Lexmark Cloud Services

Security and Privacy White Paper

June 2024

www.lexmark.com

Contents

Overview

As cloud-based software solutions become prominent, discussions continue to revolve around security. When organizations implement a cloud-based solution, they put their trust in the solution provider to protect their data and deliver a secure platform.

Lexmark takes this trust seriously.

Cloud Print Management lets users print securely, retrieve documents, monitor print behavior, and view statistics. Users can also manage the printer configurations and monitor the status of printers.

Cloud Fleet Management lets partner and organization administrators manage their fleets, create and deploy printer configurations, monitor the status of printers, and view statistics.

The solution offers scalability and cost-effectiveness of print and on-demand content services, while maintaining the same levels of security, control, and performance.

This document is intended for Lexmark customers and Lexmark partners who are interested in understanding how the information assets are handled within Lexmark Cloud Services. The document also contains information on how the solution interacts with the information systems of the customer.

Frequently asked questions

How is customer data encrypted?

Data waiting to be uploaded to Lexmark Cloud Services is protected at rest using AES-256 encryption. While the data is in transit to Lexmark Cloud, Transport Layer Security (TLS) protects the data. Once the incoming print data is converted to a printer-ready format, it is again encrypted using an AES/CBC 256-bit encryption key unique to each file.

For Hybrid Print Management, data is never sent to Lexmark but is encrypted at rest, similar to how it is encrypted in Lexmark Cloud.

How are users authenticated?

User authentication and authorization are done using a token-based OAuth protocol for client access during the print job submission and release, device discovery, and enrollment processes.

For seamless identity management, Lexmark Cloud Services supports single sign-on identity federation with an OIDC or SAML 2.0 compliant provider using OAuth protocols. Lexmark Cloud Services can integrate securely with your existing identity management solution and does not store user passwords.

If federation with an OIDC or SAML 2.0–compliant provider is not an option, then Lexmark Cloud Services can manage the user credentials in a secure cloud-based authentication system.

How can customers audit user activity?

Administrators can track metrics that give them a clear picture of the print behavior of their users. You can view a summary of these statistics in the Lexmark Cloud Services web portal. You can also export data to a CSV file.

Security

Physical and operational security

Lexmark Cloud Services is instantiated in data centers in the United States and The Netherlands that comply with ISO 27001 and SSAE 16 standards.

Network security

Lexmark Cloud Services exists inside a Virtual Private Cloud (VPC). It is a secure network logically isolated from other virtual networks in the hosting provider using private IP addressing, in accordance with RFC 1918.

- Access to the services within the VPC is controlled through security groups that allow traffic only on specific ports for both inbound and outbound traffic.
- Access to the VPC configuration and services configuration is controlled using the hosting provider management tools.
- Outgoing traffic is signed using a certificate from a trusted root certificate authority (CA).
- The Lexmark Network Operations Center (NOC) monitors all incoming and outgoing traffic for the VPC.
- The Network Intrusion Detection System (NIDS) monitors all network traffic within the VPC. The NIDS immediately notifies the NOC if any issue is detected.

Application security

Security is incorporated into every aspect of the development and the delivery of Lexmark Cloud Services.

- **Software design**—Potential security issues are identified as early as possible. Design documentation is peer-reviewed.
- **Code development**—Static code analysis tools are used to identify security issues. Peer code reviews are held on all changes.
- **Quality assurance**—Manual and automated security testing identifies potential security issues.
- **Before release**—Independent security service providers analyze and monitor Lexmark Cloud Services for potential security risks.

Lexmark Cloud Services provides two token-based authentication options:

- **Single sign-on federated authentication**—Lexmark Cloud Services provides single sign-on identity federation with an OIDC or SAML 2.0–compliant provider using OAuth protocols. The user credentials reside in your corporate identity management system, not in Lexmark Cloud Services.
- **Full identity management life cycle**—If federation is not an option, Lexmark Cloud Services handles the full identity management life cycle and manages user credentials in a secure cloud-based authentication system.

For customers who are using the Lexmark Cloud Services identity management support, the customer administrator can control the following password complexity requirements:

- The minimum password length can be configured from 8 to 64 characters.
- Password must contain any three of the following:
  - Uppercase characters
  - Lowercase characters

  - Special characters
  - Numbers

When users connect to Lexmark Cloud Services and are authenticated, they are assigned a token during their session. Before printing a document, the token is validated before any actions are performed.

Cookies used by the solution do not store any sensitive information on the user's system.

Lexmark Cloud Services uses the following methods to prevent, detect, and eliminate malware.

- Cloud Print Management converts only valid files.
- Documents submitted to Cloud Print Management through email are checked for malware before they are converted to PDF format.
- The supported file types are the following:

  .csv, .doc, .docx, .gif, .html, .jpg, .odp, .ods, .odt, .pdf, .ppt, .pptx, .rtf, .tiff, .txt, .xls, .xlsx

The database layer of Lexmark Cloud Services plays a significant role in security by ensuring the following:

- Each printed document is encrypted using AES/CBC 256-bit encryption using a separate key before being stored.
- Stored passwords are protected by a salted SHA/256 one-way cryptographic hash function.

After a document is printed, unless requested by the user, the file is deleted from the file system. The related metadata needed to show it in the user print queue is removed. Administrators can configure how long the jobs can be held in the queue before they are deleted, even if the jobs have not been printed.

Authentication

Cloud Print Management

Users are required to authenticate before they can submit and release jobs.

The following authentication methods are supported:

- User name and password
  - Workstation authentication during submission.
  - Mobile device authentication during submission and release.
- Badge authentication at the printer during release
- Secure login code at the printer during release when federated with the identity management system of the customer
  - The secure login code is a single-use code and expires in 15 minutes when not used.
  - The Lexmark Cloud Services Print Management web portal generates the secure login code. The Lexmark Mobile Print application can also be used on a device running the iOS operating system or the Android™ platform.
- PIN login at the printer during release
  - Replaces the user name and password when authenticating at the printer during release.
  - PINs are multiuse and a PIN expiry can be set.
  - The customer administrator determines the PIN length. The PIN length can be 4–12 digits.
  - The customer administrator determines how PINs are generated. The administrator can set the PIN to be user generated, administrator generated, or auto generated.
- Badge + PIN as second factor login at the printer during release

  Users are required to use both their badge and their PIN to release jobs.

The customer administrator determines which authentication methods are supported at the printer.

Cloud Fleet Management

Users are required to authenticate with their user name and password before they can discover and enroll printers.

Security policies and procedures

Lexmark Cloud Services are operated in accordance with the following policies and procedures to enhance security:

- Customer passwords are stored using a one-way salted hash.
- If there is suspicion of inappropriate access, then Lexmark can provide customers log entry records and their analysis to help in forensic analysis when available. This service is provided to customers on a time-and-materials basis.
- Data-center physical access logs, system infrastructure logs, and application logs are kept for a minimum of 90 days. Logs are kept in a secure area to prevent tampering.
- Passwords are not logged.
- Lexmark does not set a default password for a user. Passwords are reset to a random value that must be changed on first use, and delivered automatically through e-mail to the requesting user.
- Password reset email requests expire 14 days after an administrator generates it for creating a new user, or resetting a password for an existing user.

