Xerox® Remote Services

Security White Paper

Version 1.0.10

Global Remote Services

Xerox® Information Management

June 2014

Changes are made to this document annually from the release date. Changes, technical inaccuracies and typographic errors will be corrected in subsequent editions.

Document Version: 1.0.10 (June 2014).

[Page Left Intentionally Blank]

Document Preface

General Purpose and Audience

The purpose of this document is to describe the system components, operability, and features available for securing Xerox® Remote Services within Xerox® products. It is intended to serve as a guide for deploying Xerox® Remote Services within the customer's networked environment.

The target audience for this document is focused on the following customer roles:

Role	Description
Customer Technology Vendor	Deploys equipment at the direction of the Customer's Information Technology (IT) Team
Customer Information Technology (IT) Team	Certifies and deploys the Xerox® Remote Services tool set and enabling / disabling features
Customer Security Team	Evaluates and approves the managed print service tool set for use in the customer's environment in accordance with company policies and in compliance with appropriate legislation and industry standards.

Note: Xerox® products that are not directly connected to a network are not comprehended within this white paper (i.e. stand-alone Fax / Scanner / Copier devices, etc.).

How to best use this document

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

- Review section 1 to understand the overall capabilities of Xerox® Remote Services.
- Review section 2 to determine the deployment model that best comprehends your existing Information Security policies.
- Review section 3 to understand the data that is sent from Xerox® Products.
- Review section 4 to understand the technical details behind Xerox® Remote Services.
- Review section 5 to understand best practices and recommendations when deploying and using Xerox® Remote Services.

Table of Contents

1 Executive Summary

Information is every organization's key asset, and security is essential for documents and devices, including multifunction printers (MFPs), which are connected to the network. In the 21st century, the network is the hub for practically all business activity.

Xerox is responsive to your security concerns. Xerox® Systems and Remote Service offerings are designed to integrate within your company's workflows. Remote Services transactions always originate from the device, based on authorizations made by the customer. Remote Services can only communicate with a secure server at Xerox that conforms to the stringent requirements of the internal Xerox Corporation information management infrastructure.

Remote Services can be deployed using one or more of the following models:

1. A Xerox® application can be deployed on customer's network to collect attributes describing print devices which are then forwarded externally to Xerox® Communication Servers (a.k.a. "via remote proxy applications or device managers").
2. Print devices can communicate directly with Xerox® Communication Servers through the customer firewall (a.k.a. "device direct")
3. A combination of both models

The deployment model chosen depends upon your Information Security policies for handling the transmission of the print device attributes and the print services solution purchased (basic or managed print services).

- The use of a Xerox® application to collect attributes about your print devices and then forward it to the Xerox® Communications Servers (i.e. as a "proxy") is typically deployed within small to large enterprise networks where IT policies restrict the number of connections that can be made with an external web site.

- The device direct model is typically employed when there are a few devices connected to a small network.

Regardless of the deployment model used, Remote Services leverage industry standard web-based protocols and ports to establish a secure, encrypted channel in order to transfer print device attributes externally to the Xerox® Communication Servers.

The customer network construct will determine whether changes to their internet firewall, web proxy servers, or any other security-related network infrastructure will need to be made. Both Xerox® devices and Xerox® applications authenticate with the Xerox® Communications Servers before transmission of the print attributes can occur. The set of attributes that is involved within remote services includes print device identity, properties, status, consumables levels, usage counters, and detailed diagnostic data.

No image/job data or personally identifiable information is transmitted by default to the Xerox® Communication Servers.

The amount of attributes transmitted varies depending upon the capabilities and type of print device that is used (i.e. small network printer vs. networked MFP vs. Production Copier/Printer).

If an Information Security policy specifically restricts a type of attribute that can be transmitted (e.g. network address-related attributes), some of the MPS Continuum of Services tool set has the capability to disable specific attribute fields from transmission.

Therefore, corporate Information Technology (IT) teams and security practitioners are encouraged to read this document in its entirety, to effectively comprehend the various features and operations of the Xerox® Remote Services and how they may be utilized to comply with your Information Security policies.

