October 2020
Version 6.3

Xerox® Device Agent

Security & Evaluation Guide

xerox™

To ensure the efficient fulfillment of Xerox service offerings, we leverage global competency centers and cloud technology. This may result in the personal data we process being transferred beyond the European Economic Area (EEA), but within the parameters of the defined service offering. The level of protection afforded by General Data Protection Regulation (GDPR) is not undermined through data transfers, and all transfers undertaken by Xerox are carried out in full compliance with GDPR using an approved mechanism and subject to appropriate safeguards.

Changes are periodically made to this document. Changes, technical inaccuracies, and typographic errors will be corrected in subsequent editions.

Revision History

Version	Date	Description
6.3	October 2020	support for SQL Server 2019
6.2	May 2020	Changed CloudDM to CloudFM Updated network traffic for auto update server queries
6.1	October 2019	Added reference to Cloud DM in Auto update.
6.0	May 2019	Support for Windows Server 2019. Remove references to Xerox Print Agent, which is no longer supported. Update branding. Auto upgrade is now set to automatic by default. Ability to re-register device agents in Xerox® Services Manager.
5.6	October 2018	No change
5.5	May 2018	Added note about personal data processing for GDPR. Updated hardware and software requirements, added details about remote snmp v3 discovery, new recovery services.
5.4	May 2017	Updated supported browsers
5.3	February 2016	Updates supported hardware and software requirements. Added support for Macintosh environments.
5.2	June 2015	Updated recommended hardware and software requirements

Table of Contents

Tables and Figures

Overview and How to Use this Guide

Goals and Objectives

Network and data security are one of the many challenges that businesses face on a daily basis. Recognizing this, Xerox continues to engineer and design all of its products to ensure the highest level of security possible.

This document provides additional background on the Xerox® Device Agent software capabilities, and specifically focuses on the software's security aspects. This document covers all Xerox® Device Agent configurations, and some items may not apply to the version you have. This document will help you better understand how the application functions and will help you feel confident that it transmits device data in a secure and accurate manner. This guide will help you certify, evaluate, and approve the deployment of Xerox® Device Agent in support of your contract. It includes information on the application's potential impact on security and network infrastructure as well as calculations of theoretical network traffic.

We recommend that you read this document in its entirety and take appropriate actions consistent with your information technology security policies and practices. You have many issues to consider in developing and deploying a security policy within your organization. Since these requirements will vary from customer to customer, you have the final responsibility for all implementations, re-installations, and testing of security configurations, patches, and modifications.

Intended Audience

It is expected that this guide will be used by your network administrator before installing Xerox® Device Agent. In order to get the most from this guide, you should have an understanding of:

- the network environment where you will install Xerox® Device Agent,
- any restrictions placed on applications that are deployed on that network, and
- the Microsoft Windows® operating system

Using This Guide

There are two main scenarios for using this guide: if you are a customer who does not have acceptance and evaluation procedures for this type of software or if you are a customer who has defined guidelines. In both cases, the three identified areas of concern are security, impact to the network infrastructure, and what other resources might be required to install, use, and support Xerox® Device Agent.

Use this guide to gather information about these areas and determine if you need to investigate Xerox® Device Agent further. This document is divided into these areas:

- This overview
- An introduction to Xerox® Device Agent
- Potential security-related impacts to a typical customer environment including:
- Security information, implications, and recommendations
- Roles and permission requirements of Xerox® Device Agent users

- Information about features that impact the network, which may include estimates of generated traffic, changes to the network infrastructure, or other required resources.

Limits to this Guide

This guide is meant to help you evaluate this application, but it cannot be a complete information source for all potential customers. This guide proposes a hypothetical customer printer environment; if your network environment differs from the hypothetical environment, your network administration team and Xerox Support Representative must understand the differences and decide on any certification modifications and/or future steps. Additionally:

- This guide only describes those features within the application that have some discernable impact to the overall customer network environment, whether it be the overall network, security, or other customer resources.
- The guide's information is related to the application's current release. Although much of this information will remain constant through the software's life cycle, some of the data is revision-specific, and will be revised periodically. IT organizations should check with the Xerox Support Representative to obtain the appropriate version.

Introduction to Xerox® Device Agent

Product Overview

Xerox® Device Agent discovers and monitors printing devices, specifically office printers and multi-function devices.

The application features a built-in alert detection system and has the capability to send an e-mail message to an appropriate user when certain conditions exist in the monitored devices. It also provides clear and concise status of all networked printers.

You can do the following from Xerox® Device Agent:

- Discover printers
- Notify users via e-mail when faults occur
- Monitor printers for status and alert conditions

The application supports industry-SNMP MIBs for network printers; however, the amount and type of management that it can provide is dependent on the printer's level of conformance to those standards. The following features conform to these standards:

- Printer identity (i.e. model, serial number, manufacturer, etc.)
- Printer properties (i.e. input trays, output bins, serial number, etc.)
- TCP/IP protocol suite (SNMP, TCP, UDP, IP, NIC details)
- Supported print protocols (LPD, HTTP, Port 9100)
- Consumables and levels (toner, fuser, print cartridge and device unique parts)
- Printer status including overall state, detailed status, UI messages, etc.

