Lexmark Data Collection Manager 5.0.0

Reference Guide

July 2011 **www.lexmark.com**

740 West New Circle Road
Lexington, Kentucky 40550

Version: 1.2

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.

Lexmark Global Services rights of intellectual property are applicable to the document contents. The information contained herein is for the exclusive internal use for Lexmark International, Inc. and this document, or parts cannot be passed to third parties without the written agreement of Lexmark Global Services.

Trademarks

Contents

Introducing the Lexmark Data Collection Manager

What is the Lexmark Data Collection Manager?

Distributed Fleet Management (DFM) is a Lexmark Managed Print Services (MPS) solution for those customers seeking to optimize their enterprise wide fleet of output devices. These services are designed to provide visibility to the customer into their fleet of assets while alleviating the administrative burden of managing these assets, driving output costs down and improving paper-based workflow processes.

To perform the various services included in the DFM solution, Lexmark needs to collect output device data in an efficient and timely manner, with minimal impact to the customer's environment. The Lexmark Data Collection Manager (LDCM) is a key component used by Lexmark to facilitate this requirement and increase the efficiency in DFM engagements. All information collected is treated as strictly confidential and only used for the purposes mentioned above.

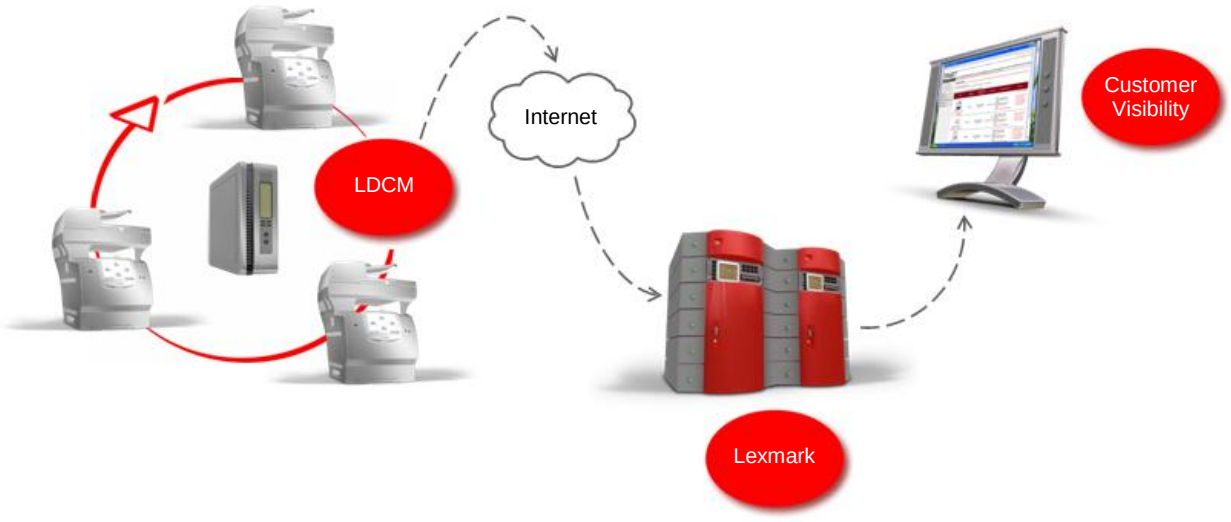
LDCM is a suite of Lexmark proprietary applications that resides on a dedicated networked server or personal computer (PC) within a customer's network, which performs the following tasks:

- Device monitoring
- Device discovery
- Data transmission

By having LDCM perform its scheduled tasks in an automated manner, the customer is able to concentrate their resources to performing the operations and services that they offer to their customers, rather than having to manage their internal output devices on a daily basis.

The data collected by LDCM is hosted and managed by Lexmark which lessens the need for customer to invest in its own management tools and infrastructure. For qualified accounts, Lexmark will provide the hardware required to host the LDCM software. If the customer needs to use server based hardware or has custom Standard Operating Environment (SOE) requirements, then they may need to supply the hardware and associated Operating System.

