Xerox® Remote Services

Security White Paper

Version 2.0

Global Remote Services

Xerox® Technology Information Management

January 2017

BR19369

IS 614672/IS 514590

Document Version: 2.0 (January 2017).

Table of Contents

General Purpose and Audience

The purpose of this document is to serve as a guide for deploying Xerox® Remote Services for networked Xerox and non-Xerox printers within the customer's environment. It is intended to provide security related details and comprehend the extensive security measures that are implemented within Xerox® Remote Services.

The target audience for this document includes technical vendors, IT network managers and IT 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.

Remote Services

Information is a key asset and security is paramount for all organizational assets, including networked multifunction print devices (MFPs). In today's "all-in-one" construct, 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. Xerox® understands this complexity and is responsive to our customers' security needs. Xerox® Products, Xerox® Systems and Xerox® Remote Services offerings are designed to securely integrate with our customers' existing workflows while employing the latest secure technologies.

The Xerox® Remote Services Security Whitepaper is intended to help the customer understand and deploy the appropriate secure Remote Services solution that is compatible with their network infrastructure. The customer network construct will determine whether changes to the Internet firewall, web proxy servers, or any other security-related network infrastructure will need to be made. The Xerox® Remote Services solution, device, and controls chosen depend on the customer's information security (IS) policies and will determine which mode of operation used.

The Xerox ® Remote Services capability is available in certain models of equipment. This capability allows print devices to be remotely serviced and supported using print device attribute data which includes*: print device identity, print device properties, status, consumable levels, usage data and detailed diagnostic data*. The print device attribute data is transmitted from within the customer's networked environment directly from the print device (device direct), through a hosted application (device management application), or via a combination of both methods using the secure Xerox® Remote Services communication path. Both Xerox® devices and Xerox® Device Management applications have a certificate to authenticate with the Xerox® Communications Servers before transmission of the print attributes can occur. Xerox® Remote Services transactions always originate from inside the customer's environment and are sent strictly based on customer authorizations.

The U.S. based Xerox® Communications Servers conform to the stringent security requirements for Information Security Management. Xerox® Datacenters and Xerox® Remote Services application maintain the annual Statement on Standards for Attestation (SSAE) No-16, Sarbanes-Oxley Act (SOX) compliance requirements and are ISO 27001:2013 certified.

By default, no customer images from print, fax, scan, copy actions or sensitive information is transmitted to the Xerox® Communication Servers.

Customer Controls

Xerox® Device Management Applications have the ability to display exported print device attribute data logs for auditing and verification purposes prior to encryption and transmission to the remote Xerox® Communication Servers. See the respective Xerox® Device Management Application User Guide for specifics.

Some small to midsize office print devices are equipped with a feature that enables customers to download and view the print device attribute data prior to encryption and transmission to the remote Xerox® Communication Servers via the Device Direct enablement method. To verify a particular print device has this capability, go to the print device's Centreware Internet Services page; Status tab, Smart eSolutions (or Remote Services) link, and under the Maintenance Assistant tab.

The Xerox® Remote Services solution can be tailored to address customer IS policies that strictly limit or restrict certain types of print device attribute that can be transmitted outside the network (e.g. network address-related attributes). Xerox® Device Management application tools have the capability to disable select fields from transmission.

Customers also have the option to invoke an *Exception request* during contract negotiations to **"opt-out"** of the Remote Services solution. This option would prevent all Remote Services communication and remote support capability for the print devices within that account.

To facilitate escalated remote support activities, customers can, as needed, enable the Remote Access feature to receive print device software releases, security patches, and remotely diagnose, repair or modify print device configurations in order to correct any diagnosed malfunctions. Remote Access will not allow Xerox® to view or download customer documents, data or any other information residing on or passing through the print device or the customer's information systems. There is an exception to this which occurs when a customer is working with Xerox support personnel on a more difficult issue and it is determined that further information may be needed to troubleshoot the problem. At that time, a customer may decide to provide permission to Xerox to access logs locally stored on the device that do include sensitive data.

Therefore, corporate Information Technology (IT) teams and security practitioners are encouraged to read this document in its entirety to effectively comprehend the various features, requirements, and operations of the Xerox® Remote Services and how they support compliance with our customers' IS policies.

Additional security resources for Xerox® product security data protections, industry partnerships and certifications can be found at http://www.xerox.com/security.

Deployment Models

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

- Device Direct Model - Device Direct enables print devices to communicate directly with the remote Xerox® Communication Servers via the internet through the customer's firewall.