Note: A single instance of Xerox® Device Agent supports a maximum of 2000 network print devices. Consumers with more than 2000 network print devices will install an additional instance of the application on a different server or PC to support the remaining networked print devices

Deployment Requirements

To deploy the application install it on a desktop computer or server that has internet access and shares the network with those printers that you want to monitor.

Note: The scheduled events for meter reads and alert activity may be affected by the software's connectivity.

XEROX® DEVICE AGENT SYSTEM COMPONENT ARCHITECTURE

This diagram shows a typical configuration that a customer may deploy within their network. In this example, Xerox® Device Agent runs on a networked computer that can access the printers through the local network.

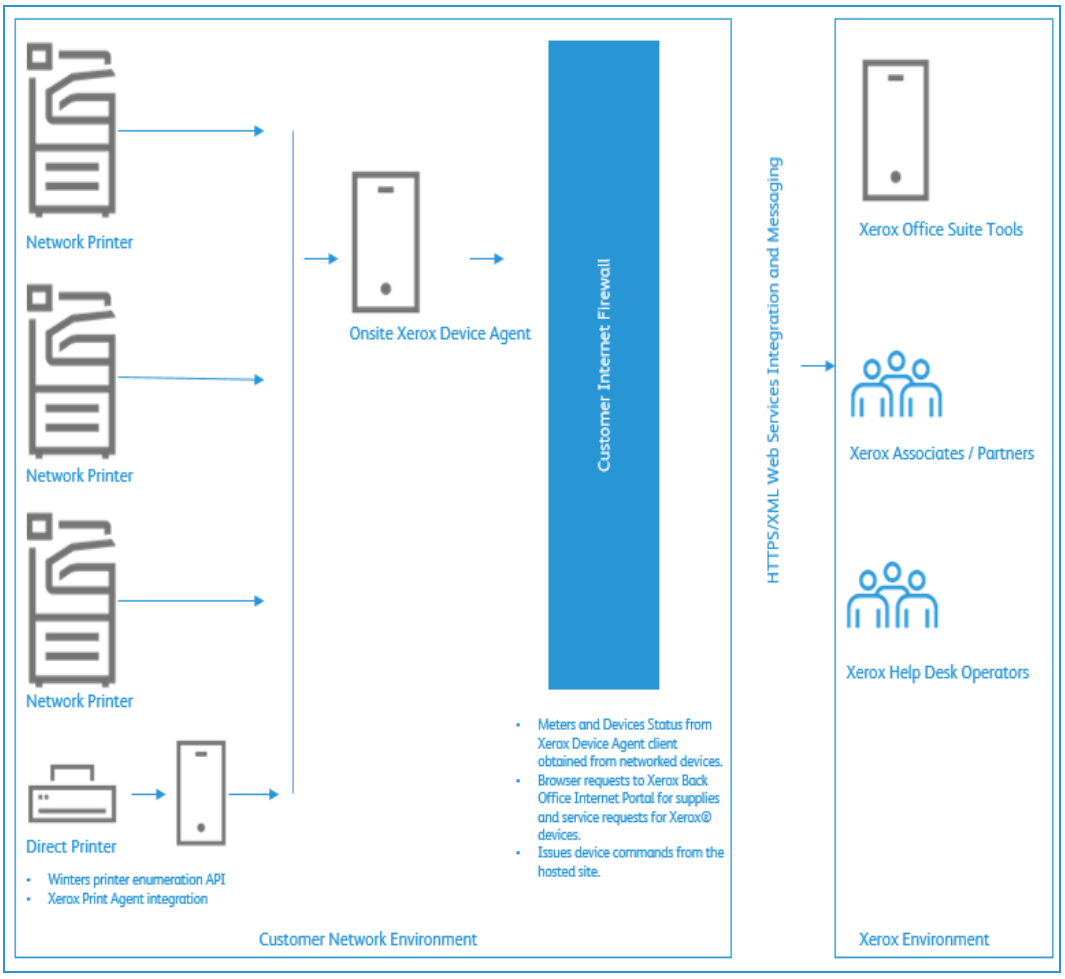

Figure 1: Typical Xerox® Device Agent Deployment

RECOMMENDED HARDWARE AND OPERATING SYSTEM REQUIREMENTS

Item	Requirement
Operating System (32-bit and 64-bit)	• Windows Server® 2012 and 2012 R2 • Windows Server® 2016 • Windows Server® 2019 • Windows® 8.1 • Windows® 10 Professional, Enterprise • Apple® OS 10.9.4 or later when run with the Parallels® Desktop hardware emulation software. Go to the Requirements to Run on a Macintosh Operating System section for requirement details. • Microsoft®.NET framework 4.5.2 Extended (Full Version) installed
Database Server	• SQL Server® Compact Edition • SQL Server® 2012 SP3 • SQL Server® 2014 SP2 • SQL Server® 2016 SP2 • SQL Server® 2017

