Remote Services at Xerox

Security White Paper

Version 5.0

2024

To ensure the efficient fulfillment of Xerox service offerings, we leverage global competency centers and cloud technology. This may result in the personal data we process being transferred beyond the European Economic Area (EEA), but within the parameters of the defined service offering. The level of protection afforded by General Data Protection Regulation (GDPR) is not undermined through data transfers, and all transfers undertaken by Xerox are carried out in full compliance with GDPR using an approved mechanism and subject to appropriate safeguards.

Changes are periodically made to this document. Changes, technical inaccuracies, and typographic errors will be corrected in subsequent editions.
.

IS 614672/IS 514590

Table of Contents

1. General Purpose and Audience

The Remote Services at Xerox security whitepaper is provided to help customers understand and deploy the secure remote services solution which works best with their network construct and information security policies. To ensure the most secure configuration method changes to the customer's internet firewall, web proxy servers, or other security-related network infrastructure may be required.

The target audience for this document includes technical vendors, network managers and network security professionals interested in the remote services capabilities and the security implementation of those features.

We recommend the document be reviewed in its entirety to certify the use of Xerox® Products and Services within a customer's networked environment.

2. Value Proposition

We offer a safe and secure way for device data to be sent to our ISO certified system to automate common tasks, provide a better service, and support experience.

- Billing meter reporting is automated and accurate.
- Automated supplies replenishment program provides toner based on the reported toner levels of the printer so there is no need to track inventory or call for supplies.
- Sending diagnostic information allows us to better support your device, often enabling quicker problem resolution.
- Certain printer models can check for important software updates and install the updates programmatically without customer intervention. See Note
- Our managed services capabilities also provide a way to manage non-Xerox branded printers in addition to Xerox-branded printers.
- These services allow our customers more efficient use of their time.

All of this is done with security in mind.

Note: This option can be disabled for environments where customers are certifying to a set software version and wish to control the print software when updates occur. This can be done without having to disable the remaining remote services capabilities.

3. Remote Services

Information is a key asset and security is paramount for all organizational assets, including networked multifunction print devices (MFPs). Today, managing a fleet of multi-function print devices while ensuring an acceptable level of security presents a set of unique challenges that are often overlooked. We understand this complexity and is responsive to our customers' security needs. Xerox® Products, Xerox® Systems and remote services offerings are designed to securely integrate with our customers' existing workflows while employing the latest secure technologies.

By default, no customer images from print, fax, scan, copy actions or other sensitive information is transmitted to our servers.

The U.S. based Xerox servers conform to stringent security requirements for Information Security Management. Our datacenters and remote services applications maintain the annual Statement on Standards for Attestation (SSAE) No-16, Sarbanes-Oxley Act (SOX) compliance requirements and are ISO 27001:2013 certified.

4. Deployment Models

Customers may choose between the following equally secure Xerox Remote Services deployment models:

- **Combination Model** – ***(Preferred Model)*** The implementation of both the Device Direct and Device Management Application Model together is ideal as it provides the most robust data set and device management capabilities.

- **Device Direct Model** - Device Direct enables print devices to communicate directly to the remote Xerox® Communication Servers via the internet through the customer's firewall to support Automatic Supplies Replenishment (ASR), Automatic Meter Reads (AMR) and device diagnostics reporting. This deployment model provides a set of data elements in the standard payload to include device faults, alerts, counters, High Frequency Service Items (HFSI), and other print device attributes.
- **Device Management Application Model** - Xerox® Device Management Applications can be deployed in a customer's network to collect a set of data attributes from print devices to also support Automatic Supplies Replenishment (ASR), Automatic Meter Reads (AMR) and device diagnostics reporting. Print device attributes are collected and then transmitted securely to the remote Xerox servers. Data attributes from both Xerox and non-Xerox print devices can be communicated as a part of this deployment model.