- Device Management Application Model - A Xerox® Device Management application (aka Device Manager) can be deployed on a customer's network to collect a subset of data attributes from print devices. Multiple print device attributes are collected and then transmitted securely to the remote Xerox® Communication Servers.

- Combination Model – The implementation of both the Device Direct and Device Management Application Models.

All deployment models for Xerox ® Remote Services leverage industry standard web-based protocols and ports to establish a secure, encrypted channel to transmit print device attributes externally to Xerox® Communication Servers located within Xerox® redundant secured datacenters.

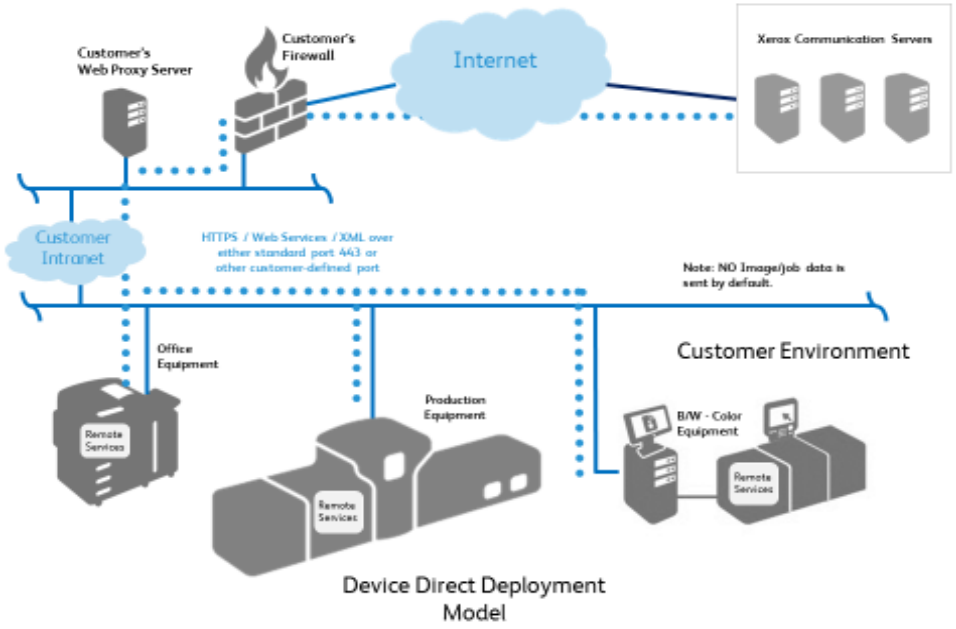
The deployment model chosen depends upon our customers' IS policies and rules for handling the transmission of the print device attributes and the type of print service solution and devices purchased from Xerox® (basic or managed print services).

Device Direct Deployment Model

The remote services module embedded within Xerox® devices utilizes a secure Transport Layer Security (TLS) 1.2 connection over the standard port 443 in order to communicate externally to the remote Xerox® Communication Servers.

- Print devices within the customer environment directly initiate all communications with the remote Xerox® Communications Servers. Standard firewall configurations on the site are required to enable communication.
- A valid URL for the remote Xerox® Communications Servers must be used.
- The Xerox® Communications Servers sit behind a secure firewall and are not accessible from the internet.