Item	Requirement
	• SQL Server® 2019 • The software includes Microsoft SQL Server® Compact Edition for operation.
Memory	• Windows® 8.1, Windows® 10, Windows Server® 2012, Windows Server® 2012 R2: 2 GB of RAM (2.5 GB or higher recommended)
Processor	• 1.7 GHz processor or better
Hard Disk	• Minimum free space is 450 MB
Minimum Resolution	• 1024 x 768
Permissions	• You must install the application software on the client computer using the administrative account or an account with administrative privileges.
Internet Connection	• Required

Notes:

- We recommend that you update your host computers with the latest critical patches and service releases from Microsoft Corporation.
- The Network Transmission Control Protocol/Internet Protocol (TCP/IP) must be loaded and operational.
- Requires SNMP-enabled devices and the ability to route SNMP over the network. It is not required to enable SNMP on the computer where the application will be installed or any other network computers.
- You must install Microsoft®.NET framework 4.5.2 Extended (Full version) before you install the application.
- The application should not be installed on a PC where other SNMP-based applications or other Xerox printer management tools are installed, since they may interfere with each other's operation.

REQUIREMENTS TO RUN ON A MACINTOSH OPERATING SYSTEM

This table lists the system requirements that you must meet to run Xerox® Device Agent in a Macintosh environment. You can only run Xerox® Device Agent in a Macintosh environment by using hardware emulation software. You cannot run Xerox® Device Agent in a native Macintosh environment.

Item	Requirement
Apple Mac Hardware	• Intel Core 2 Duo, Core i3, Core i5, Core i7, or Xeon processor
Host Operating System for Apple Mac Platforms	• Apple OS 10.9.4 or later
Hardware Emulation Software	• Parallels Desktop v10.2.1 or later required for Apple OS X 10.9 “Mavericks” – 10.10.x “Yosemite” host systems • Parallels Desktop v11.0.1 or later required for Apple OS X 10.11 “El Capitan host system
Support Guest Windows Operating Systems Running a Parallels Desktop (32 and 64-bit)	• Windows® 7 SP0 and SP1 • Windows® 8.1, and 8.1 update (64-bit only for update 1) • Windows® 10
Additional Software	• Microsoft®.NET framework 4.5.2 installed

Item	Requirement
Memory	• 2 GB for all Windows applications
Hard Disk	• Minimum free space is 600 MB (100 MB for Xerox® Device Agent and up to 500 MB for the Microsoft®.NET framework, if not previously installed.) • An additional 850 MB of disk space on the boot volume (Macintosh HD) for Parallels Desktop installation

UNSUPPORTED CONFIGURATIONS

- Installation of the application on a computer with another Xerox device management application, such as Xerox® Device Manager.
- Installation of the application on a computer with other SNMP management tools,
- Native Mac OS® operating system software (i.e., Xerox® Device Agent can only run on the Apple Mac Platform when the Parallels Emulation Software is installed.)
- Any version of UNIX® operating systems, Linux® operating systems, Windows® systems running the Novell client, Windows® 7, Windows® XP, Windows® Vista, Windows NT® 4.0, Windows Media® Center, Windows® 2000, Windows® Server 2008, Windows® Server 2003, Windows® 8 RT, Operating systems running Terminal Services for applications and Installation on Windows systems running domain controllers.
- This application has only been tested on VMware® Lab Manager™/Workstation environments. This application may work on other virtual environments; however, these environments have not been tested

DATABASE REQUIREMENTS

Xerox® Device Agent installs Microsoft SQL Server® Compact 4.0 database engine and database files that store printer data and application settings within the installation directory. No additional licensing is required by the customer for the installation of this software product. Xerox® Device Agent also supports existing instances of SQL Server, as described above.

BROWSER REQUIREMENTS

Although Xerox® Device Agent is a Windows® application that does not require a Web browser, when accessing back office systems that may be web-based (e.g., Xerox® Services Manager) a Web browser may be required.

Printer Requirements

NETWORK PRINTER DISCOVERY/MONITORING REQUIREMENTS

For successful management by the application, all SNMP-based printer devices should support the mandatory MIB elements and groups as defined by the following standards:

- RFC 1157 (SNMP Version 1)
- RFC 1213 (MIB-II for TCP/IP-based Internet)
- RFC 2790 (Host Resources MIB v1/v2)
- RFC 1759 (Printer MIB v 1)

- RFC 3805 (Printer MIB v 2)
- RFC 3806 (Printer Finishing MIB)

DIRECT PRINTER REQUIREMENTS

Queue-based discovery depends on user permissions on domain and/or across computers, NetBIOS File and Printer Sharing, Network Discovery, and WMI.