The LDCM technology coupled with Lexmark's proven business processes/methodologies and experienced resources will help customers tap into one of the best opportunities for sustained operational cost savings. DFM will help customers print less, move information faster, and better manage output across their organization.



Understanding Lexmark Data Collection Manager components

Understanding LDCM terminology

Within this document:

- Printers and print servers are sometimes called devices.
- Distributed Fleet Management (DFM) is a comprehensive set of management services and capabilities which allow for improved control of your device portfolio while driving down cost. It is a customized, dynamic solution, tailored specifically to your company.
- Managed Print Services (MPS) can help you optimize the use of your printing assets, slash downtime, and save hard earned dollars through the management of your output fleet.
- Lexmark Data Collection Manager (LDCM) is a networked server or personal computer (PC) that provides a secure and automated way to collect customer asset information.
- Management Information Base (MIB) consists of a compilation of objects in a (virtual) database used to manage equipment (such as routers and switches) in a network.
- Multifunction Printer (MFP) is an office machine which includes the functionality of multiple devices, such as printer, scanner, photocopier, fax, and e-mail.
- Simple Network Management Protocol (SNMP) is used in network management systems to monitor network-attached devices for circumstances that require administrative attention.
- Network Printing Alliance Protocol (NPAP) addresses, defined in ISO/IEC 8348, are identifying labels for network endpoints used in OSI networking.
- Hypertext Transfer Protocol (HTTP) is an application-level protocol for distributed, collaborative, hypermedia information systems.
- Hypertext Transfer Protocol Secure (HTTPS) is not a separate protocol, but refers to the combination of a normal HTTP interaction over an encrypted Secure Sockets Layer (SSL) or Transport Layer Security (TLS) connection.
- Fully Qualified Domain Name (FQDN) is an unambiguous domain name that indicates the precise location in the Domain Name System's tree hierarchy through to a top-level domain and finally to the root domain.
- RSA is the first algorithm known to be suitable for signing as well as encryption, and one of the first vast advances in public key cryptography.
- ISA is a firewall and security product primarily intended to securely publish web servers and other server systems, provide stateful, application-layer firewall, act as a VPN endpoint, and to provide internet access for client systems in a Business Networking environment.
- NT LAN Manager (NTLM) is a Microsoft authentication protocol used with the SMB protocol.
- Extensible Markup Language (XML) is classified as an extensible language, because it allows the user to define the mark-up elements. XML's purpose is to assist information systems in sharing structured data, especially via the Internet, to serialize data and to encode documents.
- Secure Sockets Layer (SSL) is a cryptographic protocol that provides security and data integrity for communications over TCP/IP networks such as the Internet.
- Internet Protocol version 4 (IPv4) is the fourth revision in the development of the Internet Protocol (IP) and the first version of the protocol to be widely deployed.
- Internet Protocol version 6 (IPv6) is a version of the Internet Protocol (IP) that is designed to succeed Internet Protocol version 4 (IPv4).

What does Lexmark Data Collection Manager do?

Device Monitoring

LDCM collects output on managed devices from device meters, counters, and logs that measure usage statistics, service events, and current status alerts.

The data collected during the device monitoring collection process is temporarily stored within an Oracle XE database on LDCM. If the status of a device changes from the previous collection period (i.e. Ready status changes to a Toner Low status), then this information is packaged for data transmission back to Lexmark so that appropriate steps may be taken. Along with the status information, the database extracts page count information for all devices for data transmission back to Lexmark once per day.

Simple Network Management Protocol (SNMP) and Network Printing Alliance Protocol (NPAP) are used to communicate and collect data from output devices.

