Security FAQs (Frequently Asked Questions) for Xerox Remote Print Services

February 30, 2012

Printed in the United States of America.

Changes and corrections will be periodically made to this document.

Document Version: 1.0 (February 2012).

Introduction

Xerox Remote Print Services is optional software available with networked Xerox products to provide remote connectivity to Xerox across the Internet to support Automated Meter Reporting (AMR), Automated Supply Replenishment (ASR) and/or trouble-shooting of problems. This document is intended to help the customer complete a formal or informal risk analysis to asXRPSs Xerox Remote Print Services.

Questions & Answers

Q1: What is involved in Xerox Remote Print Services?

A1: System components of the Xerox Remote Print Service are:

- Xerox Print or Multi-Function device
- Xerox software
- customer network
- Internet
- Xerox Communication Servers

The high level architecture is illustrated in Figure 1 below.

Xerox Remote Print Services gathers Print Device operational information automatically and reports it back to Xerox to facilitate automated meter reads, supplies replenishment and/or maintenance. Information transmitted to Xerox may include the Print Device serial number, meter name, meter values, and supply usage values. Copy, Print, Fax, or Scan image data is never transmitted to Xerox through Xerox Remote Print Service. Three services are currently available for Xerox Remote Print Services: Meter Assistant, Supplies Assistant, and Maintenance Assistant.

For more information, please visit this website: www.xerox.com/smartesolutions

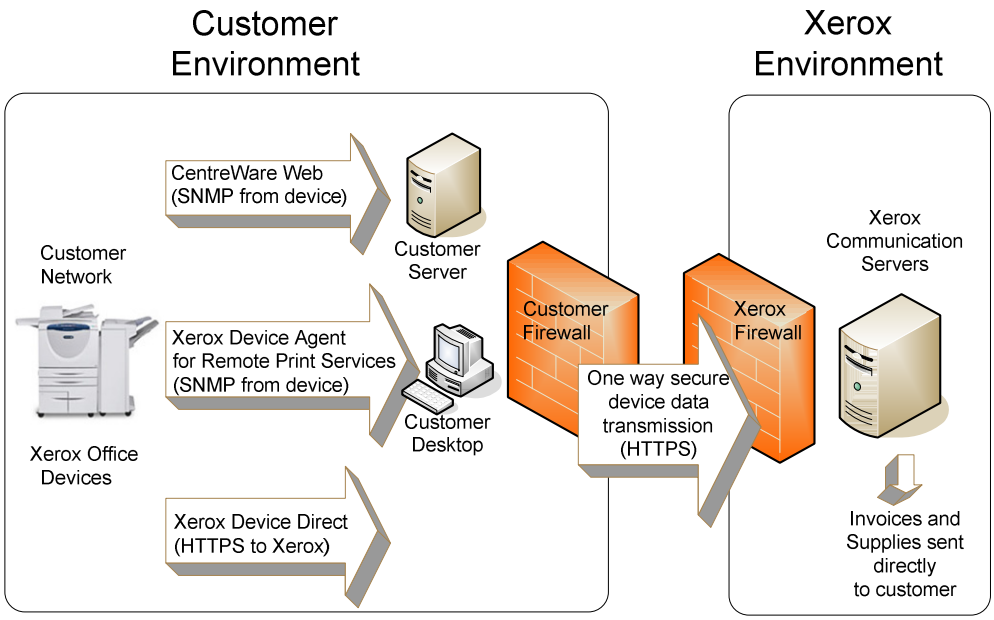

Figure 1 Xerox Remote Print Service Architecture

Q2: What Xerox software options are available for Xerox Remote Print Services?

A2: Customers can choose among three options for connecting their device with Xerox Remote Print Services.

Device Direct – Software is embedded on the device and resides on the Xerox Print Device. At installation in the customer environment, this software will automatically attempt to connect to the Xerox Communication Servers to report meter and supply information, no user intervention required. Authorization for this installation is documented in the standard lease terms and conditions for Xerox devices.

Xerox Device Agent for Xerox Remote Print Services (XDA for XRPS) – The customer is required to download software from www.xerox.com ,install and manually configure on a Windows® client device in their environment . This software must be configured at installation by the customer. It will discover Print Devices, gather meter and supply information from them , and report it to the Xerox Communication Servers. This option does not provide support for the Maintenance Assistant service.