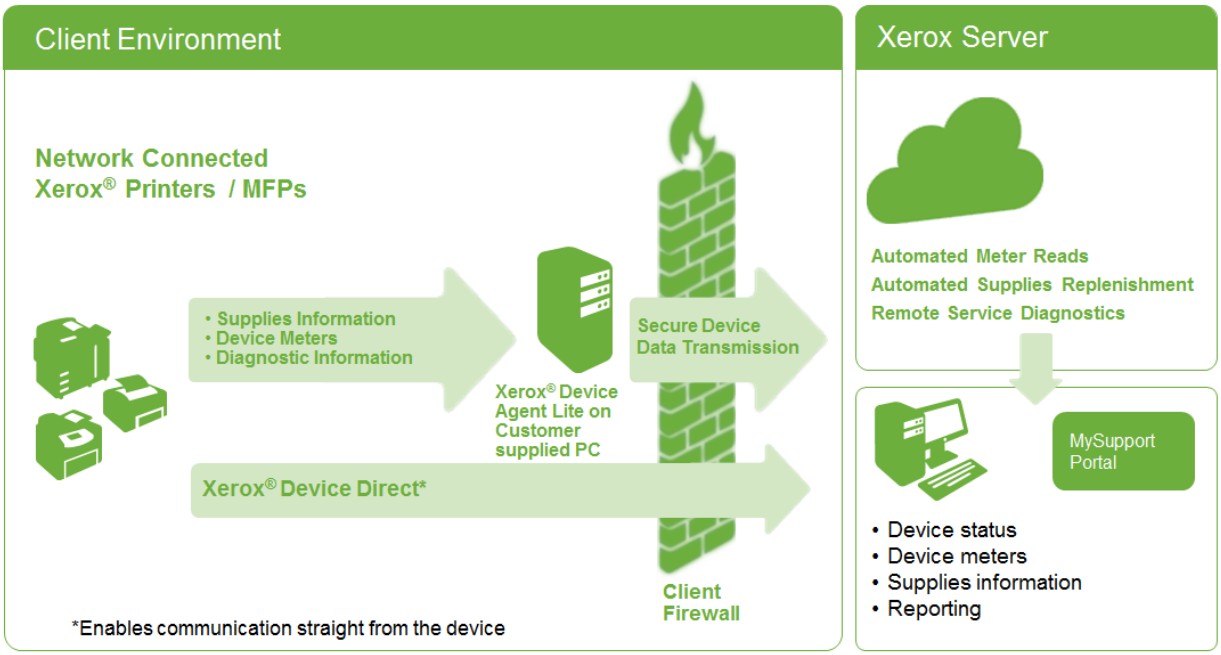
The MPS Continuum

The Xerox® Managed Print Services (MPS) Continuum of Services consists of the following four offerings briefly described below. Detailed information regarding the Xerox® MPS Continuum can be found at URL: http://services.xerox.com/managed-print-services/enus.html

1. **Xerox® Remote Print Services** automate several activities associated with managing Xerox® print devices on a network. These activities include: Automatic Meter Reads (AMR), Automatic Supplies Replenishment (ASR) and automatic reporting of diagnostic information so that Xerox can expedite resolution of print device error conditions. The **Xerox® CentreWare® Web and Xerox® Device Agent Lite** are the two applications made available from the Xerox web site (http:www.xerox.com) which enables customers to “proxy” both Xerox® and non-Xerox® Print device data back to Xerox.
2. **Xerox® Partner Print Services** is designed for Certified Reseller Partners that focus on controlling the cost of managing both networked and non-networked print devices, regardless of the vendor. Xerox® Partner Print Services is a flexible service offering the enables customers to pay for only the services they want. **Xerox® Device Agent Partner Edition** is the application typically deployed by Certified Reseller Partners to monitor print devices in the customer environment.
3. **Xerox® Print Services** is designed for small to large sized businesses. The focus of this offering is controlling costs and improving the efficiency of document printing, supplies replenishment, device procurement and device service maintenance. This offering provides a single point of contact for supporting both Xerox® and non-Xerox® print devices. **Xerox® Device Agent** is the application that offers monitoring and reporting of print device status, consumable levels, and usage across Xerox® and non-Xerox® print devices back to Xerox as a part of the Xerox® Print Services delivery process.
4. **Enterprise Print Services (EPS)** is the most comprehensive service within the MPS continuum. EPS has the most extensive set of capabilities and is designed for large-to-global sized businesses. **Xerox® Device Manager** application is deployed by Xerox to manage print devices within the customer environment. This web-based application monitors and reports on a variety of print and machine attributes back to Xerox as a part of the EPS service delivery process.

Xerox® Remote Print Services

Technology Suite



2 Deployment Models

The Remote connectivity models to Xerox can be deployed using one or more of the following models:

- Device Direct
- Remote proxy applications
- Combination of both the device direct and remote proxy applications models

Regardless of the deployment model used, it is important to note that all three deployment models are equally secure.