Security

Since security is an important consideration when evaluating tools of this class, this section provides information about the security methods used by Xerox® Device Agent.

Application

The application is compatible with the security features built into the Windows® operating systems. It relies on a background Windows® service running under the local system account credentials to enable proactive monitoring of printers, gathering of data, and submission to Xerox® Services Manager. The user interface that displays the gathered data is accessible only to the power users and administrators who have login access to the Windows® operating system.

INSTALL

The installer requires administrator privileges. A single Windows® service, "Xerox Device Agent Service" is installed and configured to run under the local system Windows® account. No special system level configuration change is required or made by the installer. Xerox® Device Agent is compatible with the security features built into the Windows® operating system including:

- User authentication and authorization
- Group policy deployment and management
- Internet Connection Firewall (ICF) including:
  - Security logging settings
  - ICMP settings

Note: Make sure that the PC or server that is running Xerox® Device Agent is continuously powered on during core business hours to prevent interruption of automatic communications between Xerox® Device Agent and Xerox.

LICENSING

The customer must accept the End User License Agreement (EULA) that is presented upon Xerox® Device Agent installation. No additional licensing is required by the customer for installation of the Microsoft SQL Server® Compact 4.database.

Note: This section only applies to Xerox® Print Services and Xerox® Partner Print Services.
To successfully operate Xerox® Device Agent, you must have a Xerox services contract and an account on Xerox® Services Manager. During the software configuration process, you will need to pair Xerox Device Agent with an Xerox® Services Manager account in order to activate Xerox Device Agent. For this reason, you are required to use a Xerox® Services Manager registration key supplied by Xerox or your service provider. Depending on your account, you may also be required to use a secondary registration key.

POST INSTALL NORMAL OPERATION

The Xerox® Device Agent Windows® service runs as a background process even when no user is logged in. This enables the application to monitor the devices on the network and generate alerts proactively. If you are a power user or an administrator authenticated by Windows and you log in to the system, then you have access to the Xerox® Device Agent's user interface. You can monitor the printers, view printer data, and change settings. The application's user interface verifies that you are a power user or you have administrative privilege as you attempt to run the application. If you are not an administrator, the application will display a message that states you need administrative privileges in order to run the application.

Network Printer

The Simple Network Management Protocol (SNMP) is the most widely-used-network-management tool for communication between network management systems and the networked printers. The application utilizes SNMP during discovery operations to retrieve detailed data from output devices detected on the network. After discovery, SNMP is used to monitor printers for alerts, changes in status, configuration changes, and to support printer troubleshooting. Xerox® Device Agent supports SNMP version 1\2 and version 3 protocols. The following application properties will help you better understand the impact to printer security:

- it does not modify the settings on the printer; it only reads them.
- it does not register for SNMP traps.

  Exception: Honeywell devices can register for traps.
- it does allow the printer to be reset (this requires that devices support printer reset via SNMP).

SNMP V1-V2 SECURITY

In its current form, SNMP's security is limited to three methods of access: read-only, write-only, and read-write. Access from Xerox® Device Agent to the devices is granted by the use of community name strings. Although usually referred to as the password, for SNMP operations, the community name provides a very simple level of authentication for all Protocol Data Unit (PDU) operations. Theoretically, you can assign community names to every subnet on a network. Every printer on a local subnet will have the same community name. You can assign printers on a different subnet to a different community name. By default, Xerox® Device Agent uses the community name string of public, which is the printer manufacturer's default setting. You can elect to change this setting on the printers and you have the ability to change the community name string that Xerox® Device Agent uses to match the settings for the configured printers.

SNMP V3 SECURITY

SNMP, however, is being expanded in version 3 to include security and administration. The SNMP V3 framework supports multiple security models, which can exist simultaneously within an SNMP entity. Messages in SNMP V3 contain a field in the header that identifies which security model must process them. To ensure some form of interoperability, a User-based Security Model (USM) is implemented to defend against unauthorized modification of managed elements and spoofing. Although SNMP V3 is a huge step forward in secure manageability, it cannot prevent denial-of-service attacks. In addition, its security system must

stand alone, meaning every device must have a database of users/passwords. In companies that do not support a standalone security system all devices are left at risk.

Xerox Back Office Integration

The application communicates with Xerox® Services Manager and our billing systems on a periodic basis. It is important to recognize that Xerox® Services Manager is hosted in an ISO 27001-compliant facility. The data exchanged during such communications is compressed and encrypted. The security of this communication is protected by several mechanisms.