Intrusion detection

Lexmark, or an authorized third party, monitors Lexmark Cloud Services for unauthorized intrusions using network-based and host-based intrusion-detection mechanisms. Lexmark may analyze data collected from users' web browsers for security purposes. Data collected include device type, screen resolution, time zone, operating system version, browser type and version, system fonts, installed browser plug-ins, and enabled MIME types. These data are collected to detect compromised browsers, to prevent fraudulent authentications, and to make sure that the services function properly.

Security logs

Information from systems used in Lexmark Cloud Services is logged to their respective system log facility or to a centralized syslog server for network systems. These systems include firewalls, routers, network switches, and operating systems. Information is logged to enable security reviews and analysis.

Incident management

Lexmark maintains policies and procedures on managing security incidents. Lexmark notifies impacted customers without undue delay of any unauthorized disclosure of their respective customer data.

Lexmark publishes system status information on the Lexmark Cloud Services Platform Status. For more information, go to **https://status.one.lexmark.com**.

Reliability and backup

All networking components, network accelerators, load balancers, web servers, and application servers are configured in a redundant configuration.

All customer data submitted to Lexmark Cloud Services are stored on a primary database server with multiple active clusters for higher availability.

All customer data submitted to Lexmark Cloud Services are stored on highly redundant carrier-class disk storage and multiple data paths to ensure reliability and performance.

All customer data submitted to Lexmark Cloud Services, up to the last committed transaction, are replicated automatically to the secondary site on a near-real-time basis. Customer data are backed up to localized data stores. The backups are verified for integrity, and stored in the same data centers as their instance.

Disaster recovery

Production data centers are designed to mitigate the risk of single points of failure, and provide a resilient environment to support service continuity and performance. Lexmark Cloud Services uses secondary facilities that are geographically diverse from their primary data centers. Secondary facilities are equipped with hardware, software, and Internet connectivity that can be used in case Lexmark production facilities at the primary data centers are unavailable.

Lexmark has disaster-recovery plans in place and tests them at least once a year. The disaster-recovery exercise validates the ability to failover a production instance from the primary data center to the secondary data center. The exercise uses developed operational and disaster-recovery procedures and documentation.

The Lexmark Cloud Services disaster-recovery plans have the following objectives:

- Restoration of the Cloud service (recovery time objective) within 48 hours after Lexmark has declared a disaster
- Maximum customer data loss (recovery point objective) of 12 hours

  Note: These targets do not include a disaster or multiple disasters causing the compromise of both data centers at the same time. Development and test bed environments are also not included.

Analytics

Lexmark may track and analyze the usage of Lexmark Cloud Services for security purposes, as well as to improve both the product and the user experience. For example, Lexmark may use the information to understand and analyze trends, or track frequently used features to improve product functionality.

Lexmark may share anonymous usage data on an aggregate basis as part of doing our regular business. For example, we may share information publicly to show trends about the general use of our services.

Information collected by Lexmark

When you access or use Lexmark Cloud Services, the following information may be collected automatically:

- **Usage information**—User activity within Lexmark Cloud Services is monitored. Information such as applications and features used, actions taken within the system, and the type and configuration of printers you enroll may be collected.
- **Device information**—When a device is enrolled in Lexmark Cloud Services, a set amount of data is polled. This data includes the model, serial number, page counts, applications installed, configuration settings, and device logs for troubleshooting. This information is collected to help partners in deploying Lexmark Cloud Services.

How information is used

The information collected is used only for the limited purposes of Lexmark Cloud Services and its related functionality and services. These limited purposes are as described in this Privacy Notice and as permitted by applicable laws. These limited purposes include circumstances where it is necessary to fulfill your requested services, or where you have given us your express consent. Other purposes include the following:

- Provide, operate, maintain, and improve Lexmark Cloud Services.
- Send you technical notices, updates, security alerts, and support and administrative messages.
- Monitor and analyze trends, usage, and activities about Lexmark Cloud Services to help in future product development.
- Personalize and improve Lexmark Cloud Services, and provide features to customize your experience and match your usage and preferences.

Data and reports are not released, sold, reproduced, transferred, or otherwise exploited or disclosed.

Privacy

Data segregation

Lexmark Cloud Services segregates customer data, making sure that only authorized data is returned. A filtering layer between you and your data is developed, and operated in a multi-tenant architecture. The architecture is designed to segregate and restrict customer data access based on business needs. It also provides an effective logical data separation for different customers using customer-specific organization IDs, allowing the use of customer and user role-based access privileges. Further data segregation is established by providing separate environments for different functions, especially for testing and production.

Control of processing

Throughout the entire chain of processing activities, Lexmark and its third-party data processors, also called sub-processors, implement strict procedures. These procedures are designed to make sure that data is processed only as the customer has instructed. Lexmark and its affiliates have written agreements with their sub-processors. These agreements contain privacy, data protection, and data security obligations that provide a level of protection appropriate to their processing activities. Compliance with such obligations, and the technical and organizational data security measures implemented by Lexmark and its sub-processors are subject to regular audits.

Data security and encryption

Lexmark Cloud Services segregates customer data, making sure that only authorized data is returned. A filtering layer between you and your data is developed.

Data waiting to be uploaded to Lexmark Cloud Services is protected at rest using AES-256 encryption. While the data is in transit to the Lexmark Cloud, TLS protects the data. Once the incoming print data is converted to a printer-ready format, it is again encrypted using an AES/CBC 256-bit encryption key unique to each file.

Jobs submitted through e-mail are accepted only as Simple Mail Transfer Protocol (SMTP) content submitted using TLS.

The solution uses port 443 for SSL. If HTTPS communication across your firewall is enabled for the following domains, then Lexmark Cloud Services can transfer data and work with your existing system security.

European Data Center

- idp.eu.iss.lexmark.com
- login.microsoftonline.com
- lexmarkb2ceu.b2clogin.com
- lexmarkb2c.b2clogin.com
- b2ccustomizationsprodsa.blob.core.windows.net
- api.eu.iss.lexmark.com
- apis.eu.iss.lexmark.com
- eu.iss.lexmark.com
- prod-westeu-lex-cloud-iot.azure-devices.net
- apis.iss.lexmark.com

- iss.lexmark.com
- prod-lex-cloud-iot.azure-devices.net
- global.azure-devices-provisioning.net
- prodwesteulexcloudk8s54.blob.core.windows.net
- ccs.lexmark.com
- ccs-cdn.lexmark.com
- prodwesteulexcloudk8s199.blob.core.windows.net
- lpm.eu.iss.lexmark.com

North American Data Center

- idp.us.iss.lexmark.com
- login.microsoftonline.com
- lexmarkb2c.b2clogin.com
- b2ccustomizationsprodsa.blob.core.windows.net
- api.us.iss.lexmark.com
- apis.us.iss.lexmark.com
- us.iss.lexmark.com
- prod-lex-cloud-iot.azure-devices.net
- apis.iss.lexmark.com
- iss.lexmark.com
- global.azure-devices-provisioning.net
- prodlexcloudk8s239.blob.core.windows.net
- ccs.lexmark.com
- ccs-cdn.lexmark.com
- prodlexcloudk8s19.blob.core.windows.net
- lpm.us.iss.lexmark.com

The solution uses certificates from a trusted root certification authority.

Files are encrypted using AES/CBC (256-bit key).