Device Direct Deployment Model

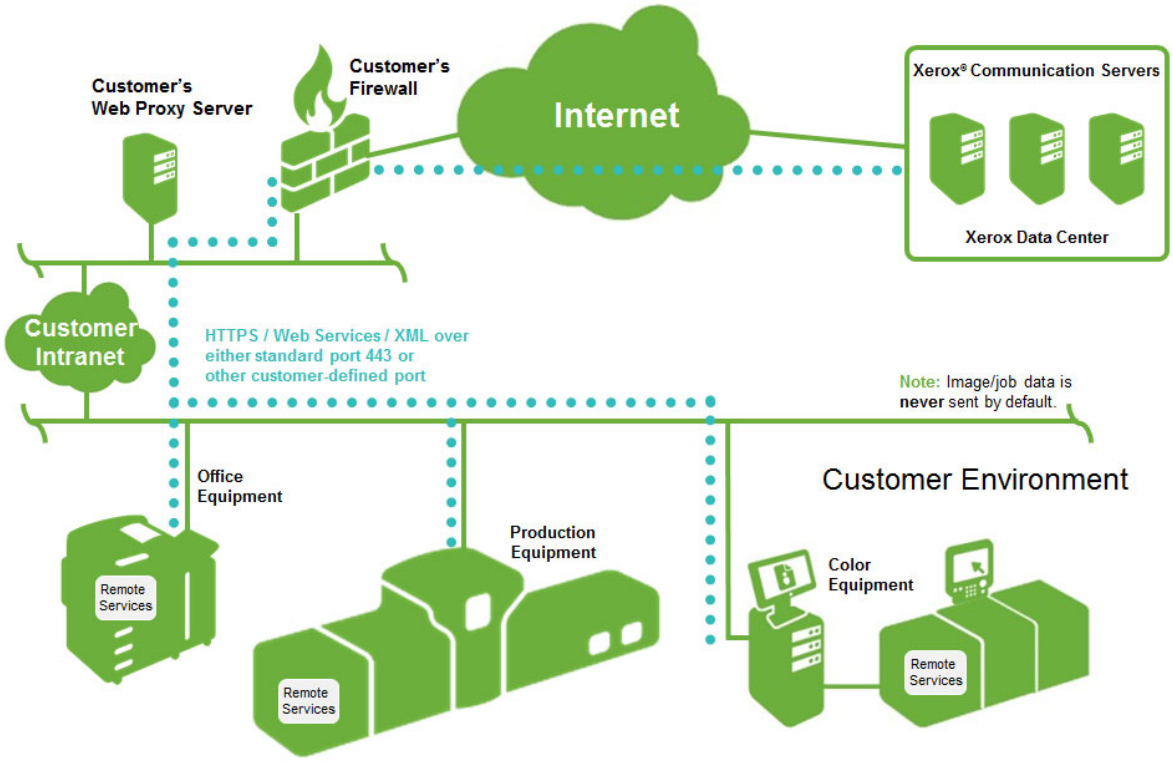


Figure 2.1 System Components & Data Flows of the Device Direct Deployment Model

Note: The Remote Services module embedded within Xerox® devices provides secure transmission of device attributes back to Xerox to enable the automated capabilities of Xerox® Remote Print Services and can be disabled on demand.

Remote Proxy Application Model

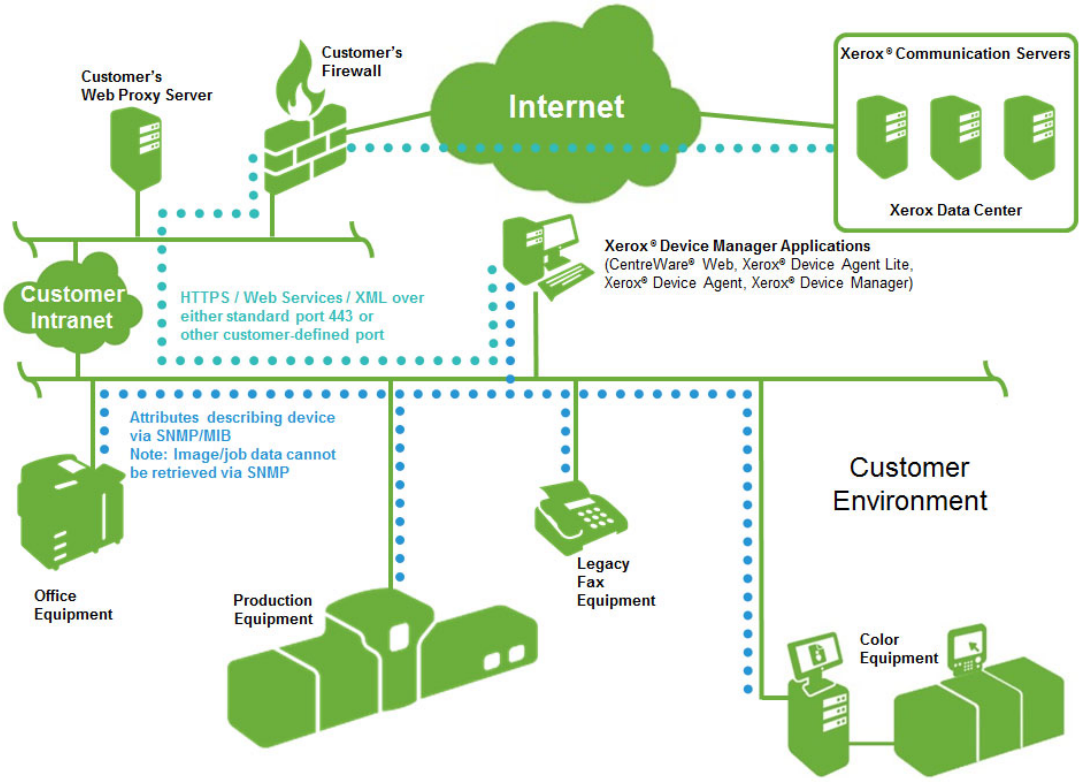


Figure 2.2 System Components & Data Flows of the Remote Proxy Application Model

Note: The Xerox® Print Agent tracks desktop printer usage (pages printed) and enforces specific printer policies (e.g. duplex, color vs. B&W, job type restriction, quotas, time of day, etc.). Xerox® Print Agent is only deployed on print servers and end user computers when the customer authorizes the use of the desktop usage monitoring and print policy enforcement components as part of Xerox® Enterprise Print Services.

