Xerox Remote Services
Security White Paper

Version 1.0.9
Global Remote Services
Xerox Information Management

November 2012
702P01061

BR4136

Document Version: 1.0.9 (November 2012).

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 a network 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 IT Team
Customer IT Team	Certifies and deploys the Xerox Remote Services tool set + enable/disable features
Customer Security Team	Evaluates and certifies/approves the MPS tool set for use in the customer's environment in accordance w/ company policies and compliance to 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

Review the entire document when preparing to certify Xerox products and services for use within a network environment.

Review section 2 within this document to understand the overall capabilities of Xerox Remote Services.

Review section 3 within this document to determine the deployment model that best comprehends your existing IT policies.

Review section 4 within this document to understand the data that is sent from Xerox products.

Review section 5 within this document to understand the technical details behind Xerox Remote Services.

Review section 6 within this document to understand best practices and recommendations when deploying and using Xerox Remote Services.

Table of Contents

Executive Summary

Managing a fleet of print devices while maintaining an acceptable level of security presents a unique challenge. IT staffs are forced to keep up with advances in print device technologies and ever changing security vulnerabilities. Furthermore, continuous improvement of operational processes, cost reduction-based activities, and asset utilization are routinely expected each year by senior management. Fortunately, Xerox has developed a continuum of remote services that can help. This collection of remote services is called the “Xerox Managed Print Services (MPS) Continuum of Services”. Xerox enables IT staffs to choose how they want to maintain an acceptable level of security while minimizing the associated costs and improving the process of managing a fleet of print devices. The basic concepts of security such as Confidentiality, Integrity, Availability, Accountability, and Non-repudiation are all comprehended within the MPS Continuum of Services.

The MPS Continuum of Services can be deployed using one or more of the following models:

1. print devices can communicate directly with Xerox Communication Servers (a.k.a. “direct connect”)

2. 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 apps”).

3. a combination of both models

The deployment model chosen depends upon your IT policies for handling the transmission of attributes about your print devices. The direct connect model is typically employed when there are a few devices connected to a small network. 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. Regardless of the deployment model used, the MPS Continuum of Services leverages 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. Customers typically do not have to make any changes to their Internet firewalls, web proxy servers, or any other security-related network infrastructure. Both Xerox devices and Xerox applications authenticate with the Xerox Communication Servers before transmission of the print device attributes can occur.

The set of attributes that is involved within the MPS Continuum of Services includes print device identity, properties, status, consumables levels, usage counters, and detailed diagnostic data. **No image/job data or personally identifiable information is ever transmitted by default to the Xerox Communication Servers.** Obviously, 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 IT policy specifically restricts a type of attribute that can be transmitted (e.g. network address-related attributes), the MPS Continuum of Services tool set has the capability to disable specific attribute fields from transmission. In production print-intensive environments which deal with complex jobs, it may become necessary to transmit job-related data from a print device back to Xerox in order to facilitate 2nd level and 3rd level support activities. 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.

Industry analysts and independent research company reports have consistently placed Xerox in the top tier of Managed Print Services vendors worldwide. (i.e. Xerox is positioned as a leader in the Gartner Magic Quadrant for Managed Print Services, IDC MarketScape Worldwide Managed Print Services Vendor Assessment, and the Quocirca Managed Print Services Vendor Assessment.). Therefore, corporate IT staffs and security-related folks are encouraged to read this entire document in order to understand how the various features and operations of the Xerox MPS Continuum of Services can be utilized to comply with your IT security-related policies.

The MPS Continuum

The Xerox Managed Print Services Continuum consists of the following 5 offerings:

1. Xerox Remote Print Services

2. Xerox® PagePack® 3.0

3. Xerox Partner Print Services

4. Xerox Print Services

5. Xerox Enterprise Print Services

It is important to note that the technology/toolset used within each of these offerings was developed from the **same** code base. This enables customers to receive consistent service delivery across all of the Xerox offerings.

2.1 Xerox Remote Print Services

Xerox Remote Print Services (XRPS) are included within contracts for those customers that either purchase or lease Xerox print devices. XRPS automate several activities typically associated with managing Xerox print devices on a network. These management activities include:

- Automatic reporting of print device usage so that a monthly bill can be produced
- Automatic reporting of consumable levels so that a new consumable can be shipped to the customer when a depletion state occurs
- Automatic reporting of diagnostic information so that Xerox can expedite the resolution of print device error conditions

XRPS applies to both Xerox print devices and non-Xerox print devices. Various levels of fee-based Maintenance Agreements (e.g. FSMA, e-Click, etc.) are offered to customers as well as traditional warranty agreements that are included within the price of the Xerox print devices.

Xerox products contain embedded remote services functionality which enables the automation of XRPS directly back to Xerox per device. Refer to the Deployment Models section for more details.