Figure 1



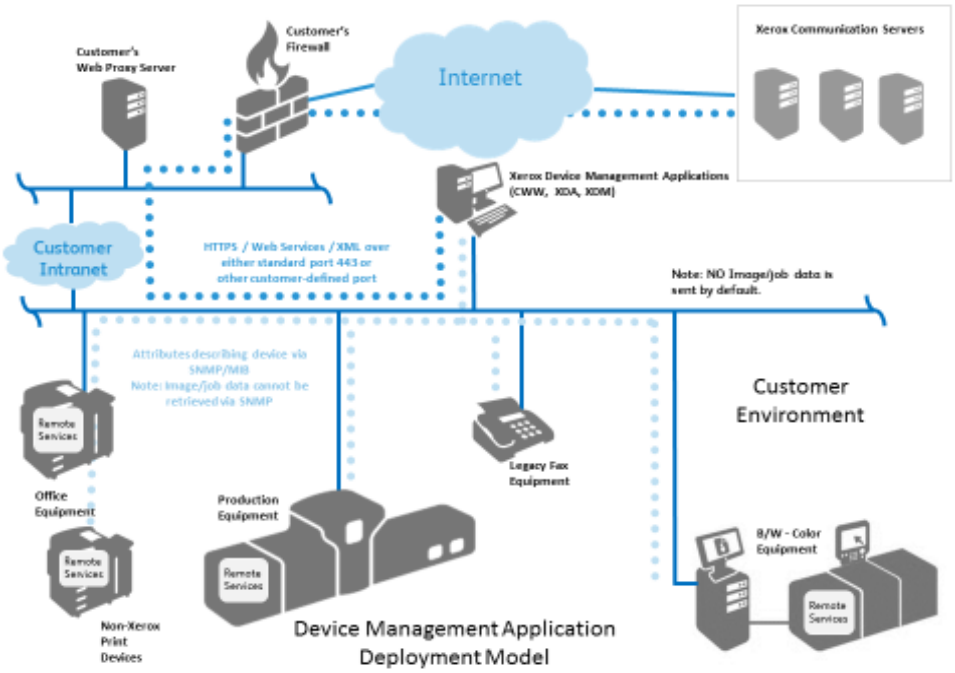
Device Direct Deployment Model

Device Management Application Deployment Model

The Device Management Applications (i.e. **Xerox® Centre Ware® Web, Xerox® Device Agent, Xerox® Device Agent Partner Edition, and Xerox® Device Manager)** also utilize a Transport Layer Security (TLS) 1.2 secure encrypted connection over the standard port 443 in order to communicate externally to the remote Xerox® Communication Servers. Additional features are leveraged to enhance security across this channel and are established during the initial installation of the Device Management applications include:

- The Device Management application within the customer environment initiates all communications with the remote Xerox® Communications Servers. Standard firewall configurations on the site are required to enable communication.
- A valid URL for the remote Xerox® Communications Servers must be used.
- The Xerox® Communications Servers sit behind a secure firewall and are not accessible from the internet.
- Either a valid account ID or a site identifier and a Xerox® Communications Server registration key must be used to access some of the services at the Xerox® Communication Servers.
- The Device Management application requests a registration with the remote Xerox® Communications Servers using the certificate authentication appropriate credentials.
- The remote Xerox® Communications Servers validate the supplied credentials and accept the requests.
- The Device Management application authenticates the remote Xerox® Communications Servers and activates the service.

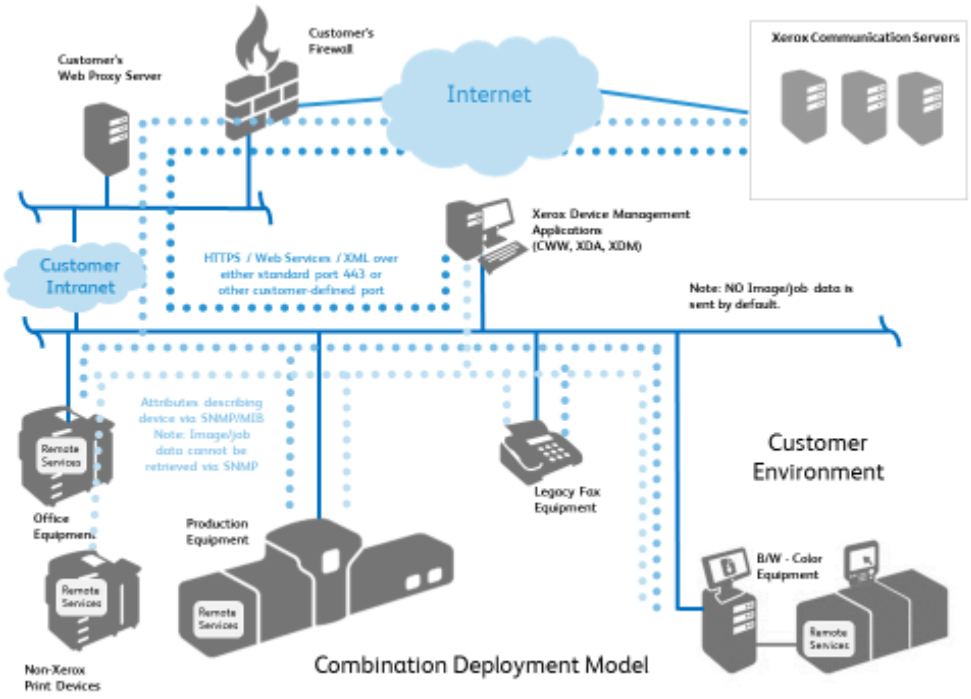
Figure 2



Combination Deployment Model

The Combination Deployment is deployed whenever a customer purchases multiple types of Xerox maintenance agreements for their print devices. 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 establish a direct connection to the Xerox® Communication Servers.