Note: *Managed Devices are those devices that Lexmark has been contracted to provide DFM services for and are identified within Lexmark's Asset Management System.*

Alert Monitoring

The Alert Monitoring process will listen for SNMP traps from network devices that have been configured to send trap alerts to the LDCM. If the contracted services require it, this provides for a more real-time monitoring solution. The set of data collected as a part of Alert Monitoring is the same as that collected in the Device Monitoring process.

Alert Monitoring is comprised of two components; the first is the actual network service that receives the device initiated SNMP traps. The second process performs a full Device Monitoring data collection when a device trap is received. This dual collection methodology is required because the standardized definition of a SNMP Trap does not contain enough device identification information to create a transactable event.

It is necessary to examine the service delivery needs of the managed print service against the potential additional network impact that enabling Alert Monitoring will generate. This additional network impact is impossible to completely characterize, as it is completely dependent on the volume of alerts generated by the devices within the managed fleet. That volume of alerting can be directly related to the usage volume and user practices within the environment, and thus is highly variable.

Simple Network Management Protocol (SNMP) and Network Printing Alliance Protocol (NPAP) are used to communicate and collect data from output devices.

Note: *Enabling Alert Monitoring also requires enabling and configuring SNMP Traps on the fleet of Managed Devices within the environment. This will require the use of a device configuration utility such as Lexmark MarkVision Professional or MarkVision Enterprise.*

Device Discovery

While device monitoring is limited to collecting data on a static IP address List or Hostname list, LDCM can also search specified subnets to identify output devices that are connected to the network, regardless of manufacturer. In addition, the system will extract device properties by looking for the associated data from within the device's Management Information Base (MIB). This allows Lexmark to identify if a device has moved within or has been added to the customer's environment.

Simple Network Management Protocol (SNMP) is used to communicate and collect data from output devices.

Device Inventory

Device inventory information includes the physical details of the Lexmark devices within a fleet. The current version of LDCM is capable of collecting details on the firmware levels of Lexmark devices only.

Simple Network Management Protocol (SNMP) and Network Printing Alliance Protocol (NPAP) are used to communicate and collect device inventory from output devices.

Device Statistics

In addition to the standard set of data needed to provide the services within Lexmark DFM, LDCM has the capability to collect other statistical information from certain Lexmark devices. This set of data contains more detailed statistics on the types and sizes of paper used by the device and the type of jobs executed on an MFP. However, the collection of this data does consume more bandwidth and requires additional time over and above the normal device monitoring described in the above sections. This is an optional service that can be provided after a consultation with a Technical Operations representative within your geography.

Simple Network Management Protocol (SNMP), Network Printing Alliance Protocol (NPAP), and TCP 6100/6110 are used to communicate and collect device statistics from output devices.

Data Transmission

Lexmark takes data security very seriously. Lexmark utilizes Secure Hypertext Transfer Protocol (HTTPS), an industry standard communication protocol for the World Wide Web with both encryption and authentication built in, to securely transmit data between the customer's network and Lexmark. At predefined intervals, LDCM connects to Lexmark over HTTPS to transmit the data collected from the customer's output devices. To complete the transmission, the customer must ensure that the LDCM is enabled to connect to the *.lexmark.com internet site via HTTPS.

Remote Monitoring/Maintenance of LDCM

At predefined intervals, LDCM checks into Lexmark's web server using HTTPS, reports uptime, pulls the specific configuration settings and/or software modules, and updates its configuration and software. The configuration settings include, but are not limited to, the time of the configuration update, the time to run data collection, list of managed devices, and the time to send the data to Lexmark.

Note: *The approximate bandwidth required for LDCM to perform a check-in is 35 KB per sending period. A typical sending period is approximately 5 minutes.*

Communication Protocols and Security

Communication Protocols

Lexmark Data Collection Manager uses TCP and UDP protocols to communicate with output devices such as printers, MFPs, and copiers. Simple Network Management Protocol (SNMP) and/or Network Printing Alliance Protocol (NPAP) are used to discover devices and then to retrieve device level data at predetermined intervals. These protocols require the following ports below to be open between the LDCM and the managed devices.