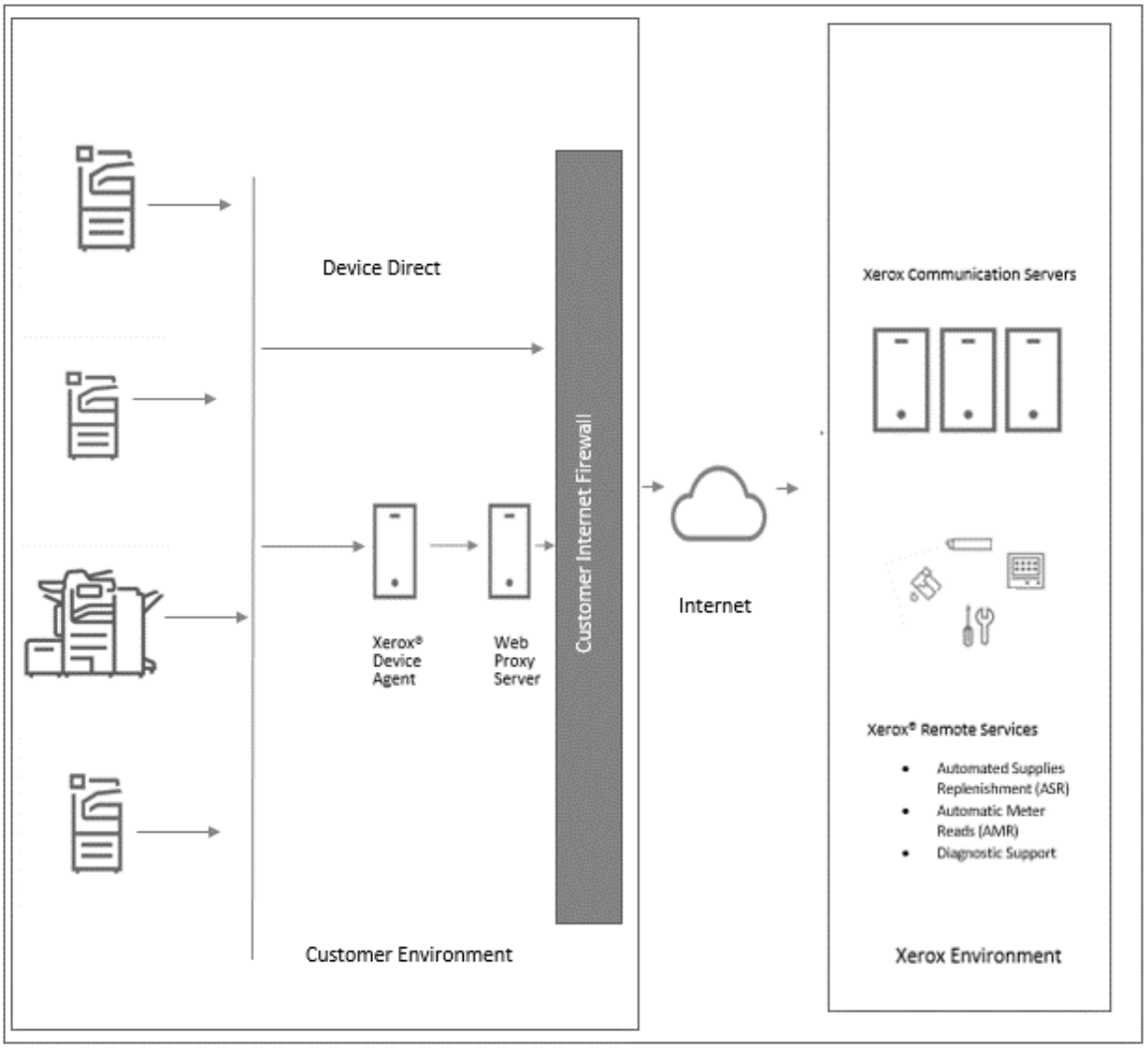
All deployment models for remote services are equally secure and leverage the latest industry standard web-based protocols and ports to establish a secure, encrypted channel when transmitting print device attributes externally to the remote Xerox servers located within our redundant secured datacenters.

The deployment model chosen depends upon our customers' type of print service solution, information security policies and rules for handling the transmission of the print device data attributes.

Combination Deployment Model (preferred)

The Combination Deployment is deployed when a customer purchases multiple types of Xerox maintenance agreements for their print devices and to achieve a more robust remote services solution. When a Xerox® Print Device is initially installed on a network, the default Xerox remote services behavior is for the print device to automatically attempt to communicate outbound to our communication servers using a secure, authenticated connection method.

Figure 1



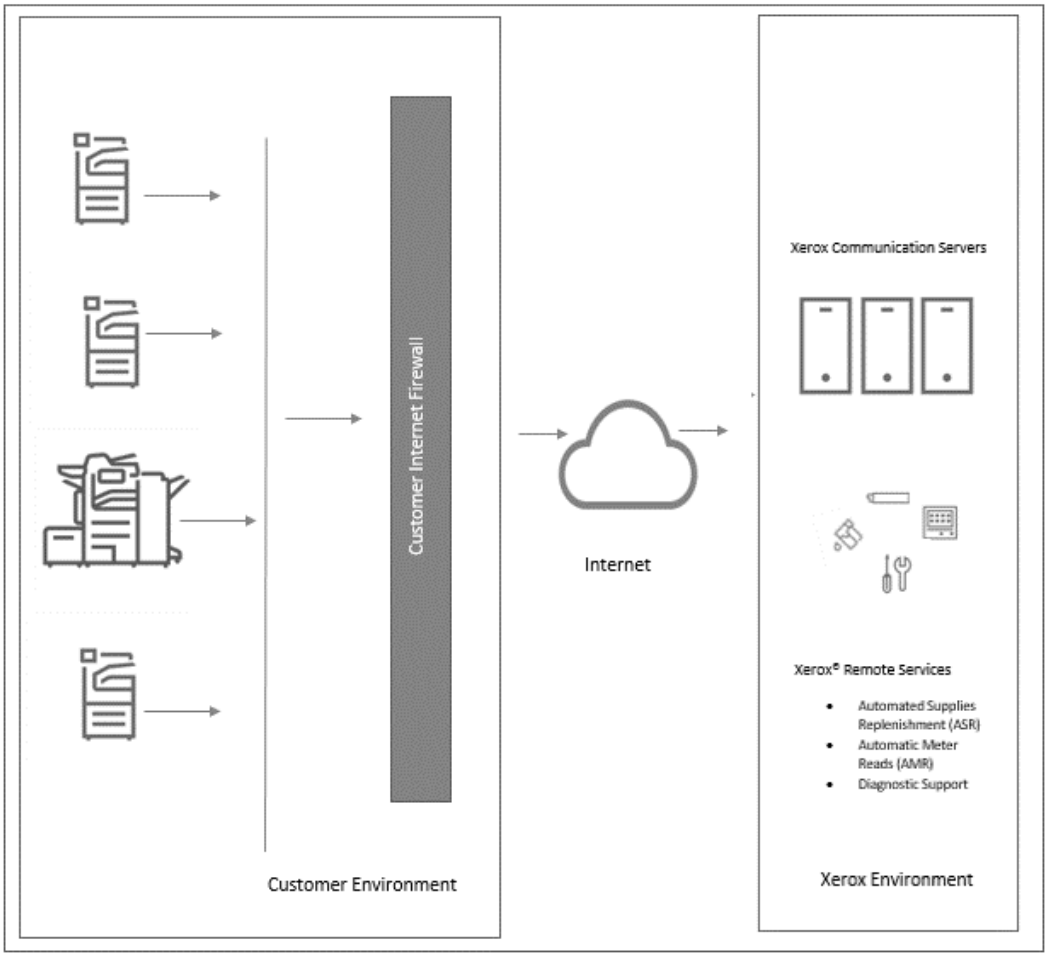
Combination Deployment Model

Device Direct Deployment Model

Remote Services capable Xerox® Devices utilize a Transport Layer Security (TLS) 1.2 protocol connection over the secure standard port 443 to communicate outbound to our secure servers.