XRPS can also be enabled using remote applications installed on the customer's network. These remote applications collect device data on the customer's network and then forwards that data directly back to Xerox. Refer to the Deployment Models section for more details. The Xerox® CentreWare® Web (CWW) and Xerox Device Agent (XDA) Lite are the 2 applications that are made available from the Xerox web site (http://www.xerox.com) which enable customers to "proxy" both Xerox and non-Xerox print device data back to Xerox. CWW provides complete device management capabilities across small, medium, or large sized networks. This web-based application includes device discovery, status, configuration, software upgrade, and reporting. XDA Lite provides a reduced set of functionality across small to medium sized networks. This Windows-based application is focused on automated reporting of print device usage, consumable depletion, and diagnostic fault data.

2.2 Xerox® PagePack® 3.0

Xerox® PagePack® 3.0 (XPP) is a service offering within the Xerox MPS continuum that is designed for Xerox Authorized Partners to sell to small-to-medium sized businesses. This entry-level offering provides Xerox Authorized Partners with an opportunity to take advantage of the growing market for MPS by offering the following options to their customers:

- Fixed cost per page program covering supplies and service for new Xerox products
- Fixed cost per page program covering supplies (and service; optional) for all print devices, regardless of vendor
- Fixed cost per month per device program that provides full fleet management, regardless of vendor

For additional details on the Xerox® PagePack® 3.0 offering, check out the following Xerox web site: URL= http://bizzmail.com/PagePack/External/bizzmail.html.

An application called the PagePack Assistant (PPA) is typically deployed by Xerox Authorized Partners to monitor Xerox print devices within customer environments. This Windows-based application is focused on sending device usage, consumable depletion, and diagnostic fault data back to the Xerox Authorized Partner as part of the XPP service delivery process.

2.3 Xerox Partner Print Services

The Xerox Partner Print Services (XPPS) offering is designed for Certified Reseller Partners to offer to small-to-large sized businesses. The focus of XPPS is on controlling the cost of managing both networked and non-networked print devices, regardless of vendor. This offering establishes a centralized process for providing installation, routine maintenance, consumable replenishment, service, and support on any type of print device. As a result, the customer's valuable IT resources can focus on other more critical tasks required to run the business. XPPS is a flexible service offering that enables customers to pay for only those services that they want. For additional details on the XPPS offering, check out the following Xerox web site: URL = http://www.office.xerox.com/managed-print-services/enus.html.

The Xerox Device Agent Partner Edition (XDA PE) application is typically deployed by Certified Reseller Partners to monitor print devices within customer environments. This Windows-based application monitors and reports on print device status, consumable levels, and usage across both Xerox and non-Xerox print devices back to the Certified Reseller Partner as part of the XPPS service delivery process.

2.4 Xerox Print Services

Perhaps the most popular offering within the Xerox MPS continuum is the Xerox Print Services (XPS) offering. XPS is designed for small-to-large sized businesses. The focus of XPS is on controlling costs and improving the efficiency of document printing, supplies replenishment, device procurement, and device service / maintenance. This offering also provides a single point of contact for supporting both Xerox and non-Xerox print devices. XPS leverages best-of-breed industry standards-based tools combined with methodologies and years of managed print service delivery experience. Benefits achieved from a deployment of XPS include environmental sustainability, improved document security, proactive device support, improved employee productivity, consolidating reporting, and reduced cost of ownership for print infrastructure. For additional details on the XPS offering, check out the following Xerox web site: URL = http://www.consulting.xerox.com/xerox-managed-print-services/print-management/enus.html.

An application called the Xerox Device Agent (XDA) is typically deployed by Xerox MPS to manage print devices within customer environments. This Windows-based application monitors and reports on print device status, consumable levels, and usage across both Xerox and non-Xerox print devices back to Xerox as part of the XPS service delivery process. It also can perform Xerox print device software upgrade and support remote triage of problems from a remote call center.

2.5 Enterprise Print Services

The Enterprise Print Services (EPS) offering is the most comprehensive service within the Xerox MPS continuum. EPS is designed for large-to-global sized businesses. The focus of EPS is on controlling costs and improving the efficiency of internal office printing, mailroom & distribution operations, internal centralized print operations, and external print vendor outsourcing. This offering has the most extensive set of capabilities within the MPS continuum and includes:

- Detailed asset management
- End-to-end incident management
- Single point of contact for all customer print equipment
- Comprehensive break / fix support, regardless of vendor
- Application of rules-based print controls
- Business process improvement for document workflows
- Application of environmental sustainability best practices
- Enforcement of corporate information security policies
- Continuous improvement measurement, monitoring, and reporting
- Change management to transform existing practices into a new corporate culture.