Port requirements

Port	Description
80/TCP	Establishes a HTTP connection needed for required software/system updates
443/TCP	Establishes a HTTPS connection
161 UDP	SNMP collects printer information
162 UDP	Receives SNMP traps from supported configured printer
6110/TCP, UDP	Lexmark collection port and printer
9300 UDP	Lexmark collection port and printer

Protocol requirements

Protocol	Description
Simple Network Management Protocol (SNMP)	SNMPv1 – RFC 1157, SNMPv2 – RFC 1441 & 1442, SNMPv3 – RFC 3411 & 3418
Network Printing Alliance Protocol (NPAP)	IEEE 1284.1

Internet Authentication

- **Web Authentication** – For security purposes, web traffic is routed through a specific type of firewall to prevent unauthorized electronic access to a network. Unlike a proxy server, a firewall does not require an IP/FQDN to function properly.
  - User ID – A user that has rights on the network firewall to go out to the Internet
  - User Password – If required, a password for the above user
- **Proxy** – A customer's proxy server acts as a mediator for requests from clients in search of resources from other servers.
  - HTTP Proxy – The IP address of FQDN of the ISA Proxy Server
  - HTTP Proxy Port – The port required for internet access (i.e. HTTP: 80, HTTPS: 443)
  - Proxy User Name – If required, a user that has rights to connect to the Internet on the customer's network
  - Proxy User Password – If required, a password for the above user
  - Proxy User Domain – Important, a domain is required to authenticate

Data Security

Across the Internet the communications that take place between LDCM and the web servers located within Lexmark's data centers are based on HTTPS. Lexmark uses an HTTPS combination of encryption technologies named asymmetric encryption (RSA via X.509 certificate) and symmetric encryption (3DES or AES). Asymmetric encryption RSA is based on the use of a public/private key pair, in which the key used to encrypt the data cannot be used to decrypt the data. RSA encryption is used to securely exchange a shared key that is used in a symmetric encryption algorithm such as 3DES and AES.

Using X.509 certificates as a key exchange technology, LDCM can be configured to take advantage of some additional benefits. For instance, when LDCM requests a connection back to the Lexmark web servers, it also requests an authenticated connection. By utilizing a VeriSign Class 3 signed certificate on the web server, Lexmark has made every effort to ensure that customer information is only sent to the correct systems. When LDCM establishes the secure connection back to Lexmark, the signed certificate provides assurance that the LDCM is in fact communicating with a valid Lexmark system.

LDCM Database

The decision to use database software was made primarily to increase performance and efficiency of LDCM operations by taking advantage of the structured storage that the database provides and the triggering capabilities to reduce decision logic contained within application code.

The LDCM Oracle XE database does not contain Personally Identifiable Information (PII), and does not maintain historical data beyond that which is necessary to determine the state-change of a device. Typically information used in the state-change detection of a device is discarded after 15 minutes. Additional security measures have also been implemented, such as, not using default database passwords, disabling unneeded accounts and permissions, and stored procedures created within the database are stored encrypted. Customer historical data is stored within the Lexmark DFM infrastructure which is located within the Lexmark data center. This historical data is protected from both physical and network access by various methods including enforced segregation of roles.

LDCM Database Updates

When Oracle releases any publicly available patch that applies to their XE product, Lexmark will acquire and validate the patch for functionality in relation to the LDCM. After testing, if Lexmark determines the Oracle XE patch is applicable to the LDCM, we will release an LDCM update where appropriate. The new LDCM version that contains the update will be produced and made accessible to the Lexmark geographies through the standard methods available today.

Device Information Collected

The data collected from output devices is dependant on the device's Management Information Base (MIB). However, the following information below is generally available and collected for reporting.