Mixed Deployment Model

Combinations of the device direct deployment model and the remote proxy application deployment model can exist within the same customer environment. This scenario is possible 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.

If the customer elects to purchase a Xerox® Managed Print Services offering, the Remote Proxy applications will automatically take over the responsibility of periodically transmitting print device data to the Xerox® Communication Servers.

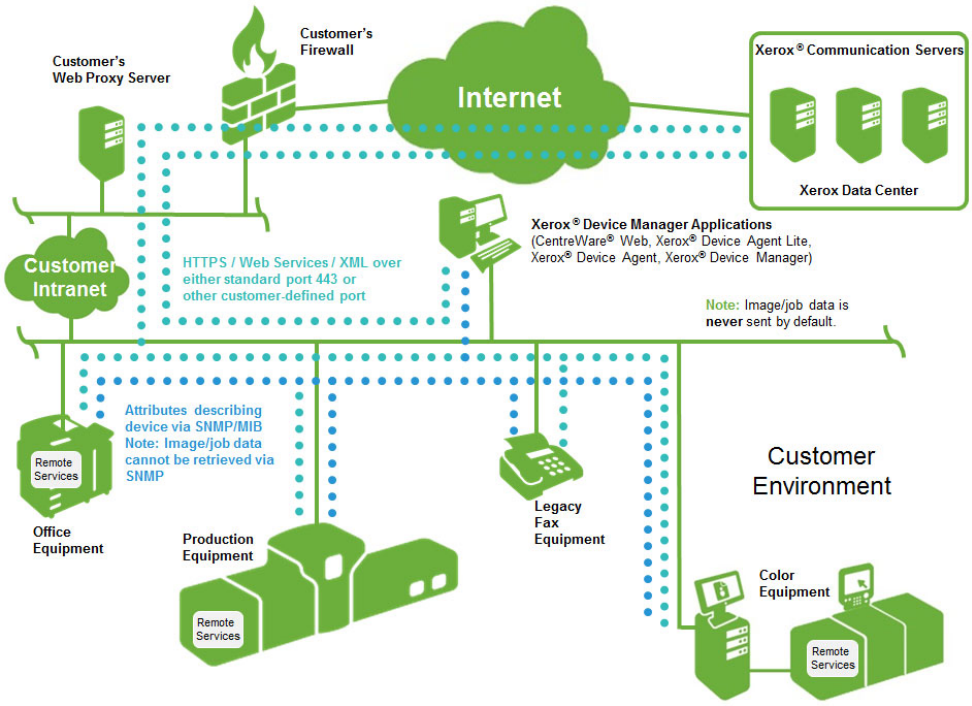


Figure 2.3 System Components & Data Flows of the Mixed Model Deployment Model

3 Data Transmission & Payloads

Securing the External Channel

Device Direct Deployment Model

The remote services module embedded within Xerox® devices utilizes a Secure Socket Layer (SSL) connection over the standard port 443 in order to communicate to the external Xerox® Communication Servers.

Remote Proxy Application Deployment Model

The Remote Proxy applications (i.e. **Xerox® CentreWare® Web, Xerox® Device Agent Lite, Xerox® Device Agent Partner Edition, Xerox® Device Agent, and Xerox® Device Manager**) also utilize a Secure Socket Layer (SSL) encrypted connection over the standard port 443 in order to communicate to the external Xerox® Communication Servers. Additional features that are employed to enhance security across this channel (which is established during the initial installation of the remote proxy apps) include:

- The Remote Proxy Application within the customer environment initiates all communications with the external Xerox® Communications Servers.
- A valid URL for the external Xerox® Communications Servers must be used.
- 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 Remote Proxy Application requests a registration with the external Xerox® Communications Servers using the appropriate credentials.
  - The Xerox® Communications Servers validate the supplied credentials and then accept the request.
  - The Remote Proxy Application detects the approval from the external Xerox® Communications Servers and then activates the service.