CentreWare Web (CWW) – The customer is required to download software from www.xerox.com and install on a Windows® client device in their environment. This software must be configured at installation by the customer. In addition to discovering Print Devices and reporting meter and supply information like the XDA for XRPS, the software provides a number of features to assist the customer in managing their Xerox devices.

Q3: Which Xerox Remote Print Services software is most secure?

A3: A customer can have high confidence in all Xerox Remote Print Services software developed by Xerox. Development teams are provided training on secure coding techniques and automated tools to identify software vulnerabilities at each point in the software device lifecycle . There are no known vulnerabilities for Device Direct software or XDA for XRPS software. Customers should take care to ensure that they are always running the most current version of software.

Xerox has a vulnerability management program in place to monitor and respond to any new vulnerabilities identified for our products and Solutions described in detail here http://www.xerox.com/download/security/white-paper/1276831-30b34-4abd1a2577dc0/cert_Vulnerability_Management_and_Disclosure_Policy.pdf Customers can sign up for an RSS feed from the www.xerox.com/security website to receive notification when security bulletins are published.

In addition to obtaining Common Criteria certification for many Xerox devices, Xerox reviews the software components of XRPS with the same external auditors that review other critical business processes.

Q4: How is Xerox Remote Print Services secured from end to end?

A4: Securing Xerox Remote Print Services requires actions from both the customer and Xerox.

Xerox Actions:

- Device Direct software is enabled by default
- Automatic detection of customer web proxy server to access the Internet
- Automatic registration of Print Devices with the Xerox Communication Servers
- Secure Development lifecycle for all Xerox developed software
- Vulnerability management program to maintain software security over life of product
- Print Device security features to secure confidentiality, integrity, and availability of information standard per device specification or available as optional security kit
- Common Criteria (CC) certification of Print Device security features. Note that Common Criteria does not lend itself to certification of all components in the system, for example the Internet.
- SSL – secures all communications between Xerox Remote Print Services and the Xerox Communication Servers across the Internet

- The Xerox Communication Servers reside in a ISO 270001 compliant facility and have a digital certificate issued by a third party Certificate Authority. A Xerox Communication Server authenticates the Xerox Print Devices by validating the username and password provided by the Xerox Devices. Xerox Devices may validate the digital certificate of the Xerox Communication Servers prior to sending information.

Customer Actions:

Required:

- Provide address of web proxy server if required. (Note: Xerox software will automatically attempt to detect the web proxy server once connected to the customer network. The auto proxy detect can be disabled.)

Recommended:

- Install Xerox Device Agent (XDA for XRPS) or CentreWare Web (CWW) for managing multiple devices
- Harden the Windows® Operating System on the device hosting XDA for XRPS or CWW. Both XDA for XRPS and CWW are compatible with the security features built into Windows® operating systems.
- Review internal Security Policy – Examples: Network Security Policy, Print Device Security Policy, Acceptable Use Policy, etc.
- Review appropriate Product Security Guidance documents for Xerox Devices published by Xerox to www.xerox.com/security
- Configure Print Device security features and periodically monitor for compliance with Customer policy
- Review Xerox Remote Print Service documentation for XRPS components selected
- Provide a secure internal network environment (Examples: Firewall, Intrusion Detection System, Vulnerability Scanning, Patch Management, and etc.)
- Sign up for RSS feed at www.xerox.com/security to monitor for Xerox Security Bulletins and deploy patches to Xerox Print Devices, if applicable
- Configure XDA for XRPS and or CWW settings to send E-mail alerts to Customer IT administrators for communication failures to the Xerox Communication Servers. This requires identification of the SMTP Server and entry of appropriate email addresses

Q5: How do CWW and XDA for XRPS find the Print Devices on the Customer Network?

A5: CWW and XDA can be manually configured to support a number of discovery options. Xerox can work with you to ensure that discovery complies with your network and security policies. After installing CWW or XDA for XRPS on a client Windows ® OS, a 'Configuration Wizard' will launch to guide the user through an initial discovery of Print Devices accessible on your network.

