Bundle manually.

- 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, do one of the following:
 - For e-Task 5 printers, click **Apps > Installed Apps > Install an app**.
 - For e-Task 4 printers, click **Settings > Apps > Apps Management > Install a New App**.
 - For e-Task 3 printers, click **Settings > Device Solutions > Solutions (eSF) > Install**.
 - For e-Task 2+, e-Task 2, or e-Task printers, click **Settings > Embedded Solutions > Install**.
- 4 Locate and select the **ap.flc** file in the “\Lexmark\Solutions\apps\wf-ldss\firmware\” folder where an LDD server is installed, and then click **Open**. Depending on your printer model, click either **Install** or **Start Install**.

The solution stops responding

If the network connection is lost on some printers, then the solution may stop responding.

- 1 Make sure the network cable is plugged into the printer and into the appropriate network outlet.
- 2 Wait a few minutes to see if the network connection returns, and then access the solution.
- 3 If the solution does not continue, then do the following:
 - a Turn off the printer.
 - b Wait a few seconds, and then turn the printer on.
 - c Check the printer network settings and the status of the network. For more information, see the documentation that came with the printer. For help with your local network, contact your network administrator.

The solution cannot connect to the network

Check the local domain settings in the proxy server settings of the printer. If necessary, add the domain on the local network that will bypass the proxy server.

Solving client software problems

Cannot create new Lexmark Document Server ports

- 1 Make sure at least one server is online using the System Status task on the System tab in LMC.
- 2 Make sure you have a license installed for software clients:
 - a Click the **System** tab.
 - b Select **Licenses**.
 - c Make sure one of the listed licenses applies to clients, and is not expired.

For more information, see [“Obtaining licenses” on page 16](#).

- 3 Make sure the IP addresses or subnets of the computers that will access the profile and a solution have been assigned to a software client group.

For more information, see [“Assigning solutions to a software client group” on page 91](#).

- 4 Check your proxy, firewall, and other network settings on the client computer to make sure communication is allowed with the LDD load balancer.

System processes terminate unexpectedly when creating a Lexmark Document Server port

If a profile assigned to Lexmark Document Server port has a name with more than 14 characters, or if the port name used has more than 75 characters, then the processes explorer.exe and spoolsv.exe may terminate unexpectedly.

- 1 If a port was created before the error occurred, then delete the port using the Ports tab of the Properties dialog for the created print queue.

Note: For more information on accessing the properties for the Lexmark Document Server port, see [“Configuring a Lexmark Document Server port” on page 94](#).

- 2 If the profile used with the port has a name with more than 14 characters, then change it to one that has 14 characters or fewer. For more information, contact the person who developed the solution, or see the *Lexmark Document Distributor SDK Guide*.
- 3 Create a new port for the created print queue, using a name with 75 characters or fewer.
- 4 Restart the computer where you added the Lexmark Document Server port.

Cannot create or configure a Lexmark Document Server port

When User Account Control is enabled, install or configure the Lexmark Document Server port with administrative privileges.

Do one or more of the following:

- Create a print queue using the Lexmark Document Server port.
- Configure or add a Lexmark Document Server port in an existing print queue.

Note: For more information, see [“Configuring a Lexmark Document Server port” on page 94](#).

Jobs are not sent to the LDD system when using LDD printers

- 1 Make sure you have created a new printer Lexmark Document Server Port and assigned a print queue using an existing print driver to that port.

For more information, see [“Adding LDD printers on a client workstation or print server” on page 92](#).

- 2 Make sure you have a license installed for software clients:

- a Click the **System** tab in LMC.
- b Select **Licenses**.
- c Make sure one of the listed licenses applies to clients and is not expired.

For more information, see [“Obtaining licenses” on page 16](#).

- 3 Make sure a solution has been properly deployed to a software client group containing the software client.
For more information, see [“Assigning solutions to a software client group” on page 91](#).
- 4 Run Windows Update to make sure the latest updates for the .NET framework are installed.
- 5 Check your proxy, firewall, and other network settings on the client computer to make sure communication is allowed with the LDD load balancer.