Figure 3



Data Transmission & Payloads

Sources of Data

The print device data attributes are collected for Xerox® Remote Services from the following sources:

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

Xerox® Office Devices

Xerox® Office class print devices transmit the device data attributes in an eXtensible Markup Language (XML) format using a compressed .zip file. Each file is then transmitted via an encrypted channel to the remote Xerox® Communication Servers.

Table 1 identifies the device data attribute that can be transmitted and their description.

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.

Data attributes	Description
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 user names, email addresses and job data. This data is sent with express permission of the customer and is intended for escalated support use only.

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

Xerox® Production Devices

Xerox ® Production-class devices transmit the device data attributes in an eXtensible Markup Language (XML) format using a compressed .zip file. Each file is then transmitted via an encrypted channel to the remote Xerox® Communication Services.

Table 2 identifies the device data attributes and their description that can be transmitted.

Data attributes	Detailed description of data attributes
Print Device Identity	Includes model, module firmware levels, module serial numbers, module install dates, customer contact information, 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 IS policies and standards.

Escalated support scenarios exist, where detailed debug information which may include data attributes outside the data set identified in tables 1-3. This data is sent with express permission of the customer and is handled in accordance with Xerox secure IS policies and standards.

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

Xerox® Device Management Applications

The Xerox® Device Management Applications (i.e. Xerox® Centre Ware® Web (**CWW**), Xerox® Device Agent (**XDA**) , Xerox Device Agent Partner Edition (**XDA PE**), and Xerox® Device Manager (**XDM**) 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 Xerox® Communications Servers.

Table 3 identifies the device data attributes and their description that can be sent via the Xerox® Device Management Application.

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, etc.
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.

Data attributes	Detailed description of data attributes
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 have to 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.

Remote Management of Print Devices

Xerox® support personnel can process the following actions through the Xerox® Device Management Application. As permitted, these actions are are conducted in support of anomaly resolution efforts and are delineated in the **Table 4** below.

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 Print Devices	• **Reboot Device** = initiate a power down/power up sequence on print device • **Print Test Page** = submit a test job to a print device to validate print path (generate a configuration report)
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.

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 application. Additional details can be found at : http://www.support.xerox.com/support/enus.html

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 running a supported operating system from Microsoft ® Corporation. However, the Xerox® Device Management applications can be run in a Macintosh OS environment if using Parallels Desktop emulation software. (You cannot currently run the Xerox® Device Management application in a native Macintosh environment.) See the respective Xerox® Device Management Application User Guides for additional details.
- We recommend that host computers are up to date with the latest critical patches and service releases from Microsoft ® Corporation.
- The Network Transmission Control Protocol/Internet Protocol (TCP/IP) must be loaded and operational.
- An Internet connection is required
- Administrative privileges are required to install the Device Management application software on the client machine.
- 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.
- You must install Microsoft®.NET Framework 4.6 (Full version) before you install the application.
- The application should not be installed on a PC where other SNMP-based applications or other Xerox® Device Management tools are installed, since they may interfere with each other's operation.

Unsupported Configurations

- Installation of the application on a computer with another Xerox® Device management application, such as Xerox® Device Manager.
- Any Unix® or Linux® operating system
- Microsoft ® operating systems at end of life such as Windows NT® 4.0, Windows® Media Center, Windows® XP, and Windows® Server 2000 and 2003.
- Virtual environments other than VMware® Lab Manager™/Workstation/vSphere Hypervisor™. This application may work on other virtual environments; however, these environments have not been tested.

Xerox® Business Process and Services

The data received by the Xerox® Communication Servers from Xerox® Office-based print devices, Xerox® Production-based print devices, and Xerox® Device Management Applications are utilized by the following Xerox business processes:

Business Process Name	Description
Automatic Meter Reads	A bill is automatically generated from meter data received from print devices.
Automatic Supplies Replenishment / Automatic Parts Replenishment	Toner is automatically sent to customers when consumable depletion status is received from print devices. 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)	Detailed fault information can be viewed by Xerox service personnel, when necessary, to expedite the preparation for an on-site visit or remotely 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.

Basic print device data is compressed, 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 Xerox® Back office Remote Services software systems are based upon ITIL best practices and Xerox Information Security Policies which are based on the ISO 27001 standards. Customers can be assured that the management of data integrity, privacy, and protection are aligned with best practices.