Sources of Data

The following system components collect data for Xerox® Remote Services:

- Xerox® Office Devices
- Xerox® Production Devices
- Xerox® Remote Proxy Applications

Xerox® Office Devices

Xerox® Office-base print devices transmit the following structured attribute data in a Xerox® eXtensible Markup Language (XML) format based upon the Distributed Management Task Force's Common Information Model (CIM). This structured attribute data is then compressed in .zip file format before it is encrypted and transmitted directly to the external Xerox® Communication Servers as part of Xerox® Remote Print Services:

Data	Description	Xerox® Service
Device Identity	Includes model, firmware level, module serial numbers, and install date.	Xerox® Remote Print Services only
Device Network Address	Includes network device/component used for connectivity configuration (no network address data exposed).	Xerox® Remote Print Services only
Device Properties	Includes detailed hardware component configuration, detailed software module configuration, features/services supported, power saver modes, etc.	Xerox® Remote Print Services only
Device Status	Includes overall status, detailed alerts, last 40 faults history, jam data, etc.	Xerox® Remote Print Services only
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.	Xerox® Remote Print Services only
Device Consumables	Includes consumable name, type (e.g. imaging, finishing, paper media), level, capacity, status, size, etc.	Xerox® Remote Print Services only
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 distribution, marked pixel counts, average area coverage per color, faults/jams, detailed scan-related counters.	Xerox® Remote Print Services only
Engineering / Debug	**None** **Note**: Although there is **no** automated transfer of engineering/debug data back to Xerox, some Office devices do contain a web UI feature for manually downloading log file data to a local PC; this is done at the customer's request to aid in specific troubleshooting efforts. This engineering/debug data does **not** contain any image/job data. The file created from this web UI download feature is encrypted and cannot be read by any users. It has to be Emailed back to Xerox and decrypted in order to be useful for analysis.	**None**

Notes:

- Refer to the Xerox website at (www.xerox.com) to determine if your devices are classified as either Office or Production.
- The file and content of the data identified varies depending upon product model.

Xerox® Production Devices

Xerox® Production-based print devices transmit the following structured attribute data in a Xerox proprietary eXtensible Markup Language (XML) format based upon the Distributed Management Task Force's Common Information Model (CIM). This structured data is then compressed in .zip file format before it is encrypted and transmitted directly to the external Xerox® Communication Servers:

Data	Description	Xerox® Service
Device Identity	Includes model, module firmware levels, module serial numbers, module install dates, customer contact information, licensing data, and location, if available.	Xerox® Remote Print Services only
Device Network Address	Includes Media Access Control (MAC) Address, subnet address.	Xerox® Remote Print Services only
Device Properties	Includes detailed hardware component configuration, detailed software module configuration, features/ services supported, etc.	Xerox® Remote Print Services only
Device Status	Includes active statuses, fault history counts, DFE event log, data transmission history	Xerox® Remote Print Services only
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.	Xerox® Remote Print Services only
Device Consumables	Includes manufacturer, model, serial number, name, type, level, capacity, status, lifetime counters, etc.	Xerox® Remote Print Services only
Detailed Machine Usage	Includes HFSI data, NVM data, parts replacement, DFE logs, detailed diagnostic data, fault resolution.	Xerox® Remote Print Services only
Engineering / Debug	Includes non-structured, detailed debug-related data intended for 3rd level support use only.	Xerox® Remote Print Services only
Customer Job-related	Includes encrypted PostScript commands to reproduce the job on another similar Xerox® Production print device (i.e. not the actual image data) Although only Xerox® Production print products provide this capability, the customer can control whether to activate this feature or not. If the customer chooses to transmit job-related data (i.e. encrypted PostScript, not image data) back to Xerox, that data is handled in accordance with Xerox policies, Xerox Confidentiality policies, or as directed by the customer.	Xerox 2nd level and 3rd level support

Notes:

- Refer to the Xerox website at (www.xerox.com) to determine if your devices are classified as either office or production.
- The file and content of the data identified varies depending upon product model.

Xerox® Remote Proxy Applications

The Xerox® Remote Proxy Applications (i.e. **Xerox® CentreWare® Web and Xerox® Device Agent Lite**, **Xerox® Device Agent Partner Edition**, **Xerox® Device Agent, and Xerox® Device Manager**) transmit the print and application attribute data is retrieved in an eXtensible Markup Language (XML) format that is compressed using .zip file format encrypted and transmitted directly to the external Xerox® Communication Servers:

Print	Description	Xerox® Services			
		Xerox® Remote Print Services	Xerox® Print Services	Xerox® Partner Print Services	EPS
Print Device Identity	Includes manufacturer, model, description, firmware level, serial number, asset tags, system name, contact, location, management state, queue name, and workstation (desktop), fax phone number, queue name.	X	X	X	X
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.	X	X	X	X
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.	X	X	X	X
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.	X	X	X	X
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.	X	X	X	X
Print Device Consumables	Includes consumable name, type (e.g. imaging, finishing, paper media), level, capacity, status, size, etc.	X	X	X	X

Print	Description	Xerox® Services			
		Xerox® Remote Print Services	Xerox® Print Services	Xerox® Partner Print Services	EPS
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). **Note:** Significant cost reduction can be achieved by monitoring end user print behavior, defining an appropriate policy for printer usage, and then using technology to enforce that policy. Xerox® Print Services, Xerox® Partner Print Services, and EPS provide that technology in the form of a user-based job tracking feature and a print controls feature. These features are only deployed for those customers willing to permit this level of data capture on their network.		X	X	X
Print Device Engineering / Debug	**None**	**None**			

Notes:

- For some Remote Proxy Applications, it is possible that certain attributes be disabled from collection and transmission. For further details refer to the respective remote proxy application user guide and/or security and evaluation guide.
- Chargeback Codes can be integrated and synchronized from the customer's from Microsoft Active Directory.