Select'N'Send cannot send files to LDD

- 1 Make sure you have a license installed for software clients:
 - a From the System tab in LMC, select **Licenses**.
 - b Make sure one of the listed licenses applies to clients and is not expired.For more information, see [“Obtaining licenses” on page 16](#).
- 2 Make sure a solution has been properly deployed to a software client group containing the software client.
For more information, see [“Assigning solutions to a software client group” on page 91](#).
- 3 Check your proxy, firewall, and other network settings on the client computer to make sure communication is allowed with the LDD load balancer.

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 the Printers control panel in Windows, 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**.
- If you are using Microsoft Word and a solution always receives a page count of 1, then see the Microsoft Knowledge Base article KB919736 *The dmCopies member always returns a value of 1 when you try to retrieve the number of copies in a print job in Word* (support.microsoft.com/kb/919736).

Appendix

Prompts supported by single-function printers

Single-function printers do not support all prompts supported by multifunction printers. Lists of supported prompts are included in the table below.

	Touch screen printers	Non-touch screen printers
Supported prompts	<ul style="list-style-type: none"> • ArrayPrompt • AuthenticationPrompt¹ • BooleanPrompt • CustomVimIPrompt • ImageBooleanPrompt • ImageListPrompt • ImageMessagePrompt • IntegerPrompt • ListPrompt • MessagePrompt • NumericPrompt • PasswordPrompt • StringPrompt • NullPrompt 	<ul style="list-style-type: none"> • ArrayPrompt • AuthenticationPrompt^{1, 2} • BooleanPrompt • IntegerPrompt • ListPrompt • MessagePrompt • NumericPrompt • PasswordPrompt³ • StringPrompt² • NullPrompt⁴
¹ Requires a supported card reader. ² Supported by T654 and W850 models only. ³ Supports only numeric PINs in e-Task printers. 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

Not all printer models support double-byte characters. If your printer is not listed in the following table, then it does not support double-byte characters.

Printer model	Simplified Chinese	Traditional Chinese	Japanese	Korean
6500	✓	✓	✓	✓
C748	✓	✓	✓	✓
C792	✓	✓	✓	✓
C925	✓	✓	✓	✓
C950	✓	✓	✓	✓
CS510	✓	✓	✓	✓

Printer model	Simplified Chinese	Traditional Chinese	Japanese	Korean
CS720	✓	✓	✓	✓
CS725	✓	✓	✓	✓
CS820	✓	✓	✓	✓
CX410	✓	✓	✓	✓
CX510	✓	✓	✓	✓
CX725	✓	✓	✓	✓
CX820	✓	✓	✓	✓
CX825	✓	✓	✓	✓
CX860	✓	✓	✓	✓
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	✓	✓
X860, X862, X864	✓	✓	X	✓
X925	✓	✓	✓	✓

Printer model	Simplified Chinese	Traditional Chinese	Japanese	Korean
X940, X945	✓	X	✓	✓
X950, X952, X954	✓	✓	✓	✓

Notices

Edition notice

July 2016

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

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

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

For Lexmark technical support, visit <http://support.lexmark.com>.

For information on supplies and downloads, visit www.lexmark.com.

© 2016 Lexmark International, Inc.

All rights reserved.

Trademarks

Lexmark, the Lexmark logo, and Perceptive Content are trademarks or registered trademarks of Lexmark International, Inc. or its subsidiaries 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 Inc.

Java is a registered trademark of Oracle and/or its affiliates.

Microsoft, Windows, Windows Server, Windows Vista, SharePoint, Internet Explorer, SQL Server, and C++ are either registered trademarks or trademarks of the Microsoft group of companies in the United States and other countries.

All other trademarks are the property of their respective owners.

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

Copyright (c) 2000-2002 The Apache Software Foundation. All rights reserved.