Users are required to authenticate before they can submit and release jobs. The following authentication methods are supported:

- User name and password
  - Workstation authentication during submission
  - Mobile device authentication during submission and release
- Badge authentication at the printer during release
- Secure login code at the printer during release when federated with the identity management system of the customer
  - The secure login code is a single-use code and expires in 15 minutes when not used.
  - The Lexmark Cloud Services web portal generates the secure login code. The Lexmark Mobile Print application can also be used on a device running the iOS operating system or the Android platform.
- PIN login at the printer during release
  - Replaces the user name and password when authenticating at the printer during release.
  - PINs are multiuse and a PIN expiry can be set.

  - The customer administrator determines the PIN length (4–12 digits).
  - The customer administrator determines how PINs are generated. The administrator can set the PIN to be user-generated, administrator-generated, or auto-generated.
- Badge + PIN as second factor login at the printer during release
  - Users are required to use both their badge and their PIN to release jobs.

The customer administrator determines which authentication methods are supported at the printer.

Data retention policy

The following data sets are maintained, each with its own lifetime:

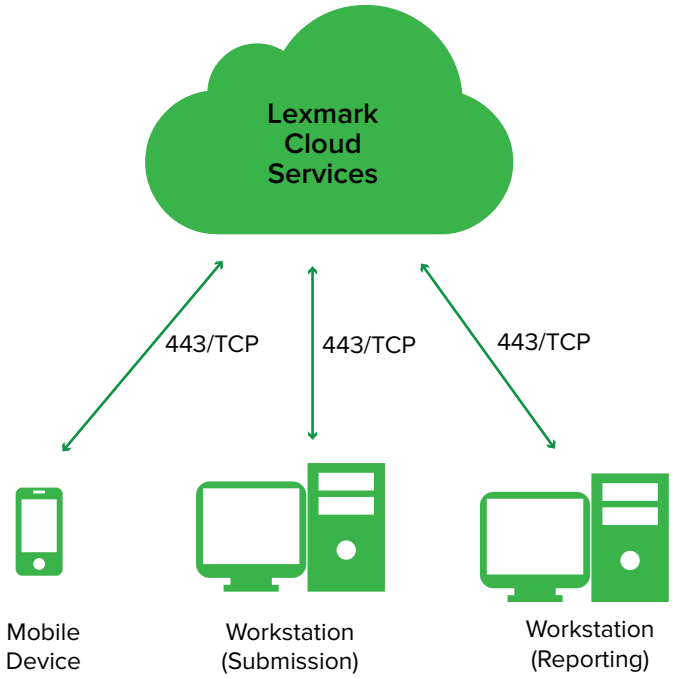
- **Analytics data**—This data is kept back to the time the organization was created.
- **Print job**—The jobs waiting to be released are held for an interval that the customer's print administrator has set. The interval can be set from one hour to seven days. When an interval for a job expires, the job is deleted from the Lexmark Cloud.
- **Print job history**—The personal history of what the user has printed. The print job history is retained for an interval that the print administrator has set. The interval can be set from one hour to seven days. Print history data older than the set interval is deleted and no longer shown.

Cloud Print Management

Cloud job submission

Using Lexmark Cloud Services, print jobs can be submitted to the Lexmark Cloud server from mobile devices and workstations using Lexmark applications. Print jobs can also be submitted through e-mail using a Lexmark Cloud e-mail address.

The Lexmark Cloud Reporting service provides the tracking of the job submission activity and various reports based on the user role.



Ports and protocols used during job submission

Port	Protocol	Function
443	HTTPS	• Job submission • Job information submission • Reporting

Note: For job submissions through e-mail, the print job is secured once it reaches Lexmark's inbox. A secure IMAP connection is used to retrieve the job from Lexmark's inbox.

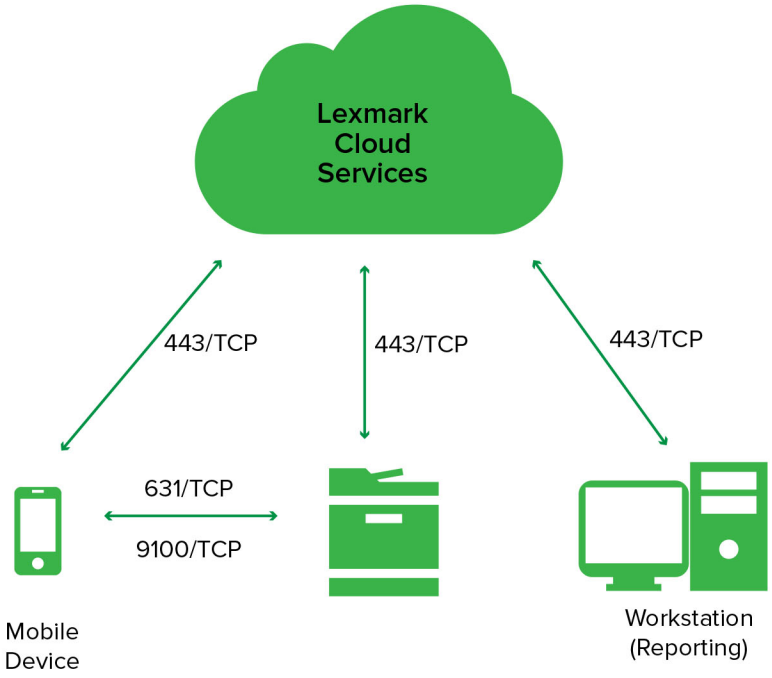
Submission categories

Category	Data collected	Purpose
Job submission	Native or rendered print file	Holding the file until it is deleted or printed
Job submission through e-mail	Native print file	Holding the file until it is deleted or printed
Job submission information	• Submission IP address • User ID • User e-mail address • Job or file name • Submission date • Number of pages • Pages per side • Color information • Two-sided printing information • Print driver • Submission source • Number of copies	Generating reports on print activity of the organization through the Analytics web portal

Cloud job release

Submitted print jobs can be released from Lexmark Cloud Services to any printer that supports the solution. Print jobs can also be released through a mobile device with the Lexmark Mobile Print application installed.

The Lexmark Cloud Services Reporting service tracks the job release activities. It also provides customized usage reports.



Ports and protocols used during job release

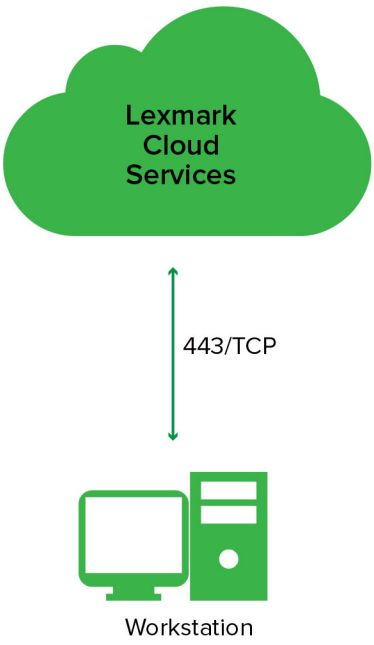
Port	Protocol	Function
443	HTTPS	• Job release • Job release statistics • Reporting
631 9100	TCP	Mobile job release

Release categories

Category	Data collected	Purpose
Job release	Native or rendered print file that the user submitted	Generating a printed version of the document that the user submitted to Lexmark Cloud Services
Job release statistics	• Job ID • Site • Submission IP address • User ID • User e-mail address • Job or file name • Submission date • Final date • Final action • Final site • Number of pages • Release IP address • Release user ID • Release method • Release model • Release model type • Release host name • Paper size • Two-sided printing information • Color information • Destination • Number of copies	Generating reports on print activity of the organization through the Analytics web portal

Hybrid job submission

In the Hybrid mode, print jobs are held locally on the user's workstation rather than being sent to the cloud. The workstation must have the Lexmark Print Management Client (LPMC) installed in Hybrid mode. The LPMC application informs the cloud that a print job is being held for release on the workstation and sends job information to the cloud.



