Xerox® Remote Services

Frequently asked security and other questions related to data transmissions for Xerox® Remote Services.

Parmetech
Office Technology Solutions

xerox

Document Version: 2.0 (January 2020).

Preface

Xerox is a leader in providing secure document technology and solutions across the globe.

These frequently asked questions around remote services and the related control mechanisms have been complied to illustrate our commitment to the security of the device data we receive to better support you. You can be assured that our remote service strategy is built on functional, advanced and usable secure practices.

1. Xerox Remote Services

WHAT IS XEROX® REMOTE SERVICES?

Xerox® Remote Services gathers printer data automatically and reports it to our communication servers in a secure manner to facilitate Automatic Meter Reads (AMR), Automatic Supplies Replenishment (ASR), and advanced support by leveraging a comprehensive set of device diagnostic information.

Components of Xerox® Remote Services include:

- Xerox® Printer or Multifunction device
- Embedded software module
- Device management application for use on a customer supplied PC or server
- Secure Internet Connection
- Secure customer network
- Xerox Communications Server

WHY IS DEVICE CONNECTIVITY IMPORTANT?

Xerox® Remote Services capabilities are based on a technology platform that provides a flexible end-to-end system for connecting products to the Xerox infrastructure which administers our direct and managed print services. Device connectivity is critical to the delivery of an enhanced customer experience that is easier and more quickly provides the services and support you need.

Remote technology is continually evolving to improve the quality of the service and support we provide our customers. Remote diagnostics utilize Xerox proprietary technologies to securely transmit critical service data, such as firmware versions, fault history, service items approaching replacement intervals, and diagnostic information to customer support personnel and technicians. This capability greatly enhances the troubleshooting and repair process, resulting in faster resolutions and reduced printer downtime.

WHAT ARE THE CONNECTION METHODS FOR XEROX® REMOTE SERVICES AND HOW IS IT SECURED?

Customers can choose between two options for connecting their devices or fleet of devices to the Xerox Communication Servers to enable Xerox® Remote Services.

Device Direct

An embedded software module within the Xerox® device which facilitates the Xerox® Remote Services connection. At installation, the software will attempt to automatically connect to the Xerox Communications Servers to report meters, supply and diagnostic information. This feature is covered in standard terms and conditions for Xerox® devices.

- This method is a direct point-to-point encrypted connection
- This method offers a robust diagnostic data set to include faults, alerts and enable remote configuration and resolution for print devices.
- Diagnostic data provides information to support troubleshooting 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 other print device performance metrics.

Xerox® Device Agent

The device management software is installed and configured on the customers Windows / Apple® Mac PC or server, with system administrator access in the customer's secure networked environment. The software application is developed using industry standard secure coding techniques and scanned for code vulnerabilities throughout each phase of the Software Development Life Cycle. The Xerox® Device Agent software is FIPS 140-2 compliant in its implementation of SNMPv3 and integrates with Microsoft Windows security features.

- One instance of the Xerox® Device Agent software application can manage up to 2000 print devices. Basic print environment management can be managed from one central location.
- Xerox® Device Agent software can be configured using a SNMP agent to discover both Xerox® and non-Xerox print devices. This connection method is preferred as it accurately discovers both Xerox® and non-Xerox printers on a customer's network.

It is possible to enable Device Direct and Xerox® Device Agent software concurrently to the Xerox Communications Servers for a Xerox® device or set of devices. The Xerox Communications Servers maintain the most current information reported for a print device. Both methods allow administrators to create audit reports with exported HTML or CSV file formats.