Application	Description	Xerox® Services			
		Xerox® Remote Print Services	Xerox® Print Services	Xerox® Partner Print Services	EPS
Remote Proxy App Identity	Includes 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.	X	X	X	X
Remote Proxy App Corporation Security Mode	**Normal Mode** = remote application configuration + action request reception + remote app status syncs w/ the Xerox® Communication Servers + print device data pushes are operational. **Lock Down Mode** = all communication with the external Xerox® Communication Servers is disabled. (i.e. remote application configuration disabled + remote device commands reception disabled + remote app status syncs to the Xerox® Communication Servers disabled + remote application IP address /DNS name disabled from transmission + print device data pushes are disabled)		X	X	X
Remote Proxy App Print Control Policy violations	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.				X
Remote Proxy App Remote Configuration	Settings that can be managed remotely include discovery operation, data export frequency, Simple Network Management Protocol (SNMP) communication-related settings (retry, timeout, community names), alert profiles, and auto remote proxy application software update frequency.		X	X	X

Xerox® Support personnel can process the following **requested actions** through the Xerox® Remote Proxy Applications process and are delineated in the chart below.

Data	*Description*	Xerox® Services			
		Xerox® Remote Print Services	Xerox® Print Services	Xerox® Partner Print Services	EPS
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 • **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 • **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® Remote Proxy Applications which support this feature.		X	X	X
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	X			
Actions to perform on the Remote Proxy Apps	Settings within each Remote Proxy App that can be managed include discovery operation, data export frequency, SNMP communication-related settings (retry, timeout, community names), alert profiles, and auto remote proxy app software update frequency.	X	X	X	X

Usage by Xerox® Back-end Systems

The data received by the external Xerox® Communication Servers from Xerox® Office-based print devices, Xerox® Production-based print devices, and Xerox® Remote Proxy Applications is 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 production 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 diagnosis upon customer service request.
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 retained and archived within an approved Xerox data center and is held in accordance with Xerox® Corporate data retention polices.

The work processes and practices that support and protect the Xerox® Back office Remote Services software systems and are based upon ITIL best practices and the ISO 27002 standards. Customers can be assured that the management of data integrity, privacy, and protection are aligned with the highest available industry standards.

4 Technology Details

This section is provided to identify additional technical details which are typically required by Information Technology (IT) team and security practitioners to enable the certification of print devices and remote proxy applications for use in the customer's network environment.

Software Design

Our commitment to Xerox® product security begins early in product development with secure coding techniques, 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.

Operability

Xerox® Remote Services Operability on a Network

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

Deployment Method	Apps Used per Xerox® Offering	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 device generates requests to an 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 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 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.)

Deployment Method	Apps Used per Xerox® Offering	Data Flow on Network	Operability Imposed on a Network
		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
Remote Proxy Applications	Xerox® Device Agent Lite + CentreWare® 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 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

Deployment Method	Apps Used per Xerox® Offering	Data Flow on Network	Operability Imposed on a Network
Remote Proxy Apps	Xerox® Device Agent app + Xerox® Device Agent Partner Edition app for monitoring network-connected print devices **Xerox® Print Agent app** for monitoring PC - connected print devices	Internal	Each Xerox® Device Agent app can submit a test page to a specific print device
		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
		Internal	The Xerox® Print Agent app can receive meter data from a PC-connected print device and then forward it onto the Xerox® Device Agent app
		Internal	The Xerox® Print Agent app can receive consumable level data from a PC-connected print device and then forward it onto the Xerox® Device Agent app
		Internal	The Xerox® Print Agent app can receive status data from a PC-connected print device and then forward it onto the Xerox® Device Agent app
		External (**outbound only)**	Each Xerox® Device Agent app traverses the company firewall to access the Internet (HTTPS over port 443)
		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
		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

Deployment Method	Apps Used per Xerox® Offering	Data Flow on Network	Operability Imposed on a Network
Remote Proxy Apps	**Xerox® Device Manager app** + Xerox® Device Agent app for monitoring network-connected print devices **Xerox® Print Agent app** for monitoring PC - connected print devices, user job tracking, and print controls	Internal	Xerox® Device Manager / Xerox® Device Agent apps can submit a test page to a specific print device
		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® Print Agent app can receive meter data from a PC-connected print device and then forward it onto the Xerox® Device Manager / Xerox® Device Agent apps
		Internal	The Xerox® Print Agent app can receive consumable level data from a PC-connected print device and then forward it onto the Xerox® Device Manager / Xerox® Device Agent apps
		Internal	The Xerox® Print Agent app can receive status data from a PC-connected print device and then forward it onto the Xerox® Device Manager / Xerox® Device Agent apps
		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 receives Xerox® Print Agent job tracking data from user workstations and print servers
		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)**	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