- You must configure Xerox® Device Agent with a valid account registration key, which is provided by a Xerox representative.
- The Xerox® Device Agent to Xerox infrastructure communication method is further secured by the use of industry-standard, secure HTTPS, which is HTTP using a Secure Socket Layer (SSL).
- Xerox® Device Agent initiates all contact with Xerox and no special firewall configuration on the site is required to enable communication.
- Xerox® Device Agent will require a valid proxy if one is required for Internet communication.
- The Xerox® Services Manager data store and administrative services sit behind a secure firewall and is not accessible from the Internet.
- Xerox® Services Manager user interface access requires authentication. Xerox® Device Agent information is stored in an account specific to the customer site. Access to that account data in Xerox® Services Manager is restricted to the Xerox® Services Manager account managers.
- Here is the list of top-level items exchanged during periodic communication with Xerox and their frequency:
  - Printer Data Export: Default once per day. User configurable via Synchronize settings.
  - List Import: Default once per day. User configurable via Synchronize settings.
  - Site Status Export: Default once per day. User configurable via Synchronize settings.
  - Site Settings Import: Default once per day. User configurable via Synchronize settings.
  - Check for a remote command: User configurable via Synchronize settings. The data traffic generated from this check is negligible. (See the Network Impact section for more information).
- Here is the list of top-level items exchanged on an as-needed basis:
  - Site Settings Export: Every time the settings are changed.
  - Commands and settings from Xerox® Services Manager.
  - Export of printers on request from Xerox® Services Manager via Remote Command.
- All communication instances are logged and can be viewed either in the **Settings>Log** screen or in the PC's Xerox DM (Device Management) event log.
- Xerox® Device Agent includes a small background service that queries the Auto Update Service hosted by Xerox to see if the Device Agent's associated Xerox® Service Manager account has been linked to a Xerox® Workplace Cloud account. If the account is linked, then the Xerox® Device Agent will then call the Xerox® Workplace Cloud to download the Cloud Agent installer. Communication between the Device Agent and the Auto Update Service is via HTTPS (port 443).

DEVICE INFORMATION COMMUNICATED TO XEROX

The data that is sent to Xerox is printer-specific, which is primarily billing counters, supply levels, and printer alerts. Here is the list of printer fields or multi-function device (MFD) attributes published by Xerox® Device Agent:

Printer Data			
2-Sided Percentage	Advanced Finishing Supported	Advanced Status Update Date	Analog Fax Capable
Alerts	Comment	Port	Workstation
Analog Fax Description	Analog Fax Modem Installed	Analog Fax Phone Number	Black Rated PPM
Can Manage	Color Capable	Color Rated PPM	Compliance Level
Console Country	Console Language	Customer Asset Number	Device Time Zone
IP Default Gateway	Description	Device Language	DNS Name
Discovery Date	Discovery Method	Discovery Type	Hard Disk Present
Duplex Capable	Fax Status	Finishing Options	Firmware Level
Hard Disk Size MB	IP Address Changed	IP Address (Device)	Icon
Last Known IP Address	Last Status Attempt	Location	MAC Address (Device)
Machine Up Time	Status	Managed State	Manufacturer (Device)
Marking Technology (Device)	Marking Technology	Manage Request Date	MIB Country
Model	Physical Memory Total MB	Queue Name	Scan to File Capable
Scan to Internet Fax Capable	Scan to Server Fax Capable	Scan to E-Mail Capable	Scanner Description
Scanner Installed	Scanner Status	Serial Number (Device)	Serial Number Scrubbed
Services Supported	Status Date	Subnet Address	Subnet Mask
Supplies (Paper Trays, Output Bins, Finisher, Imaging)	System Contact	System Name	Traps Supported
Target Volume	Traps Enabled	Type	Update Date
Utilization Percentage	Xerox Asset Number	Usage Counters	

Table 1: Printer Data Communicated to Xerox

XEROX® DEVICE AGENT SITE INFORMATION SENT TO XEROX

This table lists the attributes published to Xerox at predetermined intervals. The attributes only relate to the server or PC on which the application is installed. With the exception of administrator contact information, no Personal Identifiable Information (PII) nor business intellectual data is ever transmitted to Xerox.

Note: This information is a subset of what is collected during the registration process.

Site Information			
Xerox® Device Agent machine DNS name	Xerox® Device Agent machine IP address	Xerox® Device Agent site name	Xerox® Device Agent software build version
Number of In Scope printers	Number of Out Of Scope printers	Xerox® Device Agent database size (in MB)	Xerox® Device Agent discovery database size (in MB)

Site Information			
Operating system name	Operating system type (32-bit or 64-bit)	Processor	Hard disk size / free space
Memory Size / available	Time Zone	Discovery Version	Discovered Device Count

Table 2: Xerox® Device Agent Site Information Sent to Xerox

XEROX® SERVICES MANAGER INITIATED REMOTE COMMANDS TO XEROX® DEVICE AGENT

Note: This section only applies to Xerox® Print Services and Xerox® Partner Print Services.