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

A

- accessing Lexmark Management Console 34
- accessing LMC
 - troubleshooting 103
- accessing the System Health dashboard 52
- adding a report 60
- adding LDD printers on a client workstation 92
- adding LDD printers on a print server 92
- adding licenses to an existing server 57
- adding servers after initial installation 49
- adjusting limits on concurrent jobs 53
- Advanced Prompting Bundle
 - troubleshooting 112
- antivirus policy
 - configuration 28
 - recommendation 28
- antivirus policy requirements and recommendations 28
- AP Bundle
 - updating 52
- assigning privileges to groups 36
- assigning servers to run LMC only or process jobs 55
- assigning solutions to software client groups 91
- authentication
 - changing the administrator password 35
 - changing the administrator user name 35
 - enabling LDAP server
 - authentication for LMC 35
- avoiding conflicts with other software 15

B

- backing up the database manually 68

- backup and restore
 - connecting existing servers during recovery 66
 - installing new servers during recovery 66
 - recovering backup data with a new installation 65
 - recreating LDD printer ports after an address change 67
- backup data
 - recovering with a new installation 65
- backups
 - scheduling 64
- browser displays a 5yy error when accessing LMC 103
- built-in reports 59

C

- cannot connect to Microsoft SQL Server database 106
- cannot create new Lexmark Document Server ports 113
- cannot create or configure Lexmark Document Server port 114
- capturing documents 5
- changing the administrator password 35
- changing the IP address on a configuration 1 system 50
- client software
 - adding LDD printers 92
 - increasing LDD print queue availability 94
 - installing 91
 - installing on a Microsoft Cluster Server 92
 - overview 9
- command line
 - running the Microsoft Windows application software Select'N'Send 98
- communication
 - ports used by LDD system 15
- communications
 - configuring NPA device communication 56
- components 6
 - uninstalling 51
- concurrency
 - adjusting limits on concurrent jobs 53
 - system sizing guidelines 21
- configuration 1 system
 - changing the IP address 50
- configuration type for workgroup systems 17
- configuration types 18
- configuring a Lexmark Document Server port 94
- configuring an eSF application associated with a solution 71
- configuring connection to an SMTP server 56
- configuring default report options 61
- configuring device security 57
- configuring global settings
 - cSF apps 70
 - solutions 70
- configuring Kerberos authentication 31
- configuring Kerberos authentication on printers 32
- configuring LDD servers for Kerberos authentication 33
- configuring SNMP for discovering printers 56
- configuring the confirmation page 48
- configuring the Select'N'Send GUI 96
- confirmation 6
- confirmation page
 - configuring 48
- conflicting software 15
- connecting existing servers during recovery 66
- creating a device group 74
- creating a device group from an existing group 74
- creating a new discovery profile 75

- creating custom reports
 - using special LDD parameters 62
- creating software client groups 90
- cSF app settings
 - understanding 69
- cSF apps
 - configuring global settings 70
 - removing 72
 - understanding solution settings 69
 - understanding the deployment process 69
- cSF Apps tab
 - tasks 41
- cSF Apps tab tasks 41
- custom reports
 - querying the database 62
 - understanding included subreports 63
 - using special LDD parameters 62
- customizing columns for jobs 46
- customizing columns for system logs 46
- customizing the home screen for a device group 79

D

- data is missing in LMC 104
- database
 - installing with clustering 25
 - installing without clustering 24
 - manually backing up 68
 - querying 62
 - restoring 68
- database servers 13
- default report options
 - configuring 61
- deploying solutions to device groups 78
- deployment process
 - understanding 69
- device discovery
 - troubleshooting 105
- device groups 74
 - configuring an eSF application associated with a solution 71
 - creating 74
 - creating a new discovery profile 75