For CWW by default the discovery will perform an IP sweep on the local subnet where the software is installed. For XDA for XRPS, by default no discovery will happen until a subnet has been configured. Examples of configuration options are listed below

- Manually entered IP addresses
- IP sweep limited to configured subnet(s)
- Filter by SNMP Community Name Strings
- Search Print Queues (requires credentials from authorized customer network administrator)
- Run once or on scheduled basis to locate new devices
- Report only Xerox devices

The discovery mechanism works as follows. For every IP address in the specified range, a single packet is sent to request a value for a single SNMP-based RFC 1213 Object Identifier (OID). Each IP address that responds is added to the list of live IP addresses. These live addresses are then queried for two more OIDs, one from RFC 1213 and one from RFC 3805 to determine which devices are printers.

It is recommended that customers back up the Windows® systems where CWW and XDA for XRPS are installed to avoid having to re-enter data or repeat discovery operations.

Q6: What access control is available for the Xerox Remote Print Services software?

A6: Access control capabilities depend on the Xerox Remote Print Services software selected.
For Device Direct software, access can be controlled by changing the default admin password and configuring the device to require users to authenticate locally or remotely. This prevents unauthorized or anonymous users from viewing or changing configuration settings for Xerox Remote Print Services.
For XDA for XRPS and CWW access is controlled using standard network and/or Windows® access control features. Anyone who has access to the network where CWW is installed can view portions of the application. Anyone who is a power user or administrator for the Windows® client where XDA for XRPS is installed can also view portions of the application.

The areas that anonymous or unauthenticated users can access are limited to viewing groups, devices, servers and queues, and troubleshooting. For CWW, administrative and device management functions require an authenticated user, which is defined as:

- an administrator of the server where CWW or XDA for XRPS is installed
- a member of the Administrators group where the application is installed
- a member of the Power Users group where the application is installed

For CWW, unauthenticated users have no administrative privileges within the application, but can perform other functions that may affect the database. Unauthenticated users will be prompted for a valid user name and password in areas of the application where an action would modify the database, group, or Printer Properties, for example:

- New group
- Printer/queue install
- Printer/queue deletion
- Configure group
- Configure server
- Add/Delete server
- Configure directory
- Create/edit queue or printer E-Mail Alert Profiles
- Install, Upgrade, Clone or Export wizard
- Reports
- Administration

Q7: How are Xerox Remote Print Services software kept up-to-date for security vulnerabilities?

A7: Xerox maintains software through a vulnerability management process described here. http://www.xerox.com/information-security/information-security-articles-whitepapers/enus.html .
For all Xerox Remote Print Services software, security bulletins and software patches are posted to www.xerox.com/security. Customers can sign up at this site for an RSS feed to automatically receive notifications about security bulletins. Customers should periodically visit www.xerox.com for new general software release for the Xerox Remote Print Services software.

XDA for XRPS supports automatic software update. This feature can be configured to

- Automatically install new software when it becomes available
- Prompt a customer administrator when new software is available
- Do not check for updates or install them automatically

Xerox recommends that XDA for XRPS is configured for automated installation with a weekly schedule to check for the availability of software updates.

Q8: Where can a customer get more information about security for the Xerox Remote Print Services?

A8: Customers can use the online support assistant at www.support.xerox.com . They can also submit specific security questions to Xerox by accessing www.xerox.com/security and selecting the 'Submit a question or request more information on product security' link.

Q9: What should a customer do if a security incident is suspected or found with the Xerox Remote Print Services?

A9: Customers can contact the Xerox Customer Service at 1-800-821-2797 during normal business hours. Xerox corporate security can be reached after hours at 1-866-979-8222 to assist.

Q10: Can a customer 'opt out' of the Xerox Remote Print Services?

A10: At installation, Xerox will automatically enable the Xerox Remote Print Services software on the Print Device for all Xerox Remote Print Service services. This activity is standard, with no additional charge and is authorized per the standard lease agreement. Customers may choose to 'opt out' of the Xerox Remote Print Service Device Direct software by making a request to Xerox at any time to un-enroll the device.
Customers choosing to install the Xerox Device Agent (XDA for XRPS) or CentreWare Web (CWW) software can manually un-enroll from the Xerox Remote Print Services by contacting Xerox to un-enroll a particular device or can uninstall the software following instructions in the administration guide. No service technician or service call is required to un-enroll from any Xerox Remote Print Service..