- Print devices within the customer environment initiate all communications with the communication servers. Standard firewall configurations on the site are required to enable communication.
- A valid URL for the communication servers must be used (*.support.xerox.com) to authenticate print devices to the Xerox infrastructure. CNAMEs are recommended to communicate through the Imperva Web Application Firewall (WAF)
- The device requests a registration with the communication servers using the certificate authentication appropriate credentials.
- The communication servers validate the credentials supplied by the printers and accept the requests.
- The communication servers are behind a secure firewall and are not accessible from the internet.

Figure 2



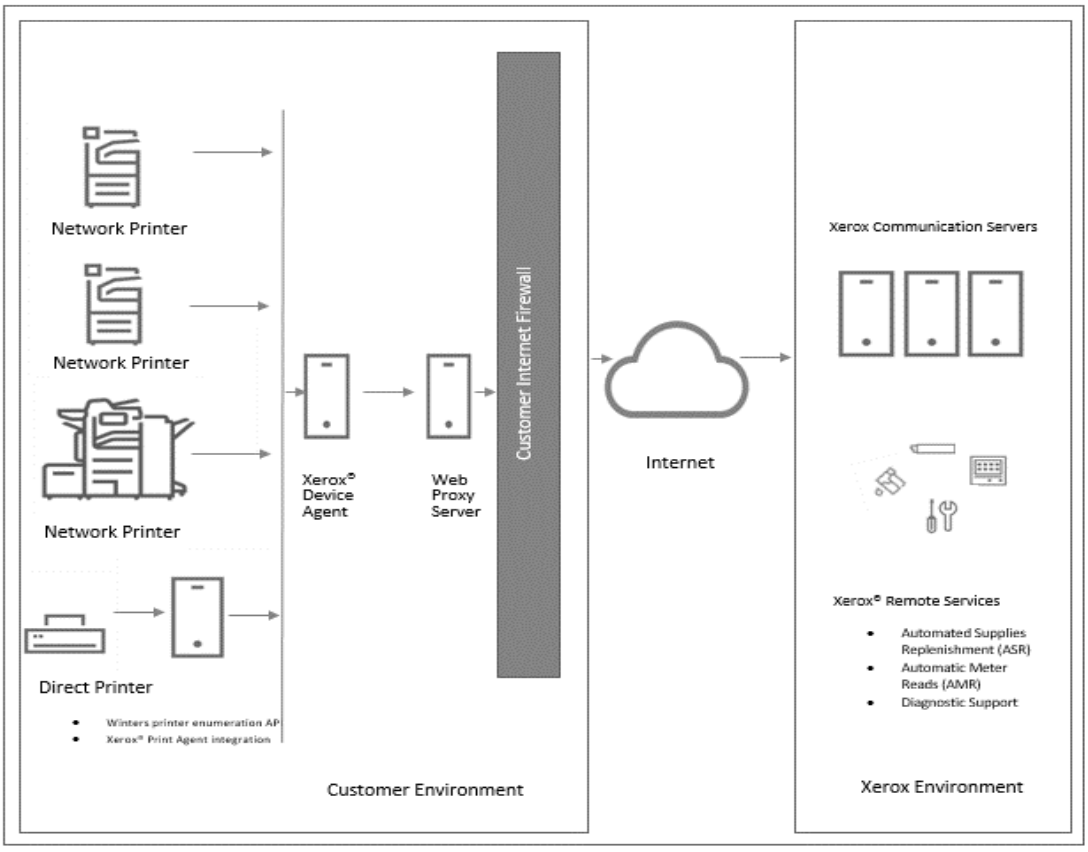
Device Direct Deployment Model

Device Management Application Deployment Model

The Device Management Applications (i.e., **Xerox® CentreWare Web, Xerox Device Agent**, **Xerox Device Agent Lite, Xerox Device Agent Partner Edition**, **and Xerox Device Manager software)** utilize a Transport Layer Security (TLS) 1.2 Protocol connection over the secure standard port 443 to communicate externally to the communication servers. Additional features are leveraged to enhance security across this channel and are established during the initial installation of the Device Management applications which include:

- The Device Management application within the customer environment initiates all communications with the communication servers. Standard firewall configurations on the site are required to enable communication.
- The communication servers are behind a secure firewall and are not accessible from the internet.
- The Device Management application requests a registration with the remote servers using certificate authentication appropriate credentials.
- The communication servers validate the credentials supplied by the printers and accept the requests.
- The Device Management application authenticates the communication servers and activates the service.

Figure 3



Device Management Application Deployment Model

5. Data Transmission & Payloads

Sources of Data

The print device data attributes that are sent as a part of the transmitted payload are from the following sources:

- Xerox® Office network printers
- Non-Xerox network printers
- Xerox® Production printers
- Xerox® Device Management Applications

Note: Not all Xerox Office and Xerox Production printers are Xerox Remote Services capable. You can find a complete list of capable products here. The print device attributes vary by product and Xerox Remote Services deployment solution.

Xerox® Office Devices

Table 1 Identifies the device data attributes that can be transmitted for Remote Services capable Xerox® Office products.

Our office class print devices transmit the device data attributes in an eXtensible Markup Language (XML) format using a compressed .zip file. Once authenticated, each file is then transmitted via an encrypted channel to the communication servers.