- customizing the home screen 79
- deploying solutions 78
- disabling validation of eSF application deployment 84
- discovering missing printers 77
- discovering printers 77
- editing local settings for a deployed or assigned solution 71
- enabling secure communication between servers and printers 84
- importing a list of printers 76
- scheduling a discovery task 78
- scheduling policy updates 84
- updating policies 83
- viewing all printers with outdated policies 78
- viewing device group profile settings 46
- viewing software client group profiles 46

Device Groups tab tasks 38

- device log 102
- device profiles
 - viewing 86
- device security
 - configuring 57
- devices
 - adding to a device group 75
 - editing the home screen layout 85
 - enabling secure communication between servers and printers in a device group 84
 - removing from the system 87
 - searching previously discovered devices 85
 - updating policies 86
 - viewing profiles 86

Devices tab

- tasks 40

Devices tab tasks 40

- disabling validation of eSF application deployment 84
- disaster recovery 7
 - connecting existing servers during recovery 66
 - installing new servers during recovery 66

- manually backing up databases 68
- recovering backup data with a new installation 65
- recreating LDD printer ports after an address change 67
- discoveries frequently time out 105
- discovering devices
 - scheduling a discovery task 78
- discovering missing printers 77
- discovering printers 77
 - configuring SNMP 56
- discovery
 - configuring chunk size 55
- discovery and policy updates running slowly 105
- discovery task
 - scheduling 78
- document capture 5
- document processing 5
- document routing 6
- Documentum 12
- double-byte character support 116
- dynamic prompting 89
- dynamic prompting support 89

E

ECM

- supported platforms 12

- editing local settings for assigned or deployed solutions 71
- editing report settings 61
- editing the home screen layout on specific devices 85
- Embedded Solutions diagnostic log
 - viewing 102
- enabling LDAP server authentication for LMC 35
- enabling secure communication between servers and printers 84
- enabling secure communication between servers and the printers in a device group 84
- enterprise systems
 - installation overview 22
- error importing license 107
- error occurs when uploading a formset 104

- eSF application deployment
 - disabling 84
- eSF applications
 - configuring applications
 - associated with a solution 71
- eSF Configuration task for device groups does not function 104
- explorer.exe terminates unexpectedly 114
- exporting system status information 47
- E-Forms tab
 - tasks 41
- e-mail
 - configuring connection to an SMTP server 56

F

- failed policy updates 111
- FileNet 12
- formsets
 - troubleshooting, upload 104

H

- health of the system
 - monitoring 52
- home screen
 - customizing for a device group 79
 - editing layout on specific devices 85
 - troubleshooting 109
- Home tab 43
 - system status 44

I

- icon does not appear on the home screen after solution deployment 109
- ImageNow 12
- importing a list of software clients to software client group 91
- importing list of printers to a device group 76
- improving performance
 - assigning servers to run LMC only or process jobs 55
 - configuring chunk size 55
- inaccurate page counts
 - troubleshooting 115
- initial setup overview 10

- installation
 - adding servers after initial installation 49
 - configuration type 17
 - configuration types 18
 - overview for enterprise systems 22
 - overview for workgroup systems 17
 - preparing 15
 - system requirements 13
 - system sizing guidelines 21
- installation logs
 - viewing 101
- installation overview for enterprise systems 22
- installation types 17
- installing client software 91
- installing client software on a Microsoft Cluster Server 92
- installing database without clustering 24
- installing LDD 12
 - upgrading 30
- installing LDD components silently 29
- installing load balancer without clustering 24
- installing new servers during recovery 66
- installing servers 27
- installing system components in a workgroup system 17
- installing the database with clustering 25
- installing the load balancer with clustering 25

J

- JK Status Manager
 - assigning servers to run LMC only or process jobs 55
- jobs
 - customizing columns 46
 - viewing 45
- jobs are not sent to the LDD system when using LDD printers 114
- jobs do not respond after an error occurred 105

K

- Kerberos
 - troubleshooting 109
- Kerberos authentication
 - configuring 31
 - configuring LDD servers 33
 - configuring on printers 32
- Kerberos authentication is not working 109