The Remote commands capability allows account administrators within Xerox® Services Manager or Xerox Operations Center personnel (depending upon contract specifications) to request Xerox® Device Agent to execute a number of commands on behalf of Xerox® Services Manager. Xerox® Services Manager does not tunnel into a customer's IT network firewall. Xerox® Device Agent periodically polls its corresponding account within Xerox® Services Manager to see if the account administrator has posted a command request to Xerox® Device Agent. This polling is a Web interface interrogation by Xerox® Device Agent. The network bandwidth loading for the customer's IT network is a function of the performed operation. Once the command request has been fetched from Xerox® Services Manager and executed by Xerox® Device Agent, any operations results will be sent back to the Xerox® Services Manager server for the account manager to review.

Default frequency for remote command check is one minute. Xerox® Services Manager can be used to configure the remote command check polling interval. When it is configured for instant remote commands, Xerox® Device Agent will make an immediate connection to Xerox® Services Manager for remote commands, and the session will be left open until a command is posted or the session times out. When a command is posted, Xerox® Device Agent will execute the command and return to Xerox® Services Manager with the results, and then reopen a new session. If there is a timeout, a new session will be established with Xerox® Services Manager within 60 seconds. In this configuration, we can get real-time responses to commands, reducing the time those operations centers wait for information.

XEROX® DEVICE AGENT REMOTE CONFIGURATION

Note: This section only applies to Xerox® Print Services and Xerox® Partner Print Services.
Xerox® Device Agent supplies device information to, and requests remote commands from, Xerox® Services Manager. This ability to query Xerox® Services Manager for commands allows you to modify some of the application's settings remotely. It is important to recognize the fact that Xerox® Services Manager does not push commands to Xerox® Device Agent; rather, this information is queued and Xerox® Device Agent will poll Xerox® Services Manager for it. You can configure the polling interval in Xerox® Device Agent.

Settings	Description
Device Discovery	Xerox® Services Manager can issue a request to Xerox® Device Agent for a specific IP Sweep discovery, which can include individual DNS or IP addresses, IP address ranges, and lists of subnets. The definition for the IP Sweep specified by Xerox® Services Manager is stored locally within Xerox® Device Agent's built-in Xerox® Services Manager Sweep. Using the results of this sweep, Xerox® Device Agent will automatically upload any new discovered printer information and a results summary, so that the Xerox® Services Manager account manager can review it.

Settings	Description
Data Export	Within Xerox® Services Manager, you can configure when the devices are exported to Xerox® Services Manager.
Network	You can use Xerox® Services Manager to change the default number of retries and timeout for printer communication, how often to retrieve status from both managed and unmanaged printers, and the SNMP "SET" and "GET" community strings names that are used when communicating with a printer.
Auto Update	Within Xerox® Services Manager, you can configure when Xerox® Device Agent checks for updates and the Update Preference setting (Automatic, Prompt or Never).

Table 5: Remote Configuration

CORPORATION SECURITY MODE

Within the Synchronize>Change Settings feature, there is a configuration item for Corporation Security Mode. The two modes that exist are Normal and Locked Down. In Normal mode, Xerox® Device Agent contacts Xerox® Services Manager daily. Settings can be remotely changed without the need for on-site visits, even when the polling schedules are switched off. In Locked Down mode, besides printer-related data synchronization, there is no communication with Xerox® Services Manager and settings have to be changed on-site. Additionally, the Xerox® Device Agent machine and printer's IP addresses are not reported to Xerox® Services Manager.

Network Impact

Company network guidelines will typically enable or disable specific network ports on routers and/or servers. Your IT department will mostly be concerned with the ports used by the application for outgoing traffic. Disablement of specific ports may impact the application's functionality. Refer to the table below for specific ports used by the application's processes. If the application is required to scan across multiple network segments or subnets, routers must allow the protocols associated with these port numbers.

Port Number	Port Name	In/Outbound	Comment
161 (typical)	SNMP	Out[1]	Network printer discovery, retrieve device capabilities/status/usage counters, single device configuration
25	SMTP	Out[3]	E-mail alerts
135	RPC	Out[1]	Windows Remote Procedure Calls (RPC)
80 (typical)	HTTP	Out[1]	Get printer image and link to the printer's webpage **Note:** If HTTPS is enabled, 443 port is used.
443	HTTPS	Out[2]	Secure Xerox® Device Agent-to-Host Xerox® Services Manager data transfer, Auto Upgrade
515, 9100, 2000, 2105	TCP/IP	Out[1]	Troubleshoot, Print Test Page, Printer Upgrade
n/a	ICMP (ping)	Out[1]	Network Printer Discovery, Troubleshoot
53	DNS	Out[1]	Default port used for DNS-based device searches.

Table 6: Xerox® Device Agent Ports

1 Communication within the Xerox® Device Agent installed local network.

2 Communication outside the Xerox® Device Agent installed local network.

3 Communication location depends on configuration.

For example, if the ping requests cannot be routed through the environment between the Xerox® Device Agent machine and the printers managed by Xerox® Device Agent, the following features will not function or will show significant performance degradation:

- Troubleshoot Printers
- Network Printer Discovery

Discovery

The discovery function allows the application to search for network printers on a customer's intranet. Printer discovery is a crucial part of the application because it is the main method to identify networked-connected devices and store them in the local database. It involves the generation and querying of network addresses (via SNMP) for printer type and general configuration information. Since this operation uses the network resources, you should consider what you want to detect and then configure the discovery to achieve this goal with a minimum of network contention. If there are specific addresses that should not

be scanned, they can be entered into an exclusion list and Xerox® Device Agent will not try to contact those addresses.