Data attributes	Detailed description of data attributes
Print Device Identity	Includes model, module firmware levels, module serial numbers, module install dates, licensing data, and location, if available.
Print Device Network Address	Includes Media Access Control (MAC) Address, subnet address.
Print Device Properties	Includes detailed hardware component configuration, detailed software module configuration, features/ services supported, etc.
Print Device Status	Includes active statuses, fault history counts, DFE event log, data transmission history
Print Device Counters	Includes billing meters, print-related counters, copy-related counters, large job-related counters, production-specific counters, scan-to-destination-related counters on low-end production models, etc.
Print Device Consumables	Includes manufacturer, model, serial number, name, type, level, capacity, status, lifetime counters, etc.
Print Detailed Machine Usage	Includes HFSI data, NVM data, parts replacement, DFE logs, detailed diagnostic data, fault resolution.
Engineering / Debug	Includes non-structured, detailed debug-related data intended for 3rd level support use only.
Customer Job-related	Xerox® Production print products provide the capability of reproducing job-related data in support of escalated support scenarios via encrypted PostScript to Xerox. The customer can control whether to activate this feature or not. If the customer chooses to transmit job-related data (i.e. encrypted PostScript) back to Xerox, that data is handled in accordance with Xerox information security (IS) policies and standards.

Xerox® Production Devices

Table 2 Identifies the device data attributes that can be transmitted for Remote Services capable Xerox® Production products.

Production class devices transmit the device data attributes in an eXtensible Markup Language (XML) format using a compressed .zip file. Once authenticated, each file is then transmitted via an encrypted channel to the remote services servers.

Data Attributes	Description
Print Device Identity	Includes model, firmware level, module serial numbers, and install date.
Print Device Network Address	Includes Media Access Control (MAC) Address, subnet address.
Print Device Properties	Includes detailed hardware component configuration, detailed software module configuration, features/services supported, power saver modes, etc.
Print Device Status	Includes overall status, detailed alerts, last 40 faults history, jam data, etc.
Print Device Counters	Includes billing meters, print-related counters, copy-related counters, fax-related counters, large job-related counters, scan-to-destination-related counters, usage statistics, etc.
Print Device Consumables	Includes consumable name, type (e.g. imaging, finishing, paper media), level, capacity, status, size, etc.
Print Detailed Machine Usage	Includes detailed print-related counters, power-on states, detailed Customer Replaceable Units (CRU) replacement quantities, detailed CRU failure data and distributions, embedded Optical Character Recognition (OCR) feature usage, print run length distribution, paper tray usage distribution, media installed, media types distribution, media size distribution, document length distribution, set number, HFSI data, NVM data, distribution, marked pixel counts, average area coverage per color, faults/jams, detailed scan-related counters.
Engineering / Debug	Includes detailed debug information which may include data outside of above listed data set. This data may include PII such as usernames, email addresses and job data. This data is only sent with expressed permission of the customer and is intended for escalated troubleshooting support use only.

Note: The file and content of the data identified varies depending upon product model.

Xerox® Device Management Applications

There are several Device Management Application options available based on the customers network environment and print device management need. Each are equally secure and have robust print device management capabilities.

The following are a list of device management applications: Xerox® CentreWare Web, Xerox Device Agent, Xerox Device Agent Lite, Xerox Device Agent Partner Edition, and Xerox Device Manager.

Each application synchronizes, by default, at least daily with the secure communication servers. To ensure maximum security for your data, the communication servers are hosted in an ISO 27001-compliant facility. Data sent is primarily printer-specific billing counters, supply levels and printer alerts. Data is compressed, encrypted, and protected by several mechanisms:

- Xerox Device Management application initiates all contact with the Xerox communication servers, standard firewall configurations in customer environment are required to enable communication.
- Xerox device management applications require a valid proxy, in the event a proxy is required for internet communication.
- Xerox communication servers sit behind a secure firewall in the Xerox environment and is not accessible from the internet.
- Xerox communication server's user interface access requires authentication. Xerox Device Management application host information is stored in an account specific to the customer site and the access to that account data in Xerox communication servers is restricted to Xerox communication servers account managers.
- All Xerox communication server's communication is logged and available for viewing.
- Data sent to your networked print devices, when enabled, consists primarily of remote commands that allow an account support administrator to request Xerox Device Management Application command level execution during escalated support scenarios.
- Requests principally involve firmware updates, printer reboots, test page printing and current device status refreshes.
- Xerox Device Management application periodically polls its Xerox communication servers account for command requests.
- Operations results from command requests are sent to the Xerox communication servers where they are then reviewed.

Note: There is a one-time registration requirement upon software installation. This registration information includes a field for device location and contact email.

The Xerox device management applications **(i.e. Xerox® CentreWare Web, Xerox Device Agent, Xerox Device Agent Lite, Xerpx Device Agent Partner Edition, and Xerox Device Manager software** transmit the print attribute data in eXtensible Markup Language (XML) format using a compressed .zip file. The file is then encrypted and transmitted via encrypted channels to the remote communications servers.

Table 3 Identifies a list of device data attributes and description that can be sent via the Xerox® Device Mgmt. app.