Category	Data Fields	Bandwidth	Ports
Device Discovery	Serial Number	1.5 Kb/ Device/Pull *(Needed basis only)*	161 UDP 9300 UDP
	IP Address		
	Host Name		
	Model		
	Lifetime Page Count		
	Color Lifetime Page Count		
	Maintenance		
Device Inventory	Serial Number	1.5 Kb/ Device/Pull *(Needed basis only)*	161 UDP 9300 UDP
	IP Address		
	Host Name		
	Model		
	Lifetime Page Count		
	Color Lifetime Page Count		
	Maintenance		
	Inputs		
	Outputs		
	Network		
	Storage		
	Supplies		
	Emulation		
	Firmware		
	Color Details		
	Duplex		
Device Statistics	Paper Size	15 Kb/Device/Pull *(Typically once per week)*	9300 UDP
	Sheets		
	Sides Mono		
	Sides Color		
	Paper Type		
	Sheets		
	Sides		

Category	Data Fields	Bandwidth	Ports
Device Status	Serial Number	2.0 Kb/ Device/Pull *(Typically every 15 minutes)*	161 UDP 9300 UDP
	IP Address		
	Host Name		
	Model		
	Lifetime Page Count		
	Color Lifetime Page Count		
	Maintenance		
	Contact		
	Location		
	Alert		
	Alert Code		
	Mac Address		
Alert Monitoring	Serial Number	2.0 Kb/ Device/ Per Alert 2.0 Kb/ Device/ Reconcile *(Typically every 15 minutes)*	161 UDP 9300 UDP
	IP Address		
	Host Name		
	Model		
	Lifetime Page Count		
	Color Lifetime Page Count		
	Maintenance		
	Contact		
	Location		
	Alert		
	Alert Code		
	Mac Address		

Note: *The bandwidth statistics listed above are only estimated due to the numerous variables that could affect data transmissions across a network.*

Understanding the system requirements

LDCM Specifications

The following are requirements for running Lexmark Data Collection Manager. Please consult with your Lexmark representative as these requirements could change based on the size and fleet of a customer's environment.

Specifications	
Processor type	x86-64 – 32 bit, 64 bit (I64 Not Supported)
Processor speed	2.0 GHz or greater
RAM	• 2 GB minimum • 3 GB Recommended (32 bit) • 4 GB Recommended (64 bit)
Hard drive	160 GB (7200 RPM)
Supported Operating systems	• Windows XP SP3 (x86) • Windows 7 (x86, x64) • Windows Server 2003 SP2 (x86) • Windows Server 2008 SP2 (x86, x64) • Windows Server 2008 R2 (x64)
Antivirus	Symantec AntiVirus or similar product. ***Note:*** *The monitoring of the installed LDCM folder will need to be disabled in order to avoid high CPU usage.*
.NET Framework	Microsoft .NET Framework 2.0 SP1 and 3.5

Note:

- *The LDCM needs to run on a dedicated platform.*
- *IPV4 must be enabled in order for the LDCM to function correctly.*
- *No Dynamic Network Address Translation (DNAT) for the IP address of the LDCM server.*
- *Lexmark does not support the use of Virtualized Server environments such as VMware. However, we have tested and validated that the installation will work on VMware ESX version 4.0.*
- *Windows on Windows (WoW64) is a subsystem of the Windows operating system that is capable of running 32-bit applications and is included on all 64-bit versions of Windows. This will need to be enabled on all supported 64 bit platforms using LDCM 5.0 or greater. The only current Microsoft operating system where this is not enabled by default is Windows Server 2008 R2 Hyper-V.*
- *The .Net framework version 3.5.1 on Windows Server 2008 R2 is disabled by default. This must be enabled before installing LDCM 5.0.0. Click **here** for step-by-step instructions.*
- *Lexmark does not recommend installing a Firewall between the LDCM and the devices that will be monitored. If a Firewall does exist, refer to the Port Requirements section to open the designated ports between the LDCM server and the monitored device.*