Q11: Can a customer enroll or un-enroll from the Xerox Remote Print Services or is a service call required?

A11: Customers can enroll or un-enroll from the Xerox Remote Print Service at any time for a single device or for all devices. No service technician or service call is required.

Device Direct – using a web browser, the Customer administrator connect to the CentreWare Internet Services (CWIS) webpage on the Print Device, logs in, and un-enrolls the Xerox Remote Print Services for a single Print Device.

Xerox Device Assistant (XDA for XRPS) – Customer administrator can uninstall the application or contact Xerox to request un-enrollment for any particular device.

CentreWare Web (CWW) – Customer administrator can uninstall the application and contact Xerox to request un-enrollment for any particular device.

Q12: How do XDA for XRPS and CWW communicate to the Xerox Print Devices?

A12: XDA for XRPS and CWW normally communicate to the Xerox Print Devices using SNMP. There are options to help secure this communication.

For Xerox Print Devices using Xerox Remote Print Services Device Direct, all communication for the Xerox Remote Print Services is through HTTPS directly to the Xerox Communication Servers.

It is possible to enable the Xerox Remote Print Services Device Direct software with either the XDA for XRPS or CWW software reporting information on a particular Xerox Print Device concurrently to the Xerox Communication Servers. The Xerox Communication Servers resolve any issues and maintains the most current information reported for a Xerox Print Device.

Q13: What information is transmitted for Xerox Remote Print Services?

A13: Information sent to the Xerox Communication Server will vary in content depending on the capabilities of the Xerox Print Device model and the Services which are enabled for each device.

Image data, including any Personally Identifiable Information (PII) cannot be sent to the Xerox Communication Servers by any Xerox Remote Print Service software.

User credentials and/or system credentials for any service accounts on the device or customer host systems are not sent to the Xerox Communication Server.

The username and password used by Xerox Remote Print Service software to authenticate to the Xerox Communication Servers are not configurable and are independent of any other username and password for the Xerox Print Device or host device for CWW and/or XDA for XRPS.

The following information fields may be sent to the Xerox Communication Servers depending on the service enabled.

- Device Meter counts
- Device Supply levels
- Device Diagnostic data
- Host Device Diagnostic data

Diagnostic data provides information to support trouble-shooting of the device for performance and reliability issues and will typically include device and/or host system identification, software versions, fault codes, installed hardware options, configuration settings, and many other metrics. Diagnostic data will never include customer image data, Personally Identifiable Information (PII), or user/host system credentials but may contain engineering data from the device that is considered confidential and proprietary by Xerox.

Q14: Is the information encrypted?

A14: Information gathered by the Xerox Remote Print Service software is always transmitted to the Xerox Communication Servers through an encrypted channel. Information at rest on the Xerox Print Device is not encrypted. Information at rest on the Windows® client hosting the XDA for XRPS or CWW software is encrypted if the host device provides hard drive encryption. Options are available to encrypt information transmitted between the Print Device and CWW or XDA for XRPS.

Q15: Our company does not allow certain information, like IP addresses, to be communicated outside of our environment. Can this information be restricted from transmission?

A15: Only XDA for XRPS offers an option for 'Corporate Security Mode'. When the software is configured for Corporate Mode by selecting 'locked down' instead of 'normal', the following data is not sent to the Xerox Communication Servers.

- IP Address and MAC address of XDA for XRPS Client Device
- IP addresses and MAC addresses of Xerox Print Devices
- IP addresses and MAC addresses of other Print Devices
- Subnets used for Print Device Discovery

Additionally, when XDA for XRPS is locked down, the 'modify' remote command described in Q 19 is disabled.

Q16: How often is information transmitted?

A16: This depends on the software solution selected.

For Xerox Remote Print Services Device Direct software, at the time of installation, the Xerox software will randomly establish an initial time to perform a daily synchronization with the Xerox Communication Servers. This time can be modified by following steps in the Administrative guide. Once a day the device will connect to the Xerox Communication Servers to report information for the core services and for the optional Supplies Assistant. The communication is encrypted using SSL to ensure confidentiality and integrity of the data. For XDA for XRPS and CWW, the data transmission time is configurable to a time that is convenient for the customer and ensures that the host device will be powered on to support the action.