Data attributes	Detailed description of data attributes
Print Device Identity	Includes manufacturer, model, description, firmware level, serial number, asset tags, system name, contact, location, management state workstation (desktop), fax phone number, and queue name.
Print Device Network Address	Includes MAC address, IP address, DNS name, subnet mask, IP default gateway, last known IP address, IP address changed, time zone, IPX address, IPX External Network Number, IPX Print Server.
Print Device Properties	Includes components installed, component descriptions, features/services supported, print speed, color support, finishing options, duplex support, marking technology, hard drive, RAM, language support, user-defined properties.
Print Device Status	Includes overall status, detailed alerts, local console messages, component status, status retrieval-related data, discovery date, discovery method/type, device up-time, traps supported/enabled.
Print Device counters	Includes billing meters, print-related counters, copy-related counters, fax-related counters, large job-related counters, scanning-related counters, usage statistics, and target volume.
Print Device Consumables	Includes consumable name, type (e.g. imaging, finishing, paper media), level, capacity, status, size, and related attributes
Print Device Detailed Usage	User-based job tracking data which includes job characteristics (ID, document name, owner, document type, job type, color, duplex, media required, size, pages, sets, errors), destination (print device, model, DNS name, IP address, MAC address, serial number), results of printing the job (submission time, job print time, pages printed, color/B&W pages printed, color mode used, N-up), accounting data (chargeback code, chargeback price, accounting source), source of print job (workstation, print server name/MAC address, queue name, port, username, user ID), Xerox management data (sent to Xerox Services Manager).
Device Management Identity	Includes application host PC information such as DNS name, IP address, OS name, OS type, PC CPU, RAM sizes (free vs. used), hard drive sizes (free vs. used), site name, app version, app license expiration date, .Net version, time zone, discovery component version, main database size, discovery database size, # of printers/ in scope/out of scope, critical services running.
Device Manager Corporation Security Mode	Normal Mode = Xerox Device Agent contacts Xerox Services Manager, Daily. Settings can be remotely changed without the need for on-site visits, even when polling schedules are switched off. Lock Down Mode = Besides printer- related data synchronization, there is no communication with Xerox Services Manager and settings must be changed on-site. Xerox Device Agent machine and printer's IP addresses are reported to Xerox Services Manager.
Device Management Print Control Policy	Includes End User PC name, print server used, print queue used, timestamp of violation, document name, End User username, job duplex, job color, total impressions of job, job price, action taken, end user notified, message displayed, print policy name, print policy rule.

6. Remote Management of Print Devices

Xerox escalated support personnel can process the following actions through device direct or Xerox Device Management Application.

Table 4 shows enhanced resolution efforts, permitted by the customer in an escalated support scenario. Permission by the customer to perform these functions must be explicitly obtained.

Data	Description
Actions to perform on Print Devices	• Get Device Status = retrieve the latest status from print device • Reboot Device = initiate a power down/power up sequence on print device • Upgrade Device = install new software/firmware on print device (.DLM over port 9100) • Troubleshoot Device = ping device + retrieve latest status from print device • Print Test Page = submit a test job to a print device to validate print path (generate a configuration report) • Start Managing Device = initiate periodic print device data transfers to the external Xerox® Communication Servers **Note**: **Each action can be disabled from use on-demand within the administration configuration portion of the Xerox® Device Management Applications which support this feature.**
Actions to perform on the Device Management applications	Settings within each device management application that can be managed include discovery operation, data export frequency, SNMP communication-related settings (retry, timeout, community names), alert profiles, and auto device management application software update frequency.
Remote Software management	Certain devices are equipped with automated remote software management capabilities. These devices send a query to the Xerox environment to see if there are any new software updates available for the device. If there are, the device will be able to then send a request for that software update and it will be updated at the prescribed time. However, if your environment prohibits automatic software updates; the remote software management option can be deselected without interruption of standard remote services.

System requirements for Device Management applications

The minimum requirements vary slightly according to offerings. Refer to the User Guide, Security Evaluation Guide and/or Certification guide for baseline requirements specific to the respective device management applications.

Upon installation, a. readme file is included to address additional and specific system requirements for the respective device management application being installed.

We recommend that host computers are up to date with the latest critical patches and service releases from Microsoft® Corporation.

- The Device Management applications are compatible with the security features built into the Windows® operating system. They rely on a background Windows® service running under the local system account credentials to enable proactive monitoring of printers and the print data attribute payload that will transmitted to Xerox. The user interface that displays the print data attribute payload is only accessible by power users and administrators with access to the Windows® OS.

- To prevent an interruption of automatic remote services communications, it is recommended that the Device Management application be loaded on a client which is powered continuously or during core business hours.

- The Network Transmission Control Protocol/Internet Protocol (TCP/IP) must be loaded and operational.

- Administrative privileges are required to install the Device Management application software on the client machine.

- We recommend that host computers are running a supported operating system from Microsoft® Corporation. However, the Xerox device management applications can be run on Apple® OS 10.9.4 or later using Parallels Desktop emulation software. Application will not run in native Macintosh environment. See the respective user guides for detailed support

- Requires SNMP-enabled devices and the ability to route SNMP over the network. It is not required to enable SNMP on the computer where Xerox® Device Management Applications will be installed or any other network computers.

- Microsoft®.NET Framework 4.8 Extended (Full version) must be installed before installing the application.

- The application should not be installed on a PC where other SNMP-based applications or other Xerox® Print management tools are installed, as they may interfere with each other's operation.

Database configurations

The application installs SQL Server Compact Edition 4.0 (SQL CE) database engine and database files that store printer data and application settings within the installation directory. No database licensing is necessary for the application. Xerox Device Agent also supports existing instances of SQL Server, as described above.

Unsupported Configurations

This section describes the configurations that are not supported.

- Installation of the application on a computer with another Xerox device management application, such as Xerox Device Manager.
- Native Mac OS® operating system software (i.e., Xerox Device Agent can only run on the ApplevMac Platform when the Parallels Emulation Software is installed.)
- Any version of UNIX® operating systems, Linux® operating systems, Windows® systems running the Novell client, Windows® 7, Windows® XP, Windows® Vista, Windows NT® 4.0, Windows Media® Center, Windows® 2000, Windows® Server 2008 and 2008 R2, Windows® Server 2012 and 2012 R2, Windows® Server 2003, Windows® 8 RT, Operating systems running Terminal Services for applications and Installation on Windows systems running domain controllers. Windows Core Servers without a GUI.
- Since this application has only been tested on VMware® Lab Manager/workstation environment, other virtual environments are not supported.