For additional details on the EPS offering, check out the following Xerox web site: URL = http://www.consulting.xerox.com/xerox-managed-print-services/enterprise-printing/enus.html.

The Xerox Device Manager (XDM) application is deployed by Xerox MPS to manage print devices within customer environments. This Web-based application monitors and reports on print device status, consumable levels, and usage across both Xerox and non-Xerox print devices directly back to Xerox as part of the EPS service delivery process. It also can perform Xerox print device software upgrade and support remote triage of problems from a remote call center.

Deployment Models

Xerox Remote Services can be deployed using one or more of the following 3 models:

- direct connect
- via remote proxy apps
- a combination of direct connect and remote proxy apps

Regardless of the deployment model used, it is important to note that all 3 deployment models are equally secure.

3.1 Direct Connect

The direct-connect deployment model utilized within Xerox Remote Services consists of the follows system components:

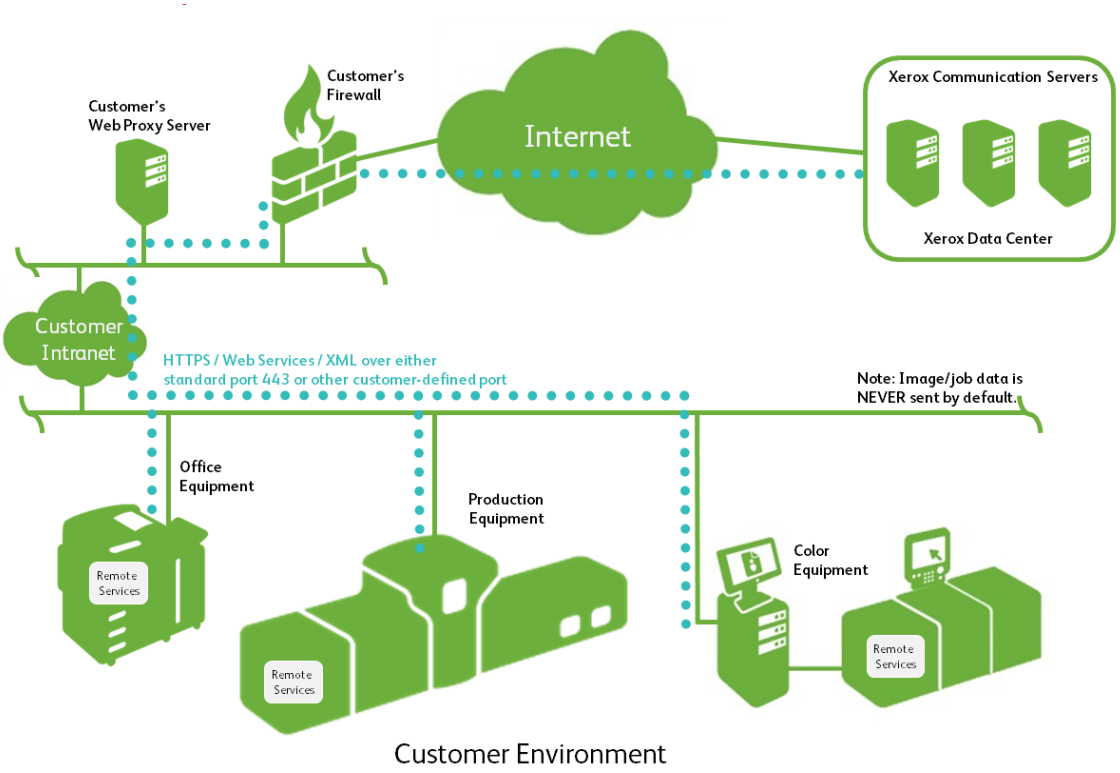

Figure 3.1.1 System Components & Data Flows of the Direct-Connect Model

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. It can be disabled on demand.

3.2 Remote Proxy Apps

The remote proxy app-based deployment model utilized within Xerox Remote Services consists of the follows system components:

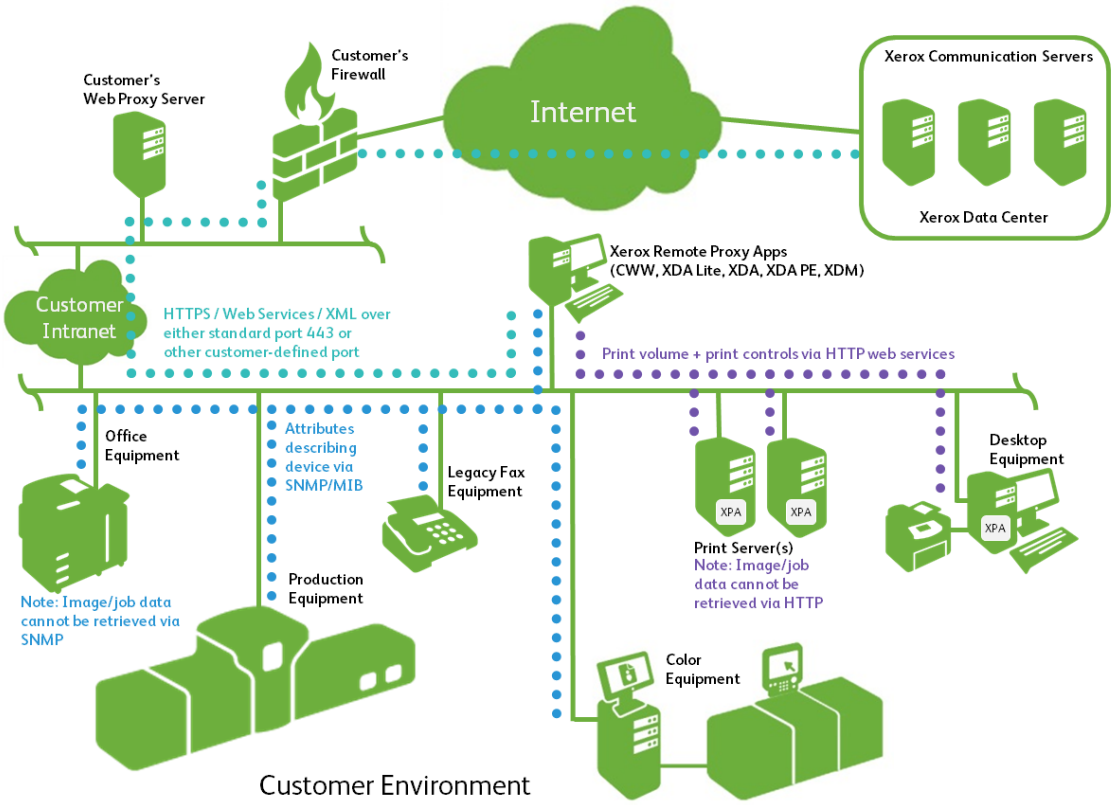

Figure 3.2.1 System Components & Data Flows of the Remote Proxy App-based Model

Note: The Xerox Print Agent (XPA) 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.). XPA 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.

3.3 Mixed Deployment Model

A combination of the direct connect deployment model and the remote proxy app-based 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 (i.e. direct connect deployment model). If the customer eventually decides to purchase one of Xerox's Managed Print Services offerings, the Remote Proxy apps will automatically take over the responsibility of periodically transmitting print device data to the Xerox Communication Servers (i.e. remote proxy app-based deployment model).

Data Transmission & Payloads

4.1 Securing the External Channel

Direct Connect Deployment Model

The remote services module embedded within Xerox devices utilizes a SSL connection over the standard port 443 in order to communicate to the external Xerox Communication Servers. This secure connection utilizes MD5 and RSA technologies to encrypt the data. Furthermore, an additional Xerox proprietary authentication mechanism is utilized to access the services at the Xerox Communication Servers.

Remote Proxy App Deployment Model

All of the Remote Proxy applications (i.e. CWW, XDA Lite, XDA PE, XDA, XDM) also utilize a SSL connection over the standard port 443 in order to communicate to the external Xerox Communication Servers. This secure connection utilizes MD5 and RSA technologies to encrypt the data. Other 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 App initiates all communications with the external Xerox Communications Servers (i.e. one-way).
- A valid URL for the external Xerox Communications Servers must be used.
- A Xerox proprietary authentication mechanism is utilized to access some of the services at the Xerox Communication Servers.
- 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 App 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 App detects the approval from the external Xerox Communications Servers and then activates the service.

4.2 Sources of Data

The following system components generate/accumulate data for Xerox Remote Services:

- Xerox Office Devices
- Xerox Production Devices
- Xerox Remote Proxy Apps

4.2.1 Xerox Office Devices

Xerox Office-base print devices transmit the following structured attribute data in a Xerox proprietary XML format based upon the Distributed Management Task Force's Common Information Model (CIM). This structured attribute data is then compressed in ZIP format before it is 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 CRU replacement quantities, detailed CRU failure data and distributions, embedded 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

Data	Description	Xerox Service
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 this type of data to a local PC. 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:

- Check the Xerox web site 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.

4.2.2 Xerox Production Devices

Xerox Production-based print devices transmit the following structured attribute data in a Xerox proprietary XML format based upon the Distributed Management Task Force's Common Information Model (CIM). This structured data is then compressed in ZIP format before it is 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, location	Xerox Remote Print Services only
Device Network Address	Includes 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

Data	Description	Xerox Service
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:

- Check the Xerox web site 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.