L

- launching a solution from a printer 95
- LDAP server authentication
 - enabling for LMC 35
- LDD components
 - installing silently 29
 - uninstalling 51
- LDD elements
 - viewing information
 - summaries 45
- LDD parameters, special
 - using, for custom reports 62
- LDD print queues
 - using 95
- LDD printer ports
 - recreating after an address change 67
- LDD printers
 - adding on client workstation or print server 92
 - increasing LDD print queue availability using printer pooling 94
- LDD system
 - rebooting 50
 - troubleshooting, jobs 114
- LDSS Server
 - server unavailable 107
- LDSS Server is unavailable 107
- Lexmark Document Distributor
 - overview 5
 - system administration 10
 - system requirements 13
 - system sizing guidelines 21
- Lexmark Document Server Port
 - adding LDD printers on a client workstation or print server 92
- Lexmark Document Server port
 - increasing LDD print queue availability 94

- Lexmark Document Server ports
 - configuring 94
 - troubleshooting 113, 114
- Lexmark Management Console
 - overview 10
- Lexmark Management Console (LMC)
 - accessing 34
- Lexmark Solutions Application Server
 - restarting 51
- licenses
 - adding to an existing server 57
 - obtaining 16
 - troubleshooting 107
- licensing
 - adding licenses to an existing server 57
- LMC
 - LDAP server authentication 35
 - troubleshooting 103, 104
- LMC does not finish loading 104
- LMC responds very slowly 103
- load balancer
 - adjusting limits on concurrent jobs 53
 - assigning servers to run LMC only or process jobs 55
 - installing with clustering 25
 - installing without clustering 24
 - tuning for unequal servers 54
- local settings
 - editing for assigned or deployed solutions 71
- logs
 - customizing columns 46
 - Embedded Solutions diagnostic log 102
 - installation 101
 - viewing 45
 - viewing server 101

M

- managing scheduled tasks 48
- managing solution-related files 72
- manually backing up databases 68
- Microsoft Cluster Server
 - installing client software 92

- Microsoft SQL Server database 23
 - cannot connect 106
 - configuring LDD with 23
- Microsoft Windows application software Select'N'Send
 - running from the command line 98
- minimum system requirements 13
- sizing guidelines 21
- missing printers
 - discovering 77
- monitoring system health 52
- multiple systems
 - configuration types 18

N

- networking
 - ports used by LDD system 15
- NPA
 - configuring device communication 56

O

- obtaining LDD licenses 16
- one or more servers cannot be set offline 107
- one or more servers cannot be set online 106
- order of installation for enterprise systems 22
- outdated policies
 - viewing printers 78
- out-of-policy printers
 - viewing for all device groups 78
- overview
 - software client setup 89
 - system setup 10

P

- password, administrator
 - changing 35
- policies
 - scheduling policy updates 84
 - updating for device groups 83
 - updating on specific devices 86
- viewing printers with outdated policies 78

- policies, device
 - updating 86
- policy updates
 - configuring 75
 - configuring chunk size 55
 - scheduling 84
 - troubleshooting 105, 111
- policy updates failed for a printer 111
- ports
 - used by LDD system 15
- ports used by LDD system 15
- preparing for the installation 15
- print queues
 - using 95
- print server
 - adding LDD printers 92
 - increasing LDD print queue availability 94
- printer pooling
 - increasing LDD print queue availability 94
- printer returns to the home screen only after attempting to execute an LDD profile 112
- printers supported 11
- privileges setting 36
- processing documents 5
- profiles 5
 - accessing on a printer 95
 - viewing for a device group 46
 - viewing for a software client group 46
- profiles, device
 - viewing 86
- prompts
 - supported by single function printers 116

Q

- querying the database 62

R

- rebooting the LDD system 50
- recommended system requirements 13
- recovering backup data with a new installation 65
- recovery
 - connecting existing servers 66
 - installing new servers 66