Ports and protocols used during job submission

Port	Protocol	Function
443	HTTPS	• Workstation information • Job submission information

Submission categories

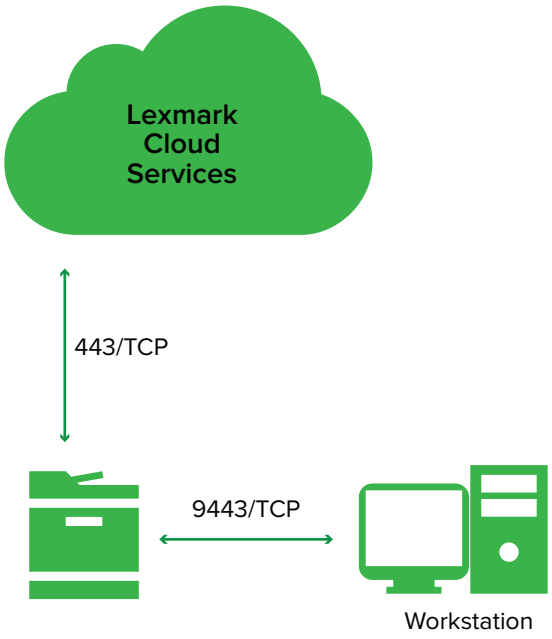
Category	Data collected	Purpose
Workstation information	• User ID • Workstation name • Workstation IP address	Identifying the workstation where print jobs are held

Category	Data collected	Purpose
Job submission information	• Submission IP address • User e-mail address • Job or file name • Submission date • Number of pages • Pages per side • Color information • Two-sided printing information • Print driver • Submission source • Number of copies	• Generating report on the organization print activity using the Analytics web portal • Tracking usage when print quotas are used

Hybrid job release

In the Hybrid mode, the printer receives workstation information from the cloud. The printer connects directly to the workstation that holds the Hybrid print job and pulls the job for printing. The printer reports the job information to the Lexmark Cloud Services.

The Analytics web portal provides the tracking of the job submission activity and other user reports.



Ports and protocols used during job release

Port	Protocol	Function
443	HTTPS	• Workstation information • Job release information
9443	TCP	Job release from workstation

Release categories

Category	Data collected	Purpose
Workstation information	• User ID • Workstation IP address	Identifying the workstations where the user is holding jobs to be printed
Job release from workstation	Print job held on the workstation	Generating a printed version of the document retrieved from the workstation
Job release information	• Submission IP address • User e-mail address • Job or file name • Submission date • Number of pages • Pages per side • Color information • Two-sided printing information • Print driver • Submission source • Number of copies	• Generating report on the organization print activity using the Analytics web portal • Tracking usage when print quotas are used

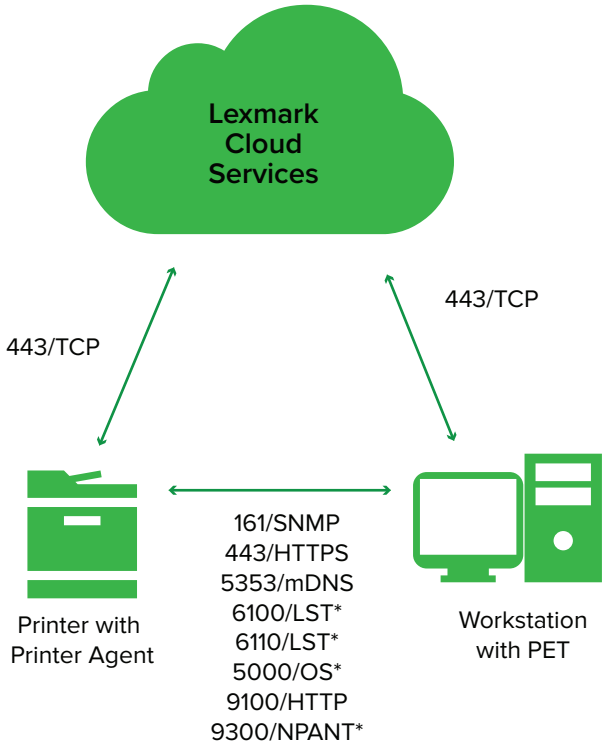
Cloud Fleet Management

Printer discovery

Printers must be enrolled to the Cloud Fleet Management web portal before they can be managed. You can manage printers using either the Printer Agent, Fleet Agent or Native Agent.

Using the Printer Agent

Printer discovery is done using the Printer Enrollment Tool (PET), a Lexmark workstation application. A Lexmark embedded application is installed on the enrolled printers. Enrolled printers regularly poll the Lexmark Cloud Services website for configuration changes or other tasks.



Ports and protocols used during discovery and enrollment using the Printer Agent

Port	Protocol	Function
161	SNMP	Printer discovery
5353	mDNS	
6100 UDP 6110 TCP	Lexmark Secure Transport (LST)*	
9300	NPA Network Transport (NPANT)*	
5000	ObjectStore (OS)*	
*The protocol is used in some Lexmark printer models.		

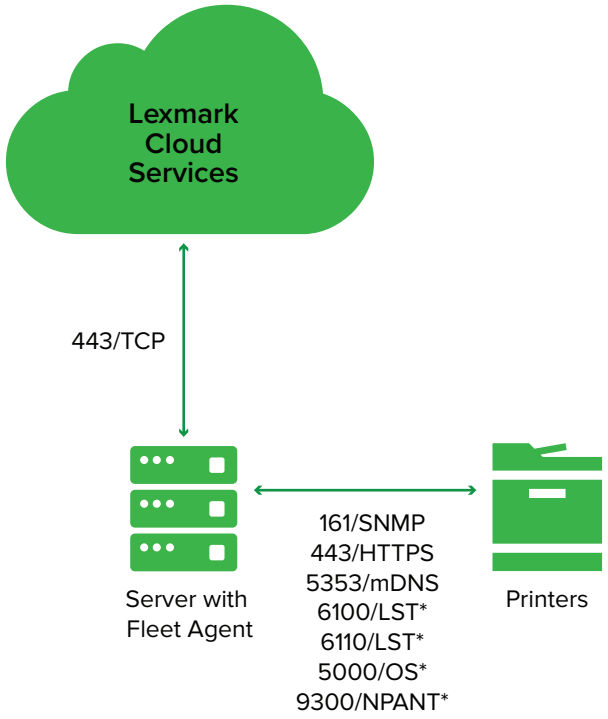
Port	Protocol	Function
443	HTTPS	• Printer enrollment • Printer setup
9100	HTTP	Printer enrollment
*The protocol is used in some Lexmark printer models.		