DEVICE DISCOVERY METHOD

After you install the application onto a networked computer, select what subnet(s) to scan (default is local subnet), and the application will begin to automatically discover network printers according to these settings. Depending upon network configuration, this initial discovery could identify all of the network printers within the customer's environment. A method known as IP Sweep is used to perform this local subnet network printer discovery. The application also allows the network administrator to perform the discovery beyond the local subnet. For this purpose, the network administrator can specify individual IP addresses or DNS addresses of the printers, a range of addresses, or subnets that will be searched.

Note: As a rule of thumb, each discovered printer might generate as much as 50 KB (maximum) of network message traffic including device capabilities, usage counters, and an alert table.

IP SWEEP OPERATION

IP Sweep Discovery method is the preferred method of accurately discovering printers on a network. A packet is sent to every IP address in the user-defined address or address range list. The address list should be known and provided before running the discovery.

Specifically:

- A single packet is sent to each IP address contained within each subnet or address range defined within the current IP address for the current IP Sweep. In this packet, Xerox® Device Agent requests a value for a single SNMP-based RFC 1213 Object Identifier (OID).
- For each device that responds to the RFC 1213 OID, Xerox® Device Agent will add the IP address of the response packet into its list of live IP addresses.
- Xerox® Device Agent then queries those devices with live IP addresses for two more OIDs: one RFC 1213 OID and one RFC 3805 OID. This enables Xerox® Device Agent to identify printing devices from non-printing devices. Both groups of devices are stored within the Xerox® Device Agent database, however, only printing devices are exposed via the Xerox® Device AgentUI.
  - For those printer devices that respond to the RFC 3805 OID query, Xerox® Device Agent flags them as printers.
  - For those devices that do not respond to the RFC 3805 OID query, Xerox® Device Agent then checks an RFC 1213 OID value against database values to determine if the device is in fact a known printer. This is necessary because some printing devices (i.e. printers using external print server boxes, older printers, etc.) do not support RFC 3805 – the Printer MIB.
    - The database contains RFC 1213 values for several known supported and unsupported printers.
- Xerox® Device Agent then queries all live IP addresses for three RFC 1213 OIDs and one RFC 2790 OID.
- For those devices identified as printers, Xerox® Device Agent queries three more RFC 2790 OIDs and four more RFC 3805 OIDs to obtain some basic attributes of the printer.
- Based upon the identity of each printing device, Xerox® Device Agent then queries the appropriate vendor-specific OID and an OID from the Printer MIB in order to obtain the printer's serial number.
- Xerox® Device Agent then queries 3 RFC 3805 OIDs in order to display the printing device's rated speed in pages per minute (PPM).

- Based upon the identity of each printing device, Xerox® Device Agent then queries the appropriate OID (s) to obtain the printing device's software/firmware level.

Network Impact

The amount of network traffic generated by a sweep-based discovery is minimized because the requests are directed to specific IP addresses.

Accuracy

The IP Sweep method produces a controlled and orderly flow of data between the printers and the server, reducing network packet collisions that can introduce errors in the printer information.

DISCOVER SNMP V3 DEVICES

As accounts become more security-conscious, some of them are deciding to enable SNMP v3. Xerox® Device Agent can discover and manage these devices. To discover SNMP V3 devices, use one of two authentication modes as well as a set of keys or passwords. It is important to understand what the device settings are before setting up a SNMP v3 Discovery.

For SNMP V3 sweeps, you have the option to manage device discovery remotely through Xerox® Services Manager. The discovery method settings are synchronized on both sides during every import and export. The process to run SNMP V3 discovery remotely is documented in the Xerox Services Manager guides.

During a sync, Xerox® Device Agent will download the discovery settings from Xerox® Services Manager if there is any change in the settings. Any updates in Xerox® Device Agent will be synchronized in Xerox Services Manager during the next sync.

To Discover SNMP V3 Devices:

1. In the Search Setting dialog box, select Specified Search.
2. In the Printer Search section, select the SNMP v3 button on the top.
3. Select Search Type > Import. (This is the only supported option for SNMP v3 searches.)
   Note: To download a sample CSV file, select **Export Template** and add the relevant SNMP V3 data in the file. If you need directions on how to format the CSV file, select the instruction link to display a dialog box showing the possible format for the rows in the CSV file or see the directions below.
4. When you are ready to import the CSV file containing the discovery settings, click **Select File**, and then browse to and select choose the file.
5. Click **OK** to import the settings.

CSV File Format Overview:

The bullets below explain the fields within the CSV file.