4.2.3 Xerox Remote Proxy Apps

The Xerox Remote Proxy Apps (i.e. CWW, XDA Lite, XDA PE, XDA, XDM) transmit the following **attribute data that is retrieved from print devices** in an XML format that is compressed using ZIP and then encrypted before it is transmitted directly to the external Xerox Communication Servers:

Data	Description	Xerox Services
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.	All (XRPS, XPS, XPPS, EPS, Xerox® PagePack® 3.0)
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.	All (XRPS, XPS, XPPS, EPS, Xerox® PagePack® 3.0)
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.	All (XRPS, XPS, XPPS, EPS, Xerox® PagePack® 3.0)
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.	All (XRPS, XPS, XPPS, EPS, Xerox® PagePack® 3.0)

Data	Description	Xerox Services
Print Device Counters	Includes billing meters, print-related counters, copy-related counters, fax-related counters, large job-related counters, scanning-related counters, usage statistics, target volume.	All (XRPS, XPS, XPPS, EPS, Xerox® PagePack® 3.0)
Print Device Consumables	Includes consumable name, type (e.g. imaging, finishing, paper media), level, capacity, status, size, etc.	All (XRPS, XPS, XPPS, EPS, Xerox® PagePack® 3.0)
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 XSM). 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. XPS, XPPS, 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.	XPS, XPPS, EPS
Print Device Engineering / Debug	**None**	NONE

NOTES:

- All print device-related data fields can be disabled for transmission back to the Xerox Communication Servers **except** device service number and all device usage counters.
- The collection of certain job attributes can be disabled from collection and transmission.
- Chargeback Codes can be integrated from MS Active Directory.

The Xerox Remote Proxy Apps (i.e. CWW, XDA Lite, XDA PE, XDA, XDM) also transmit the following **application-related data** in an XML format that is compressed and then encrypted before it is transmitted directly to the external Xerox Communication Servers:

Data	Description	Xerox Services
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.	XPS, XPPS, EPS
Remote Proxy App Corporation Security Mode	**Normal Mode** = remote app 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 app configuration disabled + remote device commands reception disabled + remote app status syncs to the Xerox Communication Servers disabled + remote app IP address /DNS name disabled from transmission + print device data pushes are disabled)	XPS, XPPS, EPS
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.	EPS only
Remote Proxy App Remote Configuration	Settings that can be managed remotely include discovery operation, data export frequency, SNMP communication-related settings (retry, timeout, community names), alert profiles, and auto remote proxy app software update frequency.	XPS, XPPS, EPS

Some of the Xerox Remote Proxy Apps (i.e. XDA PE, XDA, and XDM but not CWW nor XDA Lite) can process the following **actions requested** by the external Xerox Communication Servers:

Data	Description	Xerox Services
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 Apps which support this feature.	XPS, XPPS, EPS
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.	XPS, XPPS, EPS

4.3 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 Apps 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	Toner is automatically sent to customers when consumable depletion status is received from print devices.
Serviceability (Maintenance Assistant)	Detailed fault information is automatically sent to service personnel PDAs/RIM Blackberries to expedite the preparation for an on-site visit.
3rd Level Support (Engineering/Debug)	Product support personnel can debug difficult problems when given access to detailed engineering and debug logs .
Automatic Parts Replenishment	Replaceable components are automatically shipped to customers when needed for their production devices.

Basic print device data is retained and archived within a Xerox data center for a period of 3 years. After 3 years, both the print device data and archive are deleted by the Xerox Information Management Team. Engineering/debug log data is retained for a period of either 90 days or when the print device problem has been resolved to the satisfaction of the customer. Xerox follows many security practices very aggressively to safeguard customer data.

The work processes and practices that support and protect the Xerox back-end Remote Services software applications and customer print device attribute-related data are based upon ITIL best practices and the ISO 27000 standard. Customers can be assured that the management of data integrity, privacy, and protection are aligned with the highest available industry standards.

Technology Details

This section is provided to identify additional technical details which are typically required by IT folks and Security teams in order to enable the certification of print devices and remote proxy apps for use on the customer's network.

5.1 Software Design

Developing secure software is taken very seriously at Xerox. Software developers are required to attend security awareness training as part of the product development process. The design of both the software that controls the operations of the Xerox print devices as well as the remote proxy applications that monitor/manage these Xerox print devices is based upon secure coding guidelines disclosed within this security awareness training.