Disablement Thresholds

- When disablement thresholds are enabled in Xerox Services Manager, if Xerox Services Manager has not communicated with Xerox Device Agent within the specified period of time, or the customer or account has been disabled in Xerox Services Manager, then the Xerox Device Agent may be disabled or terminated. These thresholds cannot be edited in Xerox Device Agent.
- To re-enable a Xerox Device Agent that has been disabled for exceeding the communication threshold, you need to resolve the issue that caused the disablement. It is impossible to re-enable a Xerox Device Agent that has been terminated; in this instance, you must reinstall the Xerox Device Agent.
- When a Xerox Device Agent is pending disablement or termination due to communication failure, warning emails are sent if email alerts are configured in Xerox Device Agent. See Viewing the Local Alerts section in this document to configure emails.

7. Xerox Business Process and Services

The data received from Xerox® Office-based print devices, Xerox® Production-based print devices, and Xerox device management applications as a part of the remote services solution are utilized by the Xerox business processes listed below:

Table 5 details the name and description of the business processes and services that are supported as a part of the Remote Services solution.

Business Process Name	Description
Automatic Meter Reads	Meter read data is used in the billing process.
Automatic Supplies Replenishment / Automatic Parts Replenishment	Toner is automatically sent to customers based on consumable depletion status received from print devices. Certain replaceable components are automatically shipped to customers when needed for their print devices. These options are available to customers who opt for metered supply contracts only.
Serviceability (Maintenance Assistant)	Remote management of the device provides detailed fault information which can be viewed by Xerox service personnel, when necessary, to expedite the preparation for an on-site visit or diagnose and resolve issues.
3rd Level Support (Engineering/Debug)	Product support personnel can debug difficult problems when given access to detailed engineering and debug logs.
Product development	Printer performance and use data is used to identify product improvements for future releases.

Basic print device data is aggregated, transmitted, retained, and archived within an ISO-27001 certified Xerox data center and is held in accordance with Xerox corporate data handling retention polices.

The work processes and practices that support and protect the remote services software systems are based upon ITIL best practices and Xerox Information Security Policies which directly align with the International Standards Organization ISO 27002 information security management system standards. Customers can be assured that the management, protection, and storage of device data comprehends the basic tenets of information security: confidentiality, integrity, availability, authentication, and non-repudiation.

8. Technology Details

This section provides additional technical details which are typically required by Information Technology (IT) teams and security practitioners who manage risks by obtaining assurance of secure development practices. Such assurance enables them to certify our print devices and Device Management applications for use within the customer's network environment.

Software Design

Our commitment to Xerox product security begins early in product development where Xerox developers follow a formal security development life cycle that manages security problems through identification, analysis, prioritization, coding, and testing. Many Xerox® Print Devices are Common Criteria certified ISO IEC 15408 or are actively under certification review.

Operability

Xerox remote services perform the following types of operations on a network. These operations depend on the deployment method configured.

Table 6.

Deployment Method	Application Used	Data Flow on Network	Operability Imposed on a Network
Device Direct	None	Internal	Xerox® Print Device attempts to detect a Web Proxy Server (automatic or directed to a specific address)
		Internal	Xerox® Print Devices can be programmed to generate requests to a Simple Mail Transport Protocol (SMTP) server to send alert notification Email messages to a defined recipient list
		External to Network	Xerox® Print Device traverses the company firewall to access the Internet (HTTPS over port 443)
		External to Network	Xerox® Print Device authenticates with its certificate to the remote Xerox Communication Server prior to transmitting any data attributes
		External to Network	Xerox® Print Device automatically transmits print device attribute data through an encrypted channel (HTTPS over port 443) to the Xerox® Communication Servers at a specified time daily or upon customer request.
		External to Network	Xerox® Print Device automatically queries the Xerox® Communication Servers through an encrypted channel (HTTPS over port 443) at a specific time every day for a list of actions to perform (e.g. send billing data now, add service, etc.)
		External to Network	One-way on-demand transmission of Xerox® Print device engineering log data through an encrypted channel (HTTPS over port 443) to the Xerox® Communication Server

Deployment Method	Application Used	Data Flow on Network	Operability Imposed on a Network
Device Direct	None	Outbound, initiated by dev to pull latest s/w	Device send query to remote software management server to check for software / security updates. If the customer environment prohibits automatic software updates, the remote software management option can be deselected only without interruption of standard remote services.
Device Management applications	Centre Ware® Web	Internal	Each app detects a Web Proxy Server (automatic or directed to a specific address)
		Internal	Each app retrieves print device capabilities across the fleet via SNMP
		Internal	Each app retrieves print device configuration across the fleet via SNMP
		Internal	Each app retrieves print device status across the fleet via SNMP
		Internal	Each app retrieves print device consumable data across the fleet via SNMP
		Internal	Each app can reboot a print device via SNMP or via the print device web UI
		Internal	Each app can submit a test page to a specific print device
		Internal	Each app can launch a print device's web page
		External **(outbound only)**	Each app traverses the company firewall to access the Internet (HTTPS over port 443)
		External (**outbound only)**	Each app authenticates with its certificate to the remote Xerox Communication Server prior to transmitting any data attributes
		External **(outbound only)**	Each app automatically transmits print device attribute data through an encrypted channel (HTTPS over port 443) to the Xerox® Communication Servers at a specific time every day
		External **(outbound only)**	Each app automatically queries the Xerox® Communication Servers through an encrypted channel (HTTPS over port 443) at a specific time every day for a list of actions to perform
		Internal	Each Xerox Device Agent app detects a Web Proxy Server (automatic or directed to a specific address)
		Internal	Each Xerox Device Agent app retrieves print device capabilities across the fleet via SNMP
		Internal	Each Xero® Device Agent app retrieves print device configuration across the fleet via SNMP
		Internal	Each Xerox Device Agent app retrieves print device status across the fleet via SNMP
		Internal	Each Xerox Device Agent app retrieves print device consumable data across the fleet via SNMP
		Internal	Each Xerox Device Agent app can request that the device print a configuration report
		Internal	Each Xerox Device Agent app can launch a print device's web page