Printer Agent discovery and enrollment categories

Function	Action	Purpose
Printer discovery	Collects the following printer details: • Manufacturer • Model • IP address • Serial number	Identifying the printers that are eligible for enrollment
Printer setup	Downloads and installs the Printer Agent.	Enabling printer communication with the Lexmark Cloud Services
Printer enrollment	• Retrieves enrollment code from the cloud and initiate the connection from the printer to the cloud. • Shows the following agent information to the user: – Agent ID – Version – Polling interval – Logging level • Sends the following printer information to the cloud: – Model – Serial number – Manufacturer – IP address – MAC address – Host name – Contact name – Location – Asset tag – Time zone – Asset capabilities (color, two-sided printing, hard drive, fax, scan) – Firmware version – Installed applications – Alerts – Supplies – Page count	• Initiating enrollment and add the printer to the customer organization in the cloud • Confirming enrollment to the cloud • Providing the data required to manage the printer in the cloud

Using the Fleet Agent

Printer discovery and enrollment are done using the Fleet Agent. The Fleet Agent sends the printer information that it discovers to the Lexmark Cloud Services portal.



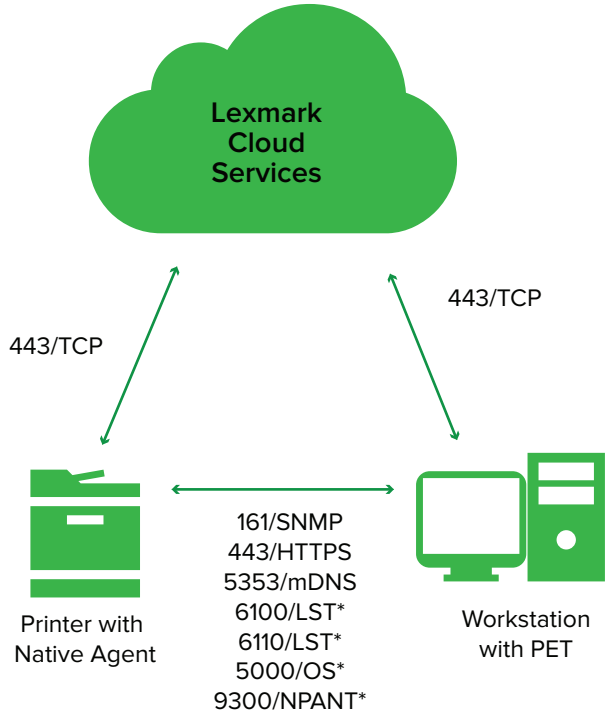
Ports and protocols used during discovery and enrollment using the Fleet Agent

Port	Protocol	Function
161	SNMP	Printer discovery
5353	mDNS	
6100 UDP 6110 TCP	Lexmark Secure Transport (LST)*	
9300	NPA Network Transport (NPANT)*	
5000	ObjectStore (OS)*	
443	HTTPS	• Fleet Agent setup • Printer enrollment
*The protocol is used in some Lexmark printer models.		

Fleet Agent discovery and enrollment categories

Function	Action	Purpose
Fleet Agent setup	Installs the Fleet Agent and activates it in the cloud.	Establishing connection with the cloud for printer configuration and management
Printer discovery	Collects the following printer details: • Manufacturer • Model • IP address • Serial number	Identifying printers that are eligible for enrollment
Printer enrollment	Sends the following printer information to the cloud: • Model number • Serial number • Manufacturer • IP address • MAC address • Host name • Contact name • Location • Asset tag • Time zone • Asset capabilities (color, two-sided printing, hard drive, fax, scan) • Firmware version • Installed applications • Alerts • Supplies • Page count	Providing the required data to manage the printer in the cloud

Using the Native Agent



Note: This workflow applies only to supported printers with firmware version 075.xx or later preinstalled in the factory.

1. Log in to the Lexmark Cloud Services website.
2. Pre-enroll the printers.
3. From the Embedded Web Server, enter the enrollment code to complete the enrollment.

Notes:

- The system assigns one enrollment code for all supported printers.
- To skip the pre-enrollment process, obtain the enrollment code from the Embedded Web Server.

After enrollment, the enrolled printers are listed on the Fleet Management web portal home page.

From the Fleet Management web portal, you can create and deploy printer configurations, view printer information, and request printer logs.

Ports and protocols used during discovery and enrollment using the Native Agent

Port	Protocol	Function
161	SNMP	Printer discovery
5353	mDNS	
6100 UDP 6110 TCP	Lexmark Secure Transport (LST)*	
9300	NPA Network Transport (NPANT)*	
5000	ObjectStore (OS)*	
443	HTTPS	• Printer enrollment • Printer setup
*The protocol is used in some Lexmark printer models.		

Native Agent discovery and enrollment categories

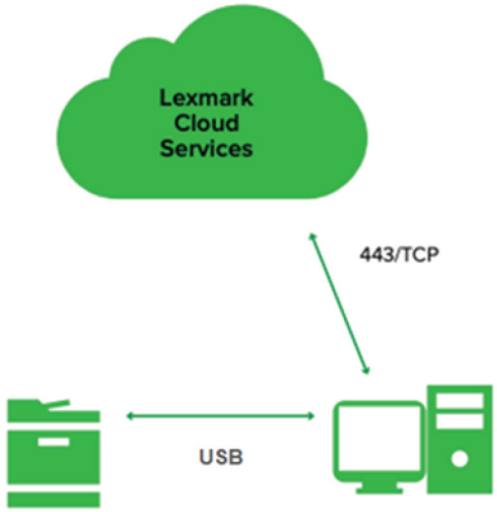
Function	Action	Purpose
Printer discovery	Collects the following printer details: • Manufacturer • Model • IP address • Serial number • Native Agent compatibility • Native device status	Identifying the printers that are eligible for enrollment
Printer setup	The Native agent is part of the firmware. Hence, PET does not perform a separate installation.	Enabling printer communication with the Lexmark Cloud Services

Function	Action	Purpose
Printer enrollment	• PET retrieves the enrollment code from the device. • Shows the following agent information to the user: – Agent ID – Version – Polling interval – Logging level • Sends the following printer information to the cloud: – Model – Serial number – Manufacturer – IP address – MAC address – Host name – Contact name – Location – Asset tag – Time zone – Asset capabilities (color, two-sided printing, hard drive, fax, scan) – Firmware version – Installed applications – Alerts – Supplies – Page count	• Initiating enrollment and add the printer to the customer organization in the cloud • Confirming enrollment to the cloud • Providing the data required to manage the printer in the cloud

Using the Local Agent

The Local Agent is a Fleet Management agent for managing USB-connected printers that otherwise do not have a means of communicating directly with Cloud Fleet Management. The Local Agent is a workstation application. Printer discovery and enrollment are done using the Local Agent. The Local Agent discovers printer information and sends it to the Lexmark Cloud Services portal.

Note: The Local Agent only supports Lexmark printers.