5.2 Operability

5.2.1 Xerox Remote Services Operability on a Network

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

Xerox Offering	Deployment Method	Apps Used per Xerox Offering	Data Flow on Network	Operability Imposed on a Network
Xerox Remote Print Service	Direct-connect (Figure 3.1.1)	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 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

Xerox Offering	Deployment Method	Apps Used per Xerox Offering	Data Flow on Network	Operability Imposed on a Network
			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
	Remote Proxy Apps (Figure 3.2.1)	XDA Lite + CWW	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

Xerox Offering	Deployment Method	Apps Used per Xerox Offering	Data Flow on Network	Operability Imposed on a Network
			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
Xerox® PagePack® 3.0	Remote Proxy Apps	PagePack Assistant app (PPA)	Internal	PPA app detects a Web Proxy Server (automatic or directed to a specific address)
			Internal	PPA app retrieves print device capabilities across the fleet via SNMP
			Internal	PPA app retrieves print device configuration across the fleet via SNMP
			Internal	PPA app retrieves print device status across the fleet via SNMP
			Internal	PPA app retrieves print device consumable data across the fleet via SNMP
			Internal	PPA app can submit a test page to a specific print device
			Internal	PPA app can launch a print device's web page
			External (outbound only)	PPA app traverses the company firewall to access the Internet (HTTPS over port 443)
			External (outbound only)	PPA 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)	PPA 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 XDA app detects a Web Proxy Server (automatic or directed to a specific address)
			Internal	Each XDA app retrieves print device capabilities across the fleet via SNMP

Xerox Offering	Deployment Method	Apps Used per Xerox Offering	Data Flow on Network	Operability Imposed on a Network
XPS / XPPS	Remote Proxy Apps	XDA app + XDA PE app for monitoring network-connected print devices **Xerox Print Agent (XPA) app** for monitoring PC - connected print devices	Internal	Each XDA app retrieves print device configuration across the fleet via SNMP
			Internal	Each XDA app retrieves print device status across the fleet via SNMP
			Internal	Each XDA app retrieves print device consumable data across the fleet via SNMP
			Internal	Each XDA app can submit a test page to a specific print device
			Internal	Each XDA app can launch a print device's web page
			Internal	Each XDA app can upgrade print device software via print job submission
			Internal	The XPA app can receive meter data from a PC-connected print device and then forward it onto the XDA app
			Internal	The XPA app can receive consumable level data from a PC-connected print device and then forward it onto the XDA app
			Internal	The XPA app can receive status data from a PC-connected print device and then forward it onto the XDA app
			External (outbound only)	Each XDA app traverses the company firewall to access the Internet (HTTPS over port 443)
			External (outbound only)	Each XDA 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 XDA 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	XDM/XDA apps detect a Web Proxy Server (automatic or directed to a specific address)

Xerox Offering	Deployment Method	Apps Used per Xerox Offering	Data Flow on Network	Operability Imposed on a Network
EPS	Remote Proxy Apps	**Xerox Device Manager (XDM) app** + XDA app for monitoring network-connected print devices **Xerox Print Agent (XPA) app** for monitoring PC - connected print devices, user job tracking, and print controls	Internal	XDM/XDA apps retrieve print device capabilities across the fleet via SNMP
			Internal	XDM/XDA apps retrieve print device configuration across the fleet via SNMP
			Internal	XDM/XDA apps retrieve print device status across the fleet via SNMP
			Internal	XDM/XDA apps retrieve print device consumable data across the fleet via SNMP
			Internal	XDM/XDA apps can submit a test page to a specific print device
			Internal	XDM/XDA apps can launch a print device's web page
			Internal	XDM/XDA apps can upgrade print device software via print job submission
			Internal	The XPA app can receive meter data from a PC-connected print device and then forward it onto the XDM/XDA apps
			Internal	The XPA app can receive consumable level data from a PC-connected print device and then forward it onto the XDM/XDA apps
			Internal	The XPA app can receive status data from a PC-connected print device and then forward it onto the XDM/XDA apps
			Internal	The XDM app supports SNMPv3 communications w/ print devices
			Internal	The XDM app can make changes to the print device configuration via SNMP and web UI
			Internal	The XDM app retrieves job-based accounting logs from certain Xerox MFPs
			Internal	The XDM app receives XPA job tracking data from user workstations and print servers

Xerox Offering	Deployment Method	Apps Used per Xerox Offering	Data Flow on Network	Operability Imposed on a Network
			Internal	The XDM app manages / enforces print control policies
			External (outbound only)	XDM/XDA apps traverse the company firewall to access the Internet (HTTPS over port 443)
			External (outbound only)	XDM/XDA 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)	XDM/XDA 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