- recreating LDD printer ports after an address change 67
- reliability 7
- removing a report 61
- removing devices from the system 87
- removing non-communicating servers 47
- removing solutions or cSF apps 72
- reports
 - adding 60
 - built-in 59
 - configuring default options 61
 - editing settings 61
 - querying the database 62
 - removing 61
 - running 57
 - scheduling 58
 - troubleshooting 104
 - understanding included subreports 63
- reports are not displayed when run 104
- restarting the Lexmark Solutions Application Server 51
- restoring the database manually 68
- routing documents 6
- running a report 57
- running the Microsoft Windows application software
- Select'N'Send from the command line 98

S

- scalability 7
- scheduled tasks
 - managing 48
 - viewing 48
- scheduling
 - reports 58
 - scripts 99
- scheduling a discovery task 78
- scheduling a report 58
- scheduling automatic backups 64
- scheduling policy updates 84
- scheduling scripts 99
- scripts
 - scheduling 99
- searching for devices 85

- secure communication
 - enabling between servers and printers in device group 84
- security
 - overview 10
- security overview 10
- Select'N'Send
 - configuring the GUI 96
 - troubleshooting 115
- Select'N'Send cannot send files to LDD 115
- server log contains Quartz errors 109
- server logs
 - viewing 101
- servers
 - adding after initial installation 49
 - adjusting limits on concurrent jobs 53
 - assigning to run LMC only or process jobs 55
 - connecting existing servers during recovery 66
 - installing 27
 - installing during recovery 66
 - removing non-communicating servers 47
 - setting online or offline 47
 - troubleshooting 107
 - tuning the load balancer for unequal servers 54
 - viewing and changing status 47
- servers cannot be set offline 107
- servers cannot be set online 106
- servers, LDD
 - configuring for Kerberos authentication 33
- services
 - configuring chunk size 55
 - configuring connection to an SMTP server 56
 - configuring NPA device communication 56
 - configuring policy updates 75
 - configuring the confirmation page 48
- Services tab tasks 42
- setting server status 47
- setting up multiple systems for high availability 18

- setting up software clients, overview 89
- SharePoint 12
- silent installation 29
- SMTP server
 - configuring connection to 56
- SNMP
 - configuring for discovering printers 56
- software client group
 - importing a list of software clients 91
- software client groups 88
 - adding software clients 90
 - assigning solutions to software client groups 91
 - creating 90
 - understanding 88
- Software Client Groups tab tasks 39, 42
- software client setup
 - understanding 89
- software clients 88
 - adding to a software client group 90
 - importing 91
 - understanding 88
 - understanding setup 89
- solution cannot connect to the network 113
- solution settings
 - understanding 69
- solution stops responding 113
- solutions
 - assigning to software client groups 91
 - configuring an eSF application associated with a solution 71
 - configuring global settings 70
 - deployed, editing settings 71
 - deploying to device groups 78
 - disabling validation of eSF application deployment 84
 - editing settings 71
 - launching from a printer 95
 - removing 72
 - troubleshooting 109
 - understanding solution settings 69
 - understanding the deployment process 69

- uploading to the LDD
 - system 70
 - viewing forms 47
 - workflow 8
- solutions are receiving inaccurate page counts 115
- solutions deployment
 - troubleshooting 109
- Solutions tab does not function 104
- Solutions tab tasks 41
- solution-related files
 - managing 72
- some printers on the network cannot be discovered 105
- spoolsv.exe terminates unexpectedly 114
- status bar 44
 - system status 44
- subreports
 - understanding 63
- supported database servers 13
- supported ECM platforms 12
- supported printers 11
- system administration
 - Lexmark Management Console 10
- system components 6
 - installing in a workgroup system 17
- system health
 - monitoring 52
- System Health dashboard
 - accessing 52
 - adjusting limits on concurrent jobs 53
 - tuning the load balancer for unequal servers 54
- system log
 - customizing columns 46
- system logs
 - viewing 45
- system overview
 - client software 9
 - Lexmark Management Console 10
 - system components 6
- system processes terminate unexpectedly when creating a Lexmark Document Server port 114