A high-level Xerox® Remote Services architecture is illustrated in Figure 1

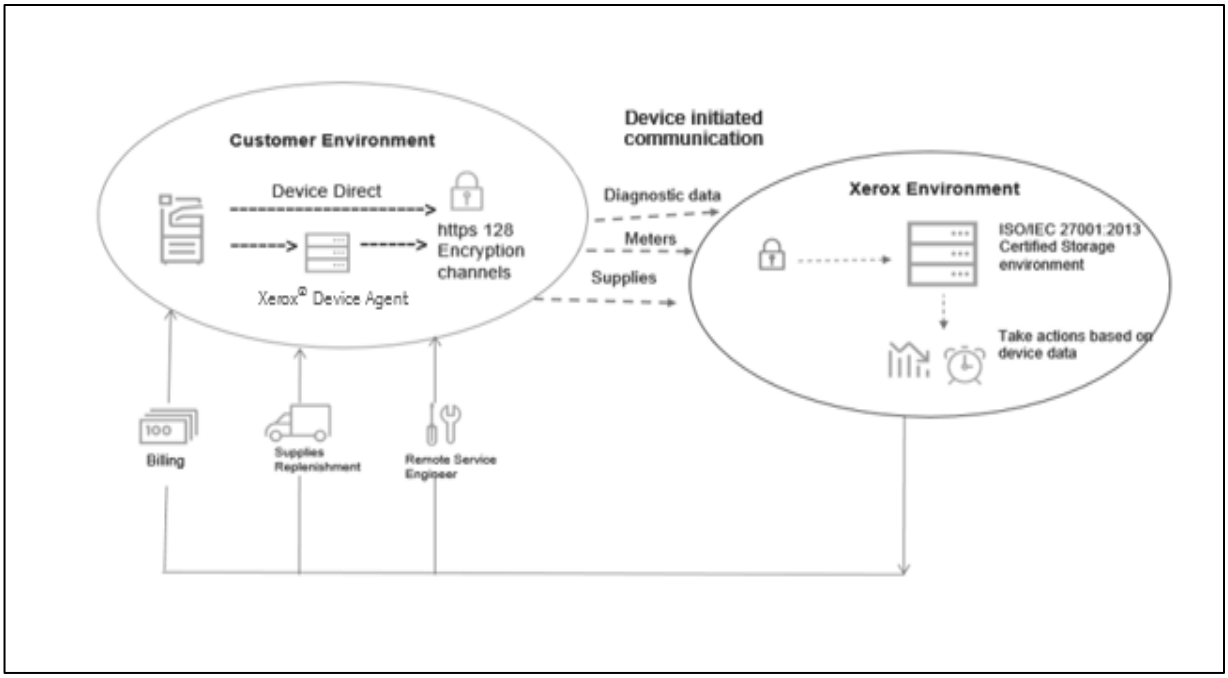

Figure 1

WHAT NETWORK PORTS ARE USED AS A PART OF THE XEROX® REMOTE SERVICES SOLUTION?

Network ports that must be open to facilitate the Xerox® Remote Services communication are listed in Table 1:

Port Number	Protocol	Description of Use	Connection Method
161	SNMP	Simple Network Management Protocol – Internal software agent used to discover Xerox® and non-Xerox print devices within the customers networked environment. v1, v2, and v3.	Xerox® Device Agent
443	HTTPS	Secure Transport Path, Secure Socket Layer(SSL)/ Transport Layer Protocol (TLS) v1.2	Device Direct and Xerox® Device Agent
515,9100,2000,2105	TCP/IP	Communication from the Device / Device Agent to Xerox Communications Servers	Device Direct and Xerox® Device Agent
25	SMTP	Email alerts for print device activity and management	Device Direct and Xerox® Device Agent

Table 1

Xerox® Remote Services device transmissions are initiated from inside the customer's environment, through the customers firewall and to the authenticated Xerox Communications Servers. Data integrity tools such as IPsec, IP filtering, secure FTP, SNMPv3, and encrypted email are also leveraged to ensure secure data transmissions.

Xerox Communication Servers reside in an ISO 27001 compliant facility, and have digital certificates issued by a third-party Certificate Authority. Xerox Communication Servers authenticate by validating the user/password provided by the Xerox® devices. The Xerox® devices will then validate the digital certificate of the Xerox Communication Server prior to sending information.

WHAT TYPES OF DATA ARE TRANSMITTED OUTSIDE MY ENVIRONMENT USING XEROX® REMOTE SERVICES?

Information being sent to the Xerox Communications Servers will vary slightly in content depending on the model and the services enabled within the customer's fleet of devices. The Xerox® Remote Print Services connection method deployed will also determine what information is being sent.

Table 2 provides the list of machine-related information that is sent to the Xerox Communications Servers, by default, of the workstation or server from which the Xerox® Device Agent software resides.

Print device data gathered may include:

- Device Meter Counts (Color Rated PPM, Black rated PPM)
- Device Supply levels (Supply type, Supply category)
- Device Diagnostic Data (Fault description, Diagnostic mode)
- Device Management Software PC or Server Diagnostic Data (Proxy ID, Host ID)

SITE INFORMATION			
Xerox® Device Agent machine DNS name	Xerox® Device Agent database size in MB	Xerox® Device Agent software build version	Xerox® Device Agent site IP address
Operating System name	Processor	Xerox® Device Agent discovery database in size in MB	Hard disk size / free space
Operating System type (32-bit vs 64-bit)	Time Zone	Discovered device count	Memory Size / available
Xerox® Device Agent Site name	Number of In-scope printers	Discovery Version	Number of Out of scope printers

Table 2

HOW WILL XEROX® REMOTE SERVICES AFFECT MY NETWORK?

The communication cadence between the customer environment and Xerox is established at the time of installation. Daily communication is recommended and set as the default setting to enhance the automated services that the remote services solution supports.

Once a day, the printer or device management software will connect to the Xerox Communications Servers to report information for Automatic Meter Reads (AMR), Automatic Supplies Replenishment (ASR), and print device diagnostic fault information. The information is sent via a secure encrypted channel to ensure confidentiality, integrity and availability of the data.

The time at which device data is transmitted is configurable to ensure the host device will be powered on to support the required actions. Many customers choose to turn their print devices off at night or on the weekends; if the device is powered off at the scheduled time for daily synchronization, the device will wait to perform the synchronization at the next scheduled time.

Using the Xerox® Device Agent software, a synchronization window on the application displays the last time the application received information from the networked print devices and the last time it communicated to the Xerox Communications Servers. The screen will also indicate the last successful synchronization and the next scheduled transmission time.

The size of that data payload can be compared to that of a standard-email, depending on the size of the network and the number of managed print devices.

The Xerox Engineering Services and Support (ESS) and Xerox Remote Services Delivery Device Data Network (DDN) Information Security Management Systems has been certified by BSI to ISO/IEC 27001 under certificate numbers IS 514590/IS 614672, respectively.

Free validation of this certification can be obtained by searching the BSI certificate directory at : www.bsigroup.com/clientdirectory