5.2.2 PC Requirements for the Remote Proxy Apps

- **Only** Supported Operating Systems include:
  - XPS, XPPS, XPP = Windows XP w/ SP3, Windows Vista (all versions), Windows 7 (all versions), Windows Server 2003 w/ SP2, Windows Server 2008 SP1
  - EPS = Windows Server 2003 w/ SP2, Windows Server 2008 SP1
  - Note: Unix and MAC operating systems are **not** supported
- RAM requirements vary based upon Xerox service used (minimum 2 GB recommended)
- Disk requirements vary based upon Xerox service used (600 MB to 3GB recommended)
- Processor requirement varies based upon Xerox service used (minimum 3GHz recommended)
- Browser = Internet Explorer 7.0 (recommended), 8.0, 9.0
- All services require the MS .Net v3.5 framework w/ SP1
- Xerox Remote Print Services via CWW and EPS requires IIS 6.0+
- Xerox Remote Print Services, XPS/XPPS, and XPP utilize MS SQL Server 2005 Compact Edition (free license)
- Xerox Remote Print Services via CWW and EPS utilize MS SQL Server 2008 Compact Edition (free license)
  - Remote MS SQL data servers can be deployed
  - 1 MS SQL Server 2008 Standard or Enterprise w/ 4 CAL licenses required
  - DB server minimum = 4GB RAM, 36GB disk, Intel Pentium 4 3GHz CPU

- Typically required for XPA usage OR
- Typically required when managing 6000+ devices

5.2.3 Security Features of the Remote Proxy Apps

- The Remote Proxy apps do not utilize the Windows SNMP service nor the Windows SNMP Trap service. Therefore, these OS services **must** be disabled on any PC where the Remote Proxy app is installed, if previously enabled.
  - Note: the Windows SNMP service and the Windows SNMP Trap service are **not** enabled within the Windows OS by default.
- The Remote Proxy apps 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 apps utilize the security features available from the Windows OS including:
  - User authentication and authorization
  - Services configuration and management
  - Group policy deployment and management
  - Internet Connection Firewall
- The Remote Proxy apps can be configured to leverage the additional security features of the MS SQL Server app including:
  - user account registration
  - DSN encryption
  - reduced user account privileges to access the database (i.e. database owner rights)
  - user-defined port numbers
- A Xerox registration key and a valid Xerox account is required in order to transmit data to the external Xerox Communications Servers.
- The Remote Proxy apps external communications may be impacted by the Windows Internet Connection Firewall.
- The Remote Proxy apps 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 app UIs and features are controlled via the following roles-based privileges (e.g. CWW Administrators, CWW Power Users, CWW SQL Users, CWW Customer Administrators, and CWW 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 apps 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.

5.3 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 app web page queries	Internal
135	Remote Procedure Call (RPC)	Print device discovery + XPA operations	Internal
137, 139	NetBIOS	Printer Server discovery + XPA 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

Port Number	Protocol	Description of Use	Data Flow on the Network
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	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 XDM	Internal + External (outbound only)
445	Server Message Block (SMB)	XPA 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 because all SNMP-based traffic is generated and consumed by the Xerox Remote Proxy apps and print devices which are typically connected behind a company firewall. (i.e. **no** SNMP traffic traverses the company firewall)

5.5 Basic Security Concepts

Security is comprehended throughout the Xerox MPS Continuum of Services in the following ways:

Basic Security Concepts	Impact on Xerox Remote Services
Confidentiality	• Xerox print devices communicate with the Xerox Communication Servers using industry standard web-based protocols over a 128-bit encrypted HTTPS channel via port 443. • Xerox Remote Proxy Apps communicate with the Xerox Communication Servers using industry standard web-based protocols over a 128-bit encrypted HTTPS channel via port 443. Data encryption is also performed prior to data transmission over this channel. Specific data such as network addressing-related fields can be disabled from transmission to the Xerox Communication Servers. • Xerox imposes strict guidelines for handling customer data across internal departments that handle the data. • Numerous security features can be enabled on Xerox print devices. (Refer to the Security@ Xerox web site for more details; www.xerox.com/security) • Numerous security features can be configured on the Xerox Remote Proxy Apps. (Refer to the Security@ Xerox web site for more details; www.xerox.com/security)
Integrity	• Business processes exist which inspect device data quality against previous transmissions. • Most Xerox data centers are ISO-27001 compliant and their internal processes for handling data are based upon strict corporate IT policies and ITIL-like best practices.
Availability	**Authentication** • Xerox print device software ignores all attempts to communicate with external sources not initiated by that print device. • Print device data only pushed to the Xerox Communication Servers. • To minimize software vulnerabilities, Xerox software developers are required to attend security awareness training as part of the product development process. **Authorization** • Data transmission is enabled by default. • Xerox print device identity is authenticated prior to data transmission back to the Xerox Communication Servers. • The flow of data from Xerox print devices back to the Xerox Communication Servers is always one way; ***outbound only***. • Xerox Remote Proxy app identity is authenticated prior to data transmission back to the Xerox Communication Servers. • The flow of data from Xerox Remote Proxy apps back to the Xerox Communication Servers is always one way; ***outbound only***. • Data transmission can be disabled upon demand.