Deployment Method	Application Used	Data Flow on Network	Operability Imposed on a Network
Device Management applications	Xerox Device Agent Partner Edition for monitoring network-connected print devices	Internal	Each Xerox Device Agent app can upgrade print device software via print job submission. (. DLM file over port 9100)
		External (**outbound only)**	Each Xerox Device Agent app traverses the company firewall to access the Internet (HTTPS over port 443)
		External (**outbound only)**	Each app authenticates with its certificate to the remote Xerox Communication Server prior to transmitting any data attributes
		External **(outbound only)**	Each Xerox Device Agent app automatically transmits print device attribute data through an encrypted channel (HTTPS over port 443) to the Xerox® Communication Servers at a specific time every day
		External **(outbound only)**	Each Xerox Device Agent app automatically queries the ommunication Servers through an encrypted channel (HTTPS over port 443) at a specific time every day for a list of actions to perform
Device Management applications	Xerox® Device Manager for monitoring network-connected print devices	Internal	Xerox Device Manager / Xerox Device Agent apps detect a Web Proxy Server (automatic or directed to a specific address)
		Internal	Xerox Device Manager / Xerox Device Agent apps retrieve print device capabilities across the fleet via SNMP
		Internal	Xerox Device Manager / Xerox Device Agent apps retrieve print device configuration across the fleet via SNMP
		Internal	Xerox Device Manager / Xerox Device Agent apps retrieve print device status across the fleet via SNMP
		Internal	Xerox Device Manager / Xerox Device Agent apps retrieve print device consumable data across the fleet via SNMP
		Internal	Xerox Device Manager / Xerox Device Agent apps can request that the device print a configuration report
		Internal	Xerox Device Manager / Xerox Device Agent apps can launch a print device's web page
		Internal	Xerox Device Manager / Xerox Device Agent apps can upgrade print device software via print job submission
		Internal	The Xerox Device Manager app supports SNMPv3 communications w/ print devices
		Internal	The Xerox Device Manager app can make changes to the print device configuration via SNMP and web UI
		Internal	The Xerox Device Manger app retrieves job-based accounting logs from certain Xerox® MFPs
		Internal	The Xerox Device Manager app manages / enforces print control policies

Deployment Method	Application Used	Data Flow on Network	Operability Imposed on a Network
		External **(outbound only)**	Xerox Device Manager / Xerox Device Agent apps traverse the company firewall to access the Internet (HTTPS over port 443)
		External (**outbound only)**	Each app authenticates with its certificate to the remote Xerox Communication Server prior to transmitting any data attributes
		External **(outbound only)**	Xerox Device Manager / Xerox Device Agent apps automatically transmit print device data to the Xerox© Communication Servers through an encrypted channel (HTTPS over port 443) at a specific time every day
		External **(outbound only)**	Xerox Device Manager / Xerox Device Agent apps automatically query the Xerox Communication Servers through an encrypted channel (HTTPS over port 443) at a specific time every day for a list of actions to perform
	Device Management application	External, bidirectional	Xerox Device Manager contacts Xerox Services Manager daily and allows administrators to remotely change settings, avoiding the need for on-site service calls.

9. Security Features

SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP) FOR XEROX

The Simple Network Management Protocol (SNMP) is the most widely used network management tool for communication between network management systems and networked printers. The Device Management Applications use SNMP during discovery operations to retrieve detailed print device information. Xerox® Device Management Applications supports SNMP v1/v2 and v3 protocols. Consult the respective Xerox® Device Management Application certification guides for specific details.

The SNMP v3 framework supports multiple security models, which can exist simultaneously within an SNMP entity. SNMPv3 includes tighter security by adding cryptographic security to SNMPv2. Additionally, SNMPv3 is backwards compatible with previous versions and is widely in use across robust networks.

Xerox device management applications (Xerox® CentreWare Web / Xerox Device Manager, Xerox Device Agent) can communicate with device platforms that are Federal Information Processing Standard FIPS 140-2 compliant in their implementations of SNMPv3.

The Xerox device management applications do not utilize the Windows SNMP service or the Windows SNMP Trap service. If previously installed, these services **must** be disabled on any personal computer (PC) or server where the Xerox Device Management Application is installed.

The Xerox device management applications utilize a Xerox-developed SNMP agent that:

- Contains a special encoding/decoding mechanism
- Is completely .NET-managed
- Uses .NET runtime executable - this provides enhanced security to prevent attack against software vulnerabilities such as invalid pointer manipulations, buffer overruns, and bound checking.

The Xerox device management applications utilize the security features available from the Windows operating system (OS) including:

- User authentication and authorization
- Services configuration and management
- Group policy deployment and management

Windows Internet Connection Firewall (ICF) including:

- Security logging settings
- ICMP settings

Xerox device management applications : Xerox **Device Agent, Xerox Device Agent Lite, Xerox Device Agent Partner Edition,** SQL CE 4.0 application Microsoft® SQL Server and the **Xerox Device Manager** use Microsoft® SQL Server Standard/Enterprise

The Xerox device management applications can be configured to leverage the additional Microsoft® security features to include, where applicable:

- Enabling User account registration
- Encryption of Domain Name System (DNS)
- Limit user account privileges to access the database (i.e. database owner rights)
- Implementation of a user-defined port numbers

A Xerox registration key and a valid Xerox account are required to transmit data to the remote Xerox Communications Servers.

The Xerox device management applications external communications may be impacted by the Windows Internet Connection Firewall. (We **recommend** that customers whitelist the Xerox URL on the customer firewall (*.support.xerox.com) CNAMEs are required to communicate through Imperva Web Application firewall (WAF).