Requirements for the Remote Proxy Applications

Operating System (32-bit and 64-bit)

- Windows® XP Professional with Service Pack 3
- Windows Server® 2003 with Service Pack 2
- Windows Server® 2008 with Service Pack 1 and 2008 R2 with Service Pack 1
- Windows Server® 2012, Windows Server® 2012 R2
- Windows® 8, Windows® 8 Pro, Windows® 8 Enterprise
- Windows® 8.1
- Windows® 7 Professional, Enterprise, Ultimate, Home Basic, and Home Premium
- Windows Vista® Service Pack 2 Ultimate, Business, and Enterprise

Memory

- Minimum 512 MB RAM (1 GB RAM Recommended) for Windows® XP and Windows Server® 2003
- Minimum 1 GB RAM (1.5 GB RAM Recommended) for Windows Vista®, Windows® 7, Windows® 8, Windows® 8.1, and Windows Server® 2008 and 2008 R2, 2012 and 2012 R2

Processor: 1.7 GHz processor or better

Microsoft®.NET framework 3.5 Service Pack 1 installed

Hard Disk: minimum free space is approximately 100 MB for the application and up to 500 MB for the Microsoft®.NET framework, if not previously installed.

Minimum Resolution: 1024x768

Permissions: You must install the software on the client machine using the administrative account or an account with administrative privileges.

Internet connection: Required

Notes:

- The minimum requirements vary slightly according to offerings. Refer to the User Guide and/or Security Evaluation Guide for baseline requirements specific to the respective Remote Services Application. Additional information can be found in the .readme file in the Remote Services Application that is being installed to comprehend the baseline systems requirements.
- 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.

- 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 Agent Lite will be installed or any other network computers.
- You must install Microsoft®.NET 3.5 SP1 before you install the application.
- The application should not be installed on a PC where other SNMP-based applications or other Xerox® Printer 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 version of Macintosh® operating system, Unix® operating systems, Windows NT® 4.0, Windows® Media Center, and Windows® 2000.
- This application has only been tested on VMware® Lab Manager™/Workstation/vSphere Hypervisor™ environments. This application may work on other virtual environments; however, these environments have not been tested.

Security Features of the Remote Proxy Applications

- The Remote Proxy 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 Remote Proxy application is installed.

  Note: the Windows SNMP service and the Windows SNMP Trap service are not enabled within the Windows OS by default.
- The Remote Proxy applications utilize a Xerox-developed SNMP agent that contains:
  - a special encoding/decoding mechanism
  - is completely .NET-managed
  - The .NET runtime executable provides enhanced security to prevent attack against software vulnerabilities such as invalid pointer manipulations; buffer overruns, and bound checking.
- The Remote Proxy 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
  - Internet Connection Firewall
- The Remote Proxy application can be configured to leverage the additional security features of the MS SQL Server application including:

  - user account registration
  - Domain Name System (DNS) encryption
  - reduced user account privileges to access the database (i.e. database owner rights)
  - user-defined port numbers

Note: Xerox® Device Agent, Xerox® Device Agent Partner Edition, or Xerox® Device Agent Lite use SQL CE application

- A Xerox registration key and a valid Xerox account are required in order to transmit data to the external Xerox® Communications Servers.
- The Remote Proxy applications external communications may be impacted by the Windows Internet Connection Firewall.
- The Remote Proxy 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 Remote Proxy application user-interface (UI) s and features are controlled via the following roles-based privileges (e.g. CentreWare® Web Administrators, CentreWare® Web Power Users, CentreWare® Web SQL Users, CentreWare® Web Customer Administrators, and CentreWare® Web Customers groups provided).
  - Usernames and passwords do not traverse the network; access tokens are utilized instead (by Windows® OS design).
- The Xerox® Device Manager and Xerox® Print Agent applications provide 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.

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	HyperText Transport Protocol (HTTP)	Print device web page queries + Remote Proxy application web page queries	Internal
135	Remote Procedure Call (RPC)	Print device discovery + Xerox® Print Agent operations	Internal
137, 139	NetBIOS	Printer Server discovery + Xerox® Print Agent operations	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

Port Number	Protocol	Description of Use	Data Flow on the Network
443	HyperText 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)
445	Server Message Block (SMB)	Xerox® Print Agent operations	Internal
452	Netware Service Advertising Protocol (SAP)	Print device discovery using Novell Server queries via IPX	Internal
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

Note: The use of SNMP does not pose any external security risks to an intranet. All SNMP-based traffic is generated and consumed by the Xerox® Remote Proxy applications and print devices which are connected behind a company firewall. (I.e. no SNMP traffic traverses the company firewall).