Many customers choose to turn their Xerox Print Devices off at night or on weekends. If the device is powered off at the scheduled time for the daily synchronization, it will simply wait to perform the daily synchronization at the next scheduled time.

Billing meters are reported daily in the US. Outside of the US, billing meters are only transmitted one time during the billing cycle when a remote command is picked up from the Xerox Communications Servers which requests the meters.

For XDA for XRPS and CWW, the Synchronization window on the application displays the last time that the application retrieved information from the networked devices and when it last communicated meter reads to the Xerox Communication Servers. The screen also indicates the last successful synchronization and the next scheduled synchronization information.

Q17: How can transmissions be audited?

A17: All communication to the Xerox Communication Servers is encrypted using SSL to protect the confidentiality and integrity of the information and cannot be audited directly.

Device Direct – For many devices, some Maintenance Assistant information transmitted can be viewed in a CSV file that can be downloaded from the Xerox Print Device CentreWare Internet Services (CWIS) web interface. Customer may also log into 'My Support' at Xerox.com to review meters.

XDA for XRPS – has an event log to record information transmissions and results of Print Device Discovery actions. There is also an 'Export to File' feature which captures many transmitted settings in a .CSV file.

CWW – has a transaction log that captures certain Xerox Remote Print Services events. Event entries are recorded for the following categories:

- All - will display all the events for Xerox Remote Print Services
- Device Register – occurs when a device is registered with the Xerox Communication Server for the Xerox Remote Print Services service
- Server Register – identifies a server that has been registered
- Xerox Server Communication- verifies a communication register with the Xerox Server

.

Q18: What notifications are available if something fails for the Xerox Remote Print Service?

A18: Notifications can be configured for the CWW and XDA for XRPS software.

For Device Direct software, an email alert can be configured if there is a communications failure. Additional alerts can be set to communicate when meter data is sent or if there is a change in enrollment status.

XDA for XRPS software will alert an administrator when a communication failure occurs when attempting to transmit information to the Xerox Communication Servers.

CWW also provide features to alert up to 3 customer administrators via e-mail for the following Xerox Remote Print Services events:

- Failure to Communicate with Xerox Communication Servers (date range= 1-30 days.)
- Failure to Read Data from Device for (date range= 1-30 days)
- Devices Deleted from Xerox Remote Print Services Group

Q19: What remote commands are available for Xerox Remote Print Services software?

A19: Device Direct software and CWW support limited remote commands by checking a message queue on the Xerox Communications Servers (pull method) during the daily synchronization to see if there is a command request.

For Device Direct software only, Xerox may leave a message in the queue to request that the Print Device enroll or un-enroll from a XRPS service. If so, the software will retrieve the message and enroll or un-enroll from the selected XRPS service.

The following remote commands are available for both Device Direct and CWW.

- Enable Meter Assistant
- Disable Meter Assistant
- Enable Supplies Assistant
- Disable Supplies Assistant
- Modify Supplies Assistant
- Request billing meters

Meter Assistant and Supplies Assistant have default settings of 'disabled' at installation and must be enabled by the customer by following instructions in the administrator guide. Maintenance Assistant and Service Assistant are core services and are defaulted to 'enabled' at installation. Core services cannot be disabled without disabling all communications with the Xerox Communication Servers.
Supplies Assistant may be configured to change the data transmission frequency.

No remote commands are supported by XDA for XRPS for Xerox Remote Print Services.

Q20: Who can view information sent to the Xerox Communication Servers?

A20: Xerox personnel who are involved in billing, supplies replenishment, and technical support can view the information as part of the service delivery process. Information may be used by other Xerox internal resources to help understand and improve device performance. All information Xerox receives from customers will be subject to corporate information security policies mandating secure handling. The Xerox Ethics and Compliance Program is an integral part of daily business operations and practices.

The Xerox Code of Conduct summarizes many Xerox policies for safeguarding and using customer information (page 10) and is published here http://www.xerox.com/about-xerox/citizenship/ethics/enus.html.