Technology Details

This section provides additional technical details which are typically required by Information Technology (IT) team and security practitioners with the goal of managing risks by obtaining assurance of secure development practices; thus enabling the certification of print devices and Device Management applications for use in the customer's network environment.

Software Design

Our commitment to Xerox® product security begins early in product development with industry standard best practices for secure coding, extensive testing, and analysis to eliminate vulnerabilities. Xerox® actively engages certification practices such as Common Criteria and is active in emerging standards such as P2600 Working Group and the Security Development Lifecycle (SDLC).

Operability

Xerox® Remote Services performs the following types of operations on a network:

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 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 Xerox® 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

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 launch a print device's web page
		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 Xerox® Communication Servers through an encrypted channel (HTTPS over port 443) at a specific time every day for a list of actions to perform
	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

Deployment Method	Application Used	Data Flow on Network	Operability Imposed on a Network
Device Management Applications		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
		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

Simple Network Management Protocol (SNMP)

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 found on the network. Xerox® Device Management Applications support SNMP v1/v2 and v3 protocols. Consult the respective Xerox® Device Management Application certification guides to comprehend 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 (Centre Ware® Web / Xerox® Device Manager) have the ability to communicate with device platforms that are 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 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 Partner Edition, or Xerox® Device Manager** use SQL CE application Microsoft® SQL Server

The Xerox® Device Management Application can be configured to leverage the additional security features of the Microsoft® SQL Server application including:

- 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 in order 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 and specify the IP address that can access the URL.)

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 Manager (XDM) Application user-interface (UI) s and features are controlled via the following roles-based privileges (e.g. Centre Ware® Web Administrators, Centre Ware® Web Power Users, Centre Ware® Web SQL Users, Centre Ware® Web Customer Administrators, and Centre Ware® Web Customers groups provided).

Usernames and passwords for the applications do not traverse the network; access tokens are utilized instead (by Windows® OS design).

The Xerox® Device Manager (XDM) application 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.

Notes: The use of SNMP by any Xerox® Remote Services application should 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

In addition to any scheduled synchronization by the Xerox® Device Management Applications to the Xerox® Services Manager, there is a daily synchronization performed by default. The two Corporation Security modes that exist are **Normal** and **Locked Down** mode.

In **normal** mode, the Device Management Application contacts Xerox® Services Manager daily when all other scheduled synchronizations have been switched off (***Recommended mode***).

In **locked down** mode, besides printer-related data synchronization, there is no communication with Xerox® Services Manager. Changes to this setting must be done on-site. (***Data synchronization*** is insuring the print device information sent from the Xerox® Device Management application and what is captured in the Xerox® Services Manager are the same.)

By default, the Xerox® Device Management Application contacts Xerox® Services Manager daily and allows administrators to remotely change settings, avoiding the need for on-site service calls. We recommend this setting is not changed. If a customer restricts Xerox personnel from supporting print devices remotely, device communication to Xerox® Services Manager can be locked down except for printer data synchronization. In this mode, the application does not report any computer or printer IP addresses or site settings to Xerox® Services Manager, and any setting changes require an on-site visit.

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

Protocols, Ports, & Other Related Technologies

The following table identifies the protocols, ports, and technologies that are 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
137, 139	NetBIOS	Printer Server 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
162	SNMP traps	Default community name = "SNMP_trap"	Internal
389	Lightweight Direct Access Protocol (LDAP)	Print device discovery via MS Active Directory Partition enumeration + Scan service configuration set + Active Directory Customer Import + Customer Group Configurations	Internal
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)
452	Netware Service Advertising Protocol (SAP)	Print device discovery using Novell Server queries via IPX	Internal

Port Number	Protocol	Description of Use	Data Flow on the Network
515, 9100, 2000, 2105	TCP/IP LPR & Raw Port print job submission	Print device software upgrade + Print Test page diagnostic	Internal
631	Internet Printing Protocol (IPP)	Print device discovery	Internal

Security Best Practices

Always keep print devices up-to-date with the latest firmware/software. Utilize either the print device's web user-interface (UI) or the printer management application provided by Xerox® and other print vendors to upgrade the print device firmware/software.

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-class print devices and local user-interface (UI) of production-class print devices.

Enable security features embedded within the device (e.g. image overwrite, disk encryption, secure print, etc.)

Make sure that the company firewall can route HTTPS packets across port 443 in accordance with corporate security policies.