Ports and protocols used during discovery and enrollment using the Local Agent

Port	Protocol	Function
443	HTTPS	• Local Agent enrollment • Printer Agent enrollment
USB		Printer communication

Local Agent discovery and enrollment categories

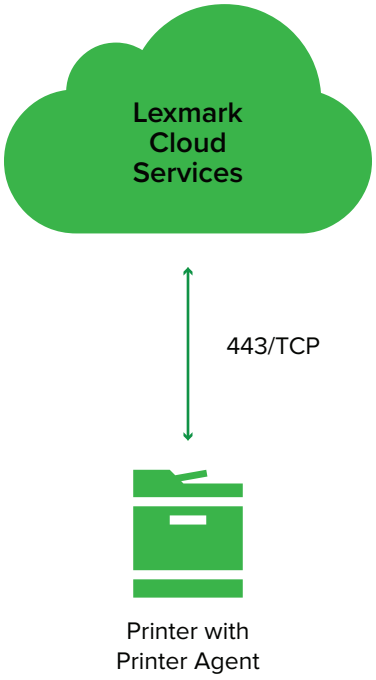
Function	Action	Purpose
Data Collection	Sends the following printer information to the cloud: • Manufacturer • Model • IP address • Serial number • IP address of the host personal computer • MAC address of the host personal computer • Host name of the host personal computer • Contact name • Location • Asset tag • Time zone • Asset capabilities (color, two-sided printing, hard drive, fax, scan) • Firmware version • Alerts • Supplies • Page count	Providing the required data to view and manage the printer in the cloud

Printer configuration and management

Several functions can be performed on printers that are enrolled to Lexmark Cloud Services. Printer applications can be installed or removed, printer firmware can be updated, and data can be collected and shown in the Cloud Fleet Management web portal.

Using the Printer Agent

All communications between the printer (Printer Agent) and the cloud are done using a secure HTTP (HTTPS) connection through port 443.



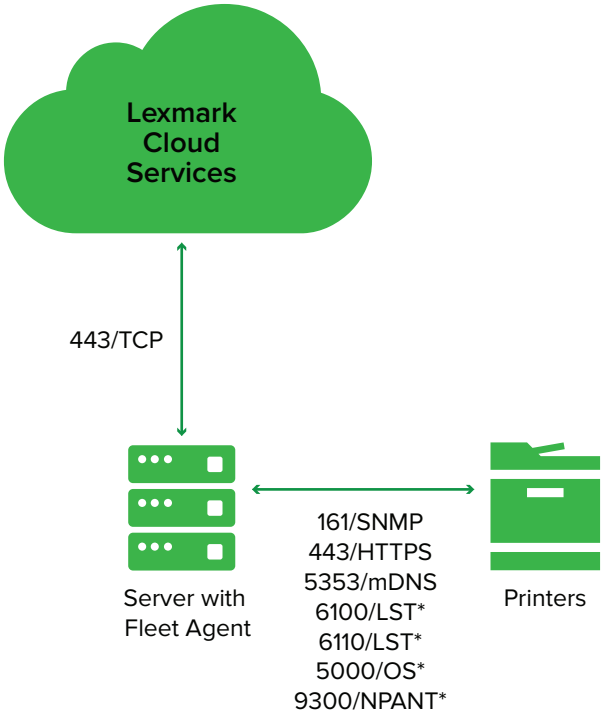
Ports and protocols used during a configuration update using the Printer Agent

Port	Protocol	Function
443	HTTPS	• Data collection • Printer configuration • Printer management

Configuration and management functions for the Printer Agent

Function	Action	Purpose
Data collection	Sends the following printer information to the cloud: • Model • Serial number • Manufacturer • IP address • MAC address • Host name • Contact name • Location • Asset tag • Time zone • Asset capabilities (color, two-sided printing, hard drive, fax, scan) • Firmware version • Installed applications • Alerts • Supplies • Page count	Providing the required data to view, configure, and manage the printer in the cloud
Printer configuration	Configures printers securely and remotely, such as upgrading the firmware, adding or removing applications, and changing settings.	Letting users configure their printers in the cloud
Printer management	Initiates actions on printers securely and remotely, such as rebooting, starting applications, stopping applications, and refreshing printer information.	Letting users manage their printer in the cloud

Using the Fleet Agent



Ports and protocols used during a configuration update using the Fleet Agent

Port	Protocol	Function
161	SNMP	• Data collection • Printer configuration • Printer management
5353	mDNS	
6100 UDP 6110 TCP	Lexmark Secure Transport (LST)*	
9300	NPA Network Transport (NPANT)*	
5000	ObjectStore (OS)*	
443	HTTPS	

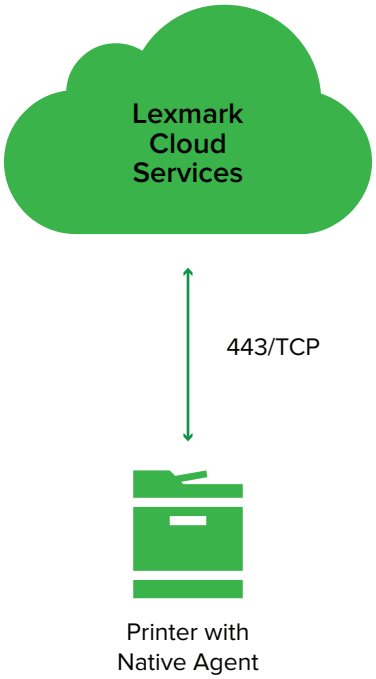
*The protocol is used in some Lexmark printer models.

Configuration and management functions for the Fleet Agent

Function	Action	Purpose
Data collection	Sends the following printer information to the cloud: • Model • Serial number • Manufacturer • IP address • MAC address • Host name • Contact name • Location • Asset tag • Time zone • Asset capabilities (color, two-sided printing, hard drive, fax, scan) • Firmware version • Installed applications • Alerts • Supplies • Page count	Providing the required data to view, configure, and manage the printer in the cloud
Printer configuration	Configures printers securely and remotely, such as upgrading the firmware, adding or removing applications, and changing settings.	Letting users configure their printers in the cloud
Printer management	Initiates actions on printers securely and remotely, such as rebooting, starting applications, stopping applications, and refreshing printer information.	Letting users manage their printer in the cloud

Using the Native Agent

All communications between the Native Agent and the cloud are done using a secure HTTP (HTTPS) connection through port 443.



Ports and protocols used during a configuration update using the Native Agent

Port	Protocol	Function
443	HTTPS	• Data collection • Printer configuration • Printer management

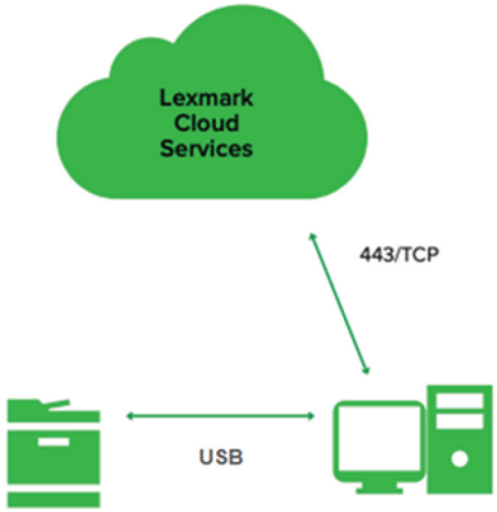
Configuration and management functions for the Native Agent

Function	Action	Purpose
Data collection	Sends the following printer information to the cloud: • Model • Serial number • Manufacturer • IP address • MAC address • Host name • Contact name • Location • Asset tag • Time zone • Asset capabilities (color, two-sided printing, hard drive, fax, scan) • Firmware version • Installed applications • Alerts • Supplies • Page count	Providing the required data to view, configure, and manage the printer in the cloud
Printer configuration	Configures printers securely and remotely, such as upgrading the firmware, adding or removing applications, and changing settings.	Letting users configure their printers in the cloud
Printer management	Initiates actions on printers securely and remotely, such as rebooting, starting applications, stopping applications, and refreshing printer information.	Letting users manage their printer in the cloud

Using the Local Agent

All communications between the Local Agent workstation application and the cloud are done using a secure HTTP (HTTPS) connection through port 443. All communications between the Local Agent and the printer are done using a USB connection.