Additional Information

- Numerous security features can be configured on the Xerox® Remote Proxy Applications. (Refer to the Security@Xerox web site for more details; www.xerox.com/security)
- Xerox® Communication Servers frequently exceed the 99.5% availability target.
- Xerox Data Centers are manned 24 hours a day, 7 days a week, and 365 days per year.
- Xerox® print devices transmit data once per day when powered on and 6-7 minutes after device power-up if a scheduled data transmission is missed.
- The frequencies of data transmission for the Xerox® Remote Proxy applications depend upon the contracted levels of service.
- Transaction-related logs (i.e. action, audit, event, E-mail, etc.) are available from the Xerox® Remote Proxy applications.
- MySupportPortal (http://www.xerox.com/about-xerox/mysupport/enus.html) provides access to meter data and supplies data sent from the Xerox® Print devices and Xerox® Remote Proxy Applications.

5 Recommendations

The following list identifies security-related best practices that should be implemented when managing print devices:

1. 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 the print vendor in order to upgrade the print device firmware/software.
2. Disable unused ports and protocols on print devices where ever 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.
3. Utilize user access control-related features on print devices, if available. 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.
4. 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.
5. Enable security features embedded within the device (e.g. image overwrite, disk encryption, secure print, etc.)
6. Make sure that the company firewall can route HTTPS packets across port 443.
7. If Information Security policies **prohibit the transmission of network address-related data outside of the network**, the remote proxy application deployment model is required. These data fields can be disabled, through remote proxy applications only, from transmission back to the Xerox® Communication Servers.
8. If the Xerox® Remote Proxy applications will be deployed:
    a. Do **not** install any of the Remote Proxy applications on a domain controller.
    b. Do **not** combine any of the Remote Proxy applications on the **same** PC/laptop/server.
    c. Do **not** enable the Windows OS-based SNMP service or the SNMP Trap service on the PC that the Remote Proxy applications will be installed on.
    d. Always install the latest patches to the Windows OS on the PC/laptop/server running the Remote Proxy applications.
        i. Before using the MPS Remote Proxy applications, make sure that the PC/ laptop/server has been rebooted after the Windows OS patches are installed.
    e. Ensure the Remote Proxy application PC/laptop/server is continuously powered on to prevent disruption of services enabled by the Xerox® Communication Servers.
    f. Ensure SNMP is enabled on your networked print devices.
    g. Change the SNMP Community names from their well-known default values (i.e. "public"). Having a minimal number of community names will ensure print device discovery performance is not adversely impacted by the number of different SNMP Community names used.

h. Ensure the SNMP Community names are known and configured properly (i.e. values need to match on both the print device and the Remote Proxy application).

i. Ensure the network supports the routing of SNMP across the various subnets.

j. Xerox® CentreWare® Web and Xerox® Device Manager applications require the use of Internet Information Service (IIS). Therefore, the following recommendations apply:

   i. Use an alternative web site instead of the IIS default web site for the Xerox® CentreWare® Web and Xerox® Device Manager installation.

   ii. Change the port number used by HTTP.

   iii. Utilize HTTPS for secure communications.

   iv. Disable anonymous communication to all Xerox® CentreWare® Web and Xerox® Device Manager pages.

   v. Restrict access to Xerox® CentreWare® Web and Xerox® Device Manager to specific IP addresses.

   vi. Disable basic authentication to prevent username and passwords from being transmitted in clear-text across the network.

k. Use the Configuration Sets feature within CentreWare® Web to apply the following security settings across your fleet of Xerox® print devices:

   i. Disable unused protocols and services.

   ii. Enable authentication for network scan services.

   iii. Change SNMP community names from their default settings.

   iv. Change the default print device Administrator password.

   v. Enable image overwrite.

   vi. Disable software upgrade when not upgrading the fleet.

6 Appendix A:

Deployment Model Selection

Which deployment model should I use?

The Device Direct deployment model should be used when:

- Xerox® print device deployment is small (e.g. < 10 devices; workgroup environment)
- Information Security policies permit the secure direct connection of print devices to external web sites
- Little to no management of print devices exist in the current architecture (i.e. want to leverage device automation features)
- Customer isn't interested in the manual billing or consumables replenishment-related activities capabilities.
- Customers may not want to use their own computer/server equipment to install the Xerox® Remote proxy applications.

The Remote Proxy Application deployment model should be used when:

- Xerox® Print device deployment is more than 10 devices (i.e. for small, medium, or large business environments)
- Information Security policies prohibit the direct connection of print devices to external web sites
- Information Technology personnel want control over the data flow to the Xerox® Communication Servers (i.e. a single data channel)
- Information Technology personnel require basic fleet monitoring of their print devices from a central location
- Customer isn't interested in any print device management-related activities i.e. customer interested in Xerox® Managed Print Services (MPS) offerings

Note: Although remote proxy applications were created for the entire Xerox® MPS Continuum of Services, only the Xerox® CentreWare® Web application and the Xerox® Device Agent Lite application are provided for customer use at **no cost**. Other similar remote proxy applications are utilized by Xerox personnel and/or 3rd party service partners to provide enhanced managed print services.