The Xerox device management applications run as a background process using local system account credentials to automatically query network print devices via SNMP and periodically transmit print device attributes back to the Xerox Communications Servers

Access to the Xerox device management applications user-interface (UI) s and features are controlled via the following roles-based privileges :

- **Xerox®** CentreWare Web Administrators, CentreWare Web Power Users, CentreWare Web SQL Users, CentreWare Web Customer Administrators, and CentreWare Web Customers groups.
- Usernames and passwords for the applications do not traverse the network; access tokens are utilized instead (by Windows® OS design).
- The Xerox device management applications provides print submission control-based security by restricting jobs based upon color usage policy, document type, job cost, time of day, user group access control, duplex policy, job impressions allowed, and print quotas.

Note: The use of SNMP by any Xerox® Remote Services application does not pose a security risk to a client's IT environment because all SNMP-based traffic generated or consumed by these applications occur within the client's intranet, behind the firewall. The Windows SNMP service and the Windows SNMP Trap service are not enabled within the Windows OS by default.

Corporation Security Mode

The ***scheduled*** synchronization by the Xerox Device Agent Application to the secure communications server is set to *daily*, by default. Note that the time of day can be set to a chosen time.

There are two Corporation Security modes that exist: **Normal** and **Locked Down.**

When set to **Normal** mode, the Device Management Application contacts Xerox Services Manager daily. Settings can be changed without the need for on-site visits, even when polling schedules are switched off. ***(Recommended mode***).

In **Locked Down** mode, besides printer-related data synchronization, there is no communication with the communication servers and settings must be changed on-site. Additionally, the Xerox Device Agent machine and printer's IP addresses are not reported to the communications server. This mode limits all other remote services benefits to include automated billing and supplies as well as diagnostic data used for technical support.

Note: If a Xerox Device Agent version does not contain the Corporation Security Mode tab, it operates in Normal mode.

10. Network Impact

Company network guidelines will typically enable or disable specific network ports on routers and/or servers. Most IT departments are concerned about the ports used by the application for outgoing traffic. Disablement of specific ports may impact the application's functionality. Refer to the table below for specific ports used by the application's processes. If the application is required to scan across multiple network segments or subnets, routers must allow the protocols associated with these port numbers.

Protocols, Ports, & Other Related Technologies

Table 7 Identifies the protocols, ports, and technologies utilized within Xerox® Remote Services:

Port Number	Protocol	Description of Use	Data Flow on the Network
Dependent upon upper layer protocols	**Internet Protocol (IP)**	**Underlying transport for all data communications**	**Internal + External (outbound only)**
NA	Internet Control Message Protocol (ICMP)	Print device discovery + troubleshooting	Internal
25	Simple Mail Transport Protocol (SMTP)	Print device + Remote Proxy App Email notification alerts	Internal
53	Domain Name Services (DNS)	Utilized for DNS-based print device discovery operations	Internal
80	Hyper Text Transport Protocol (HTTP)	Print device web page queries + Device Management Application web page queries	Internal
135	Remote Procedure Call (RPC)	Print device discovery	Internal
161	Simple Network Management Protocol (SNMP v1 / v2C / v3)	Industry standard protocol used to discover networked print devices + Retrieve status, counters, & supplies data + Retrieve & apply print device configuration. Default community names = “public” (GET), “private” (SET)	Internal

Port Number	Protocol	Description of Use	Data Flow on the Network
443	Hyper Text Transport Protocol Secure (HTTPS)	Print device secure web page queries (if configured) + Remote Proxy app secure web page queries (if configured) + Print device data transfer back to the Xerox® Communication Servers + print controls communications back to Xerox® Device Manager	Internal + External (outbound only)
515, 9100, 2000, 2105	TCP/IP LPR & Raw Port print job submission	Print device software upgrade + Print Test page diagnostic	Internal

11. Security Best Practices

- Always keep print devices up to date with the latest firmware/software. Xerox closely monitors vulnerabilities and proactively provides customers with security patches and updates, when necessary.
- Disable unused ports and protocols on print devices wherever possible. This is typically done at the web user-interface (UI) of office class print devices and local user-interface (UI) of production class print devices.
- Utilize user access control-related features on print devices, if available. This is typically done at the web user-interface (UI) of office class print devices and local user-interface (UI) of production class print devices.
- Utilize secure protocols when possible. This is typically done at the web user-interface (UI) of office-based print devices and local user-interface (UI) of production-based print devices.
- Enable security features embedded within the device (e.g. image overwrite, scan data encryption, print stream encryption, disk encryption, secure print, encrypted .pdf, CAC/PIV access authentication.)

To find additional information regarding remote services at Xerox, visit Xerox.com/RemoteServices.

For additional and specific information regarding the security mechanisms and capabilities within the array of Xerox device management applications, please see their respective guides:

Xerox Device Agent

Xerox Device Manager

CentreWare Web

Whether it's device or content security, Xerox is at the forefront with proactive security for today's emerging threats. Visit www.xerox.com/security to access a full breadth of security information, updates, bulletins, white papers, patches and more.

12. Additional Information and Resources

Security at Xerox

Xerox maintains an evergreen public web page that contains the latest security information pertaining to its products. Please see https://www.xerox.com/security

Responses to Known Vulnerabilities

Xerox has created a document which details the Xerox Vulnerability Management and Disclosure Policy used in discovery and remediation of vulnerabilities in Xerox software and hardware. It can be downloaded from this page: https://www.xerox.com/information-security/information-security-articles-whitepapers/enus.html

Additional Resources

Table 8 Identifies additional security related information:

Security Resource	URL
Frequently Asked Security Questions	https://www.xerox.com/en-us/information-security/frequently-asked-questions
Common Criteria Certified Products	https://security.business.xerox.com/en-us/documents/common-criteria/
Current Software Release Quick Lookup Table	https://www.xerox.com/security
Bulletins, Advisories, and Security Updates	https://www.xerox.com/security
Security News Archive	https://security.business.xerox.com/en-us/news/