Note: The Local Agent only supports Lexmark printers.



Ports and protocols used during a configuration update using the Local Agent

Port	Protocol	Function
443	HTTPS	• Local Agent enrollment • Printer Agent enrollment
USB		Printer communication

Configuration and management functions for the Local Agent

Function	Action	Purpose
Data Collection	Sends the following printer information to the cloud: • Manufacturer • Model • IP address • Serial number • IP address of the host personal computer • MAC address of the host personal computer • Host name of the host personal computer • Contact name • Location • Asset tag • Time zone • Asset capabilities (color, two-sided printing, hard drive, fax, scan) • Firmware version • Alerts • Supplies • Page count	Providing the required data to view and manage the printer in the cloud

Function	Action	Purpose
Printer management	Initiates action on printers securely and remotely to refresh printer information.	Letting users manage their printer in the cloud

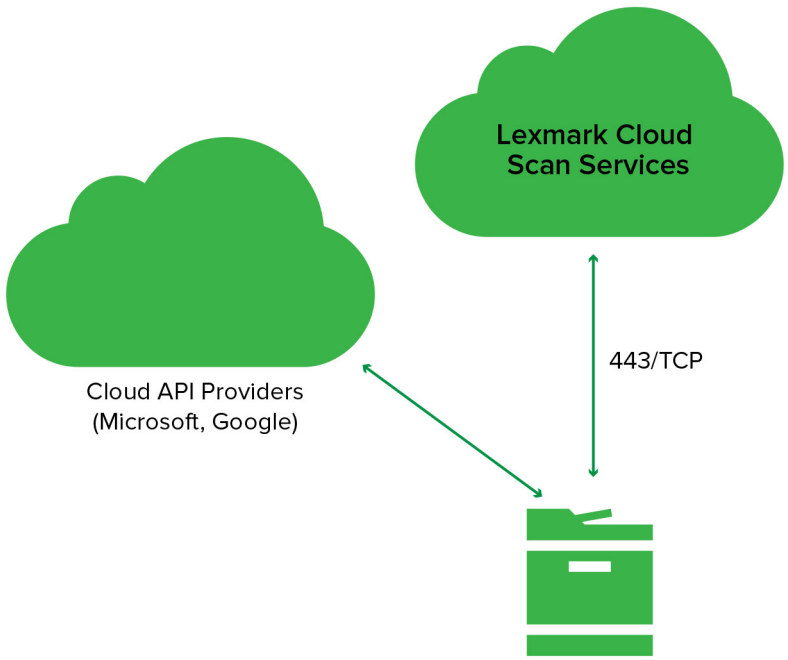
Cloud Scan Management

Device flow in Cloud Scan Management

To use Cloud Scan Management, you must have the Lexmark Cloud Services entitlement for Scan Management enabled and a Cloud Scan Management administrator or user role.

Device flow

Install the Cloud Scan eSF application to use the scan feature on any fleet-enrolled device.



Port information

Port	Protocol	Function
443	TCP	Communicates with Lexmark Cloud Scan services

Data transfer details

Category	Function
Target	Overrides scan option and links to provider location
Destination	Uploads location, provider, and scan options
Credentials	ID reference
Controls	Organization settings

Cloud service provider URLs

For Cloud Scan service to function correctly, it must be able to communicate with the following service provider URLs. Make sure that these URLs are accessible from your network environment:

- Box
  - api.box.com
  - upload.box.com
  - account.box.com
- Dropbox
  - api.dropboxapi.com
  - content.dropboxapi.com
- Google Drive
  - www.googleapis.com
- Microsoft
  - graph.microsoft.com

Notes:

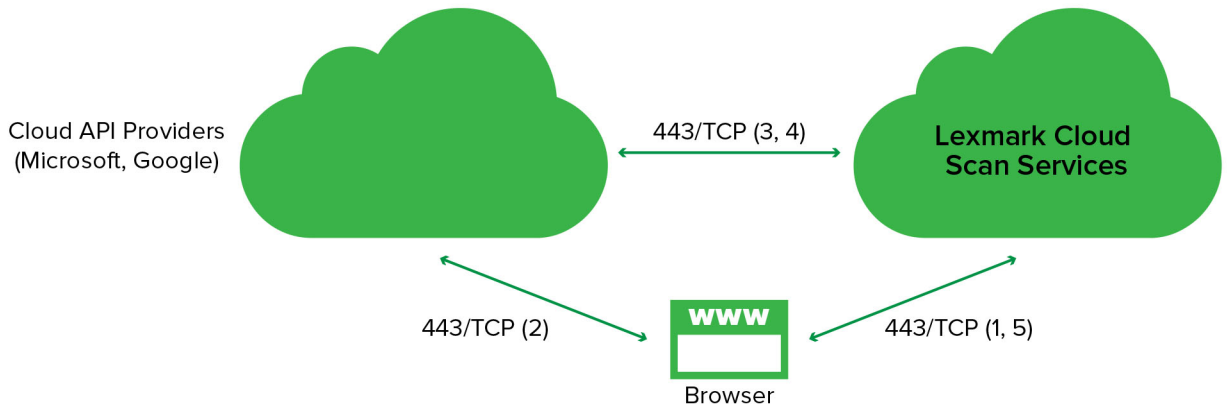
- These URLs are used by Cloud Scan for various functions, including profile creation and data transfer.
- Make sure that these URLs are not blocked by your firewall and are included in any proxy configurations if necessary.

Cloud flow in Cloud Scan Management

Cloud Scan Management is a workflow solution that integrates with cloud API providers. The solution can directly scan files to OneDrive, SharePoint, and Google Drive™. You must have a Lexmark Cloud Services account to use this solution. The third-party account details are stored and secured in the Lexmark Cloud Services server.

Cloud flow

- To scan, Lexmark Cloud Services uses the cloud storage provider account that is stored in the cloud server.
- With Identity Management, you can directly log in with cloud providers using OAuth2 on a browser.
- Cloud Scan communicates directly with cloud providers to establish a session.



