

Remote Services at Xerox

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



© 2022 Xerox Corporation. All rights reserved. Xerox® is a trademark of Xerox Corporation in the United States and/or other countries. **BR36979**

Other company trademarks are also acknowledged.

Document Version: 2.0 (April 2022).



Xerox Engineering Services and Support (ESS) and Xerox Remote Services Delivery Device Data Network (DDN) Information Security Management Systems have 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

Remote Services @ Xerox

We are 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 compiled to illustrate our commitment to the security of the device data we receive to better support you. You can be assured that our remote services strategy is built on functional, advanced, and effective secure practices.

Remote Services

Remote Service capabilities are based on a technology platform that provides a secure end-to-end system for connecting printers to the Xerox infrastructure to administer our direct and managed print services capabilities. Device connectivity is critical to the delivery of an enhanced customer experience that is simple, efficient and provides the services and support you need.

WHAT ARE REMOTE SERVICES?

Remote Services describe the process of having printer data automatically transmitted to Xerox communication servers in a secure manner to facilitate automated business processes such as Automatic Meter Reads (AMR), Automatic Supplies Replenishment (ASR), and advanced support which leverage device diagnostic information.

Components of 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
- Secure communication server

WHY IS DEVICE CONNECTIVITY IMPORTANT?

Remote technology is continually evolving to improve the quality of the service and support we provide our customers. Remote troubleshooting utilizes 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 enhances the troubleshooting and repair process, resulting in faster resolutions and reduced printer downtime.

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

Customers can choose between two options for connecting their devices or fleet of devices to the secure Xerox communication servers to enable Remote Services at Xerox.

Device Direct

An embedded software module within the Xerox® Print Device facilitates the secure remote services connection. At installation, the software will attempt to automatically connect to the secure communications servers to report meters, supply, and diagnostic information. This feature is covered in standard terms and conditions for remote services enabled Xerox® Print 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.

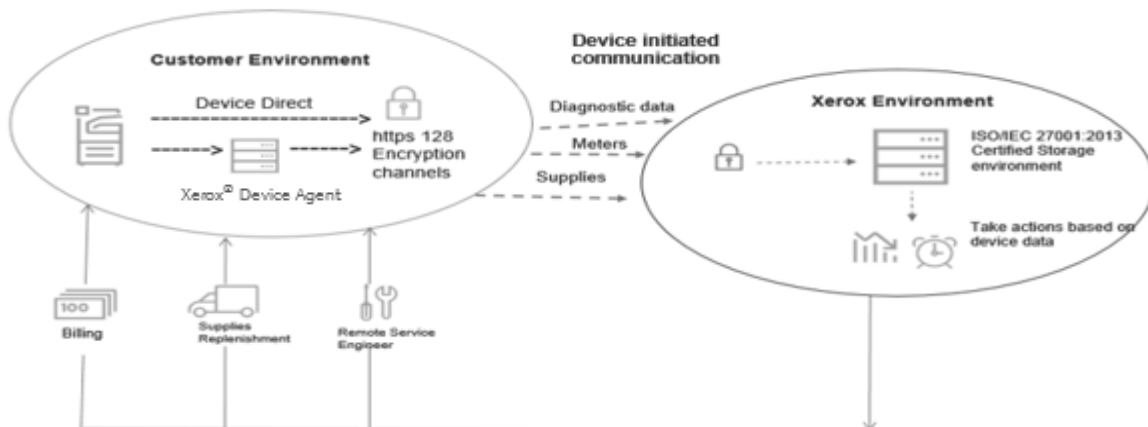
Xerox Device Agent

The device management software is installed and configured on the customer's 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 Enabling discovery verses manually inputting the device IPs of the printers you want to manage ensures all printers and MFDs are captured.

It is possible to enable Device Direct and Xerox Device Agent software concurrently to the secure communication servers for a Xerox® device or set of devices. The secure communication 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 Remote Services architecture diagram is illustrated in Figure 1



Print, Fax, or scan image data is not sent to Xerox as a part of the remote services solution. Diagnostic data **does not** include customer image data, Personally Identifiable Information (PII), user/host system credentials but may contain engineering data that is considered confidential and proprietary to Xerox

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

Network ports that must be open to facilitate the remote services communication

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 secure communication servers	Device Direct and Xerox® Device Agent
25	SMTP	Email alerts for print device activity and management	Device Direct and Xerox® Device Agent

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

The secure 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® Print Devices. The Xerox® Print Devices will then validate the digital certificate of the secure communication server prior to sending any information.

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

Information being sent to the secure communication servers will vary slightly in content depending on the printer model and the services enabled within the customer's fleet of devices. The remote services connection method deployed will also determine what information will be sent.

The table below is all machine-related information that is sent 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

HOW WILL 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 transmit the remote services 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. 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.

WHERE CAN I FIND INFORMATION ABOUT REMOTE SERVICES AND INFORMATION SECURITY AT XEROX?

Xerox Information Security

<https://security.business.xerox.com>

Remote Services @ Xerox. How to get started!

<https://www.xerox.com/en-us/about/account-management/remote-print-services>

<https://www.xerox.com/about-xerox/account-management/remote-print-services/how-to-start/>

Remote Services @ Xerox Security White paper

[Xerox Remote Services – Security White Paper](#)

Xerox® Remote Print Services supported products list:

[Xerox Remote Services Supported Products](#)

Xerox® Products Common Criteria list:

<https://www.xerox.com/information-security/common-criteria-certified>

Product Security Data Protection: Image Overwrite, Encryption and Disk Removal

https://www.xerox.com/downloads/usa/en/c/cert_Xerox_Product_Security-Data_Protection.pdf

Xerox® Product Data Overwrite Security White paper

<https://securitydocs.business.xerox.com/wp-content/uploads/2017/06/Xerox-Product-Data-Overwrite-Security-Whitepaper.pdf>

ISO/IEC 27001:2013 Information Security Management System Certification for Device Data Network

https://www.xerox.com/downloads/dl/usa/en/i/ISO_Certification_and_connectivity.pdf