Basic Security Concepts	Impact on Xerox Remote Services
	Availability • Xerox Communication Servers frequently exceed the 99.5% availability target. • Xerox Data Centers are manned 24 hours a day, 7 days a week, 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 frequency of data transmission for the Xerox Remote Proxy apps depends upon the contracted levels of service. • Minimal impact to the customer's network.
Accountability	• Transaction-related logs (i.e. action, audit, event, E-mail, etc.) are available from the Xerox Remote Proxy apps. • Audit logs are available from Xerox print devices.
Non-repudiation	• Xerox print device Web UI can be utilized to view the latest data that was transmitted back to the Xerox Communication Servers. • Transaction-related logs (i.e. action, audit, event, E-mail, etc.) are available from the Xerox Remote Proxy apps. • Audit logs are available from Xerox print devices. • MySupportPortal (http://www.xerox.com/about-xerox/mysupport/enus.html) provides access to meter data and supplies data sent from the Xerox print devices.

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 levels. Utilize either the print device's web UI or the printer management app 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 UI of office-based print devices and local 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 UI of office-based print devices and local UI of production-based print devices.
4. Utilize secure protocols when possible. This is typically done at the web UI of office-based print devices and local 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 IT policies prohibit the transmission of network address-related data outside of the network, the remote proxy app deployment model is required because these data fields can be disabled from transmission back to the Xerox Communication Servers.
8. If the Xerox Remote Proxy apps will be deployed:
    a. Do **not** install any of the Remote Proxy apps on a domain controller.
    b. Do **not** combine any of the Remote Proxy apps on the SAME PC/laptop/server.
    c. Do **not** enable the Windows OS-based SNMP service nor the SNMP Trap service on the PC that the Remote Proxy apps will be installed on.
    d. Always install the latest patches to the Windows OS on the PC/laptop/server running the Remote Proxy apps.
        i. Before using the MPS Remote Proxy apps, make sure that the PC/ laptop/server has been rebooted after the Windows OS patches are installed.
    e. Make sure that the Remote Proxy app PC/laptop/server is continuously powered on during normal business hours in order to prevent disruption of services enabled by the Xerox Communication Servers.
    f. Make sure that the print devices are powered on during normal business hours.
    g. Make sure that SNMP is enabled on your networked print devices.
    h. Change the SNMP Community names from their well-known default values (i.e. "public"). However, make sure not to use too many different names because print

device discovery performance is adversely impacted by the number of different SNMP Community names used.

i. Make sure that the SNMP Community names are known and configured properly (i.e. values need to match on both the print device and the Remote Proxy app).

j. Make sure that the network supports the routing of SNMP across the various subnets.

k. Be careful when considering the use of SNMPv3. Although this protocol does provide data encryption and authorization capabilities, it requires that user accounts be placed within all print devices to be managed which can be a very time-consuming administrative task [e.g. depending upon the account strategy used for deployment (single vs. multiple) + account configuration per device, etc.]

l. Xerox® CentreWare® Web (CWW) and Xerox Device Manager (XDM) apps require the use of IIS. Therefore, the following recommendations apply:

    i. Use an alternative web site instead of the IIS default web site for the CWW/XDM installation.

    ii. Change the port number used by HTTP.

    iii. Utilize HTTPS for secure communications.

    iv. Disable anonymous communication to all CWW/XDM pages.

    v. Restrict access to CWW/XDM to specific IP addresses.

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

m. Use the Configuration Sets feature within CWW 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 disk overwrite.

    vi. Disable software upgrade when not upgrading the fleet.

Appendix A: Deployment Model Selection

Which deployment model should I use?

The Direct-Connect deployment model (see figure 3.1.1) should be used when:

- Xerox print device deployment is small (e.g. < 10 devices; workgroup environment)
- IT policies permit the secure direct connection of print devices to external web sites
- Little or no management of print devices exist (i.e. want to leverage device automation features)
- Customer does not want to be involved w/ any manual billing or consumables replenishment-related activities
- Customers may not want to use their own computer/server equipment to install the Xerox remote proxy apps.

The Remote Proxy App-based deployment model (see figure 3.2.1) should be used when:

- Xerox print device deployment is more than 10 devices (i.e. for small, medium, or large business environments)
- IT policy prohibits the direct connection of print devices to external web sites
- IT folks want control over the data flow to the Xerox Communication Servers (i.e. a single data channel)
- IT folks require basic fleet monitoring of their print devices from a central location
- Customer does not want to be involved in any print device management-related activities (i.e. customer interested in Xerox MPS offerings)

Note: Although remote proxy apps were created for the entire Xerox MPS Continuum of Services, only the Xerox® CentreWare® Web app and the Xerox Device Agent Lite app are provided for customer use. Other similar remote proxy apps are utilized by Xerox personnel and/or 3rd party service partners to provide enhanced MPS services.

[Page Left Intentionally Blank]