Port information

Port	Protocol	Function
443	TCP	(1) Lexmark Cloud Services OAuth token
443	TCP	(2) Log in to cloud provider and authorize application
443	TCP	(3) OAuth tokens
443	TCP	(4) API access (Provider)
443	TCP	(4) API access (Lexmark Cloud Services)

Data transfer details

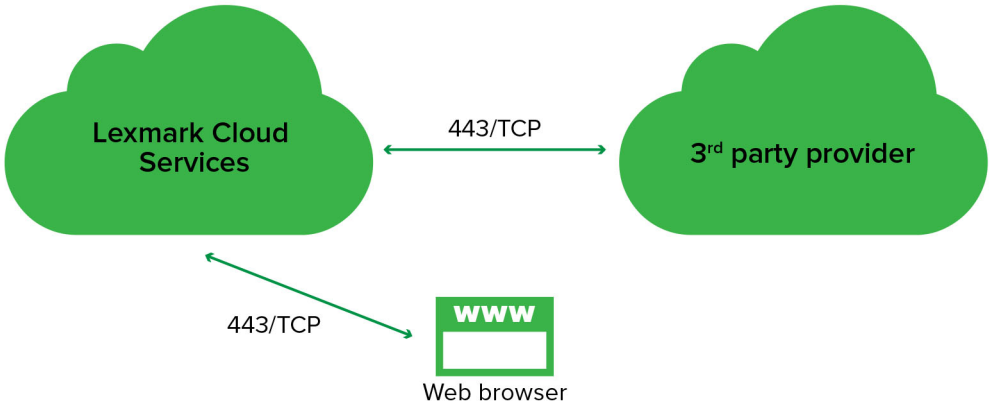
Category	Function
Authentication and authorization	Provider OAuth tokens (access token and refresh token) and Lexmark Cloud Services access token
API access	Access token and API requests, such as list folder, list folder items, and scan uploads

Translation Assistant Portal

Workflow in Translation Assistant Portal

The Translation Assistant Portal is a subscription service that lets you upload a file in a source language and translate it to a target language. The uploaded file is sent to the third-party translation provider. The translation provider provides a file link, which is valid for 15 minutes. Lexmark Cloud Services then retrieves the file from the translation provider. You can either e-mail it to the authenticated user using the Lexmark Cloud Service e-mail service or download it to your computer. The file is deleted from the cloud server after 24 hours.

Note: The Translation Assistant portal deletes both the original and translated files when the user has either downloaded or e-mailed the file. In error cases or cases where the browser is closed, the file remains until it is automatically deleted after 24 hours.



Before you begin, make sure that you have the following:

- Lexmark Cloud Services account
- Lexmark Cloud Services Organization entitlement for Translation Assistant
- Solution-specific Translation Assistant user role

Port information

Port	Protocol	Function
443	TCP	Communicates between the user's web browser and Lexmark Cloud Services. Securely communicates between Lexmark Cloud Services and the third-party translation provider.

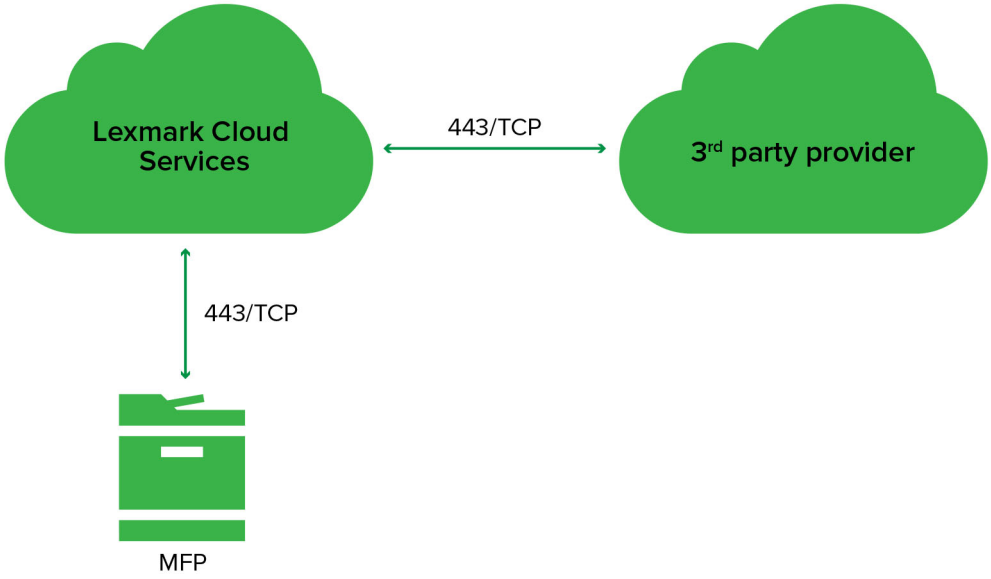
Data transfer details

Category	Function
Source	Upload a file from the user's computer to Lexmark Cloud Services using the web portal. The file size must not exceed 40MB.
Options	Language selections and destination selection (e-mail or download).
Credentials	ID reference and tokens.
Controls	Organization entitlements and user roles.

Workflow in Translation Assistant

Translation Assistant, an eSF application that runs on MFPs, works with Lexmark Cloud Services to provide users an easy way to scan documents on their MFP and have them translated by a third-party translation provider. Users can choose to have translated documents sent through e-mail or printed.

Note: Translation Assistant eSF application sends a scanned document to Lexmark Cloud Services. Lexmark Cloud Services then sends it to a third-party provider for translation. Lexmark Cloud Services sends the translated document to either the e-mail recipients or to the Translation Assistant eSF application to be printed.



Before you begin, make sure that you have the following:

- Lexmark Cloud Services account
- Lexmark Cloud Services Organization entitlement for Translation Assistant
- Printer hard disk
- A valid Optical Character Recognition (OCR) license on the printer

Port information

Port	Protocol	Function
443	TCP	Communicates between the MFP and Lexmark Cloud Services.

Data transfer details

Category	Function
Source	Scans from the MFP
Options	Language selections and destination selection (e-mail or print).
Credentials	Token
Controls	Organization entitlements

Regulatory compliance

Lexmark aims to uphold the highest standards possible.

We ensure compliance with the protection of user rights in the processing and protecting of personal data under the General Data Protection Regulation (GDPR) through the following:

- Processing of the subject data within the European Union
- Erasure of the data subject when removed from the system
- Inclusion of the data subject to the right to be forgotten

The data centers used for Lexmark Cloud Services have achieved the following:

- ISO 27001 certification
- PCI DSS certification
- SOC compliance

ISO/IEC 27001:2013

The information security management system for the managed print services provided by the Imaging Solution Services division of Lexmark passes the ISO/IEC 27001:2013 standards. For more information, see the **ISO/IEC 27001:2013 certification**.

Summary

Lexmark is an industry leader in document and device security. This expertise is the backbone of Lexmark Cloud Services, combining dedication to security with the lightweight ease of the cloud. Lexmark Cloud Services simplifies your print needs while offering the framework to manage your users and their activities. The solution lets you work better and more securely while reducing costs and expenses.

Using Lexmark Cloud Services, you can transmit and maintain your documents securely.

Notices

Edition notice

June 2024

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

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

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

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

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

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

GOVERNMENT END USERS

The Software Program and any related documentation are "Commercial Items," as that term is defined in 48 C.F.R. 2.101, "Computer Software" and "Commercial Computer Software Documentation," as such terms are used in 48 C.F.R. 12.212 or 48 C.F.R. 227.7202, as applicable. Consistent with 48 C.F.R. 12.212 or 48 C.F.R. 227.7202-1 through 227.7207-4, as applicable, the Commercial Computer Software and Commercial Software Documentation are licensed to the U.S. Government end users (a) only as Commercial Items and (b) with only those rights as are granted to all other end users pursuant to the terms and conditions herein.

Trademarks

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

Android is a trademark of Google LLC.

All other trademarks are the property of their respective owners.

Index