- system requirements 13
 - avoiding conflicts with other software 15
 - sizing guidelines 21
- system setup overview 10
- system sizing guidelines 21
- system status 44
- System tab
 - changing the administrator user name 35
 - managing scheduled tasks 48
 - viewing and changing server status 47
- System tab tasks 42

T

- tasks
 - System tab 42
- timeout
 - configuring policy updates 75
- troubleshooting
 - 500 Internal Server Error 103
 - 503 Service Unavailable 103
 - access controls 112
 - browser displays 5yy error when accessing LMC 103
 - cannot connect to Microsoft SQL Server database 106
 - cannot create new Lexmark Document Server ports 113
 - cannot create or configure Lexmark Document Server port 114
 - data is missing in LMC 104
 - device discoveries frequently time out 105
 - device discovery 105
 - discovery and policy updates running slowly 105
 - error in importing a license 107
 - error occurs when uploading a formset 104
 - eSF Configuration task for device groups does not function 104
 - explorer.exe terminates unexpectedly 114
 - formsets fail to upload 104
 - home screen 109
 - icon does not appear on the home screen after solution deployment 109
 - jobs are not sent to the LDD system when using LDD printers 114
 - jobs do not respond after an error occurred 105
 - Kerberos authentication is not working 109
 - LDSS Server is unavailable 107
 - Lexmark Document Server port cannot be created or edited 114
 - licenses 107
 - LMC 103, 104
 - LMC does not finish loading 104
 - LMC responds very slowly 103
 - one or more servers cannot be set offline 107
 - one or more servers cannot be set online 106
 - policy updates failed for a printer 111
 - printer returns to the home screen only after attempting to execute an LDD profile 112
 - reports are not displayed when run 104
 - Select'N'Send 115
 - Select'N'Send cannot send files to LDD 115
 - server log contains Quartz errors 109
 - servers 106, 107
 - slow device discovery 105
 - slow policy updates 105
 - solution cannot connect to the network 113
 - solution stops responding 113
 - solutions 109
 - solutions are receiving inaccurate page counts 115
 - solutions deployment 109
 - Solutions tab does not function 104
 - some printers on the network cannot be discovered 105
 - spoolsv.exe terminates unexpectedly 114
 - system processes terminate unexpectedly when creating a Lexmark Document Server port 114

- user can still access tasks even after removing privileges 104
- user cannot access some tasks in LMC 104
- tuning the load balancer for unequal servers 54

U

- understanding built-in reports 59
- understanding cSF app settings 69
- understanding deployment process 69
- understanding included subreports 63
- understanding installation types 17
- understanding software client groups 88
- understanding software client setup 89
- understanding software clients 88
- understanding solution settings 69
- unequal servers
 - tuning the load balancer 54
- uninstalling LDD components 51
- updating device policies 86
- updating policies for device groups 83
- updating the AP Bundle 52
- upgrading to LDD 4.9 30
- uploading solutions to the LDD system 70
- user can still access tasks even after removing privileges 104
- user cannot access some tasks in LMC 104
- user name
 - changing the administrator user name 35
- using LDD print queues 95
- using special LDD parameters 62

V

- version information 47
- viewing and changing server status 47
- viewing device profiles 86

- viewing forms associated with a solution 47
- viewing information summaries for LDD elements 45
- viewing installation logs 101
- viewing jobs 45
- viewing printers with outdated policies 78
- viewing scheduled tasks 48
- viewing system logs 45
- viewing the Embedded Solutions diagnostic log 102
- viewing the server logs 101
- viewing version information 47

W

- workflow solutions 8
- workgroup system
 - installing system components in 17
- workgroup systems
 - installation overview 17
- WorkSite 12