Note: It is important that the fields be listed in the same order as below.

- DNS Name: If using the DNS name to discover the printer then enter its name here.
- IP Address: If using the IP Address to discover the printer then enter it here.
- Start IP Address: When doing a range of IP addresses this is the start address of the range.
- End IP Address: When doing a range of IP addresses this is the end address of the range.
- Subnet Mask: The subnet mask for the subnet the printer is on and must be filled in.
- "Comment": An optional comment.
- Prefix: The IP v6 prefix for the device.

- User Name: This is the SNMP v3 user name and can be found on the SNMP v3 page on the printer. Most Xerox devices use Xadmin for this value.
- Context Name: This is the SNMP v3 context name and can be found on the SNMP v3 page on the printer.
  Note: Not all printers use this, so if it is not found on the Printer's SNMP V3 page leave this value blank.
- Authentication Mode: This is how to authenticate to the device and will be MD5 or SHA1. If the printer doesn't allow this to be changed it will be displayed on the printers SNMP v3 page.
- Authentication Type: This field will be the word "password" or "key". If on the device it asks you to enter an Authentication Password and Privacy Password then put "password" in this field.
- Authentication Key/Password: This is the same information that you entered in the Authentication field on the printer and is case sensitive.
- Privacy Key/Password: This is the same information that you entered in the Privacy field on the printer and is case sensitive.

QUEUE-BASED DISCOVERY

Note: This section only applies to Xerox® Print Services and Xerox® Partner Print Services.
Queue-based discovery is used to identify directly connected printers. Only information available on the queue is detected and reflected within the application. Proper network administrator credentials or the credentials of the computers with direct printers are necessary to obtain access to the queues.

MANAGING DISCOVERY

The discovery process can be managed in a number of ways.

- The discovery schedule is configurable. The IP addresses, DNS addresses, and subnets are configurable.
- It can be controlled by the use of SNMP community name strings to query certain network printers over others.
- The discovery will provide active status on its progress.
- Device timeout and retry parameters are pre-defined with a setting of five seconds for attempt timeout and one retry allowed to get print information from slower network subnets on a customer's network. You can modify this information on the Advanced Settings screen.

Discovery Network Data Calculations

As mentioned earlier, each discovered printer could create as much as 50KB of discovery-based traffic. IP Sweep discovery sweeps all of the addresses in the ranges supplied.

Device Discovery Data Set Magnitudes On Typical Printers

The amount of data transferred during an operation, such as discovery or status polling, is a function of the device's capabilities. Measurements made on typical devices show the variability of these parameters. It is highly unlikely that any one network would be populated with only one device type. Instead, the typical case is a variety of devices that are dependent upon the particular needs of individuals or groups on the network. Here are three printer examples to demonstrate the variability in both the amount of collected data and the data transfer rate for typical devices.

Machine Model	Discovery	Status Polling
Xerox® WorkCentre® Pro 245	49.2 KB	19 KB

Machine Model	Discovery	Status Polling
Xerox® Phaser® 8560 DN	15.3 KB	14 KB
HP LaserJet 4345 MFP	29.1 KB	6 KB
Average	31 KB	13 KB

Table 7: Data Sizes

You also need to consider the frequency at which you will perform these operations. For purposes of this document, the following schedule for device data retrieval and their data set size will be assumed to be:

Operation Type	Frequency	Average Data Set Size
Discovery	Weekly	31 KB
Status Polling	Hourly	13 KB

Table 8: Data Gathering Frequencies

Assuming that Xerox® Device Agent will discover and monitor a thousand network devices on the network and each device discovery data set size is 31 KB and its status polling data set size is approximately 13 KB, this set of devices is expected to retrieve the following printer-based discovery data over the network each month

- 4 discovery cycles/month x 1,000 printers x 31 KB/printer (Discovery data set size) is approximately 124 MB/month

Network Impact Considerations Of Status Polling

Xerox® Device Agent communicates with the printers under management regularly. Each transaction consists of a series of SNMP queries with the device, first checking for a response, then progressively asking for more information until the transaction purpose is complete.

Status polling assumptions:

- Status polling traffic averages 13 KB per transmission
- Status polling occurs every day, once per hour (24x7)
- 1000 printers are being monitored

The expected amount of data to be retrieved from this set of devices over the network for printer-based discovery over one month is:

- 1000 printers x 24 hours x 30 days x 13 KB is approximately 9.4 GB per month

Total Xerox® Device Agent Data Transfer Calculations

The next traffic calculation example shows totals for an exaggerated network data transfer size during a one-month period. The total includes the use of regularly scheduled discovery and status polling.

The calculation is inflated to show an above-the-limits traffic estimate. It assumes that every network printer discovery requires:

- 50 KB of traffic to complete (except non-printer discovery),
- 19 KB for status, and
- The organization is active 30 days per month in order to demonstrate the extreme upper limits for a network with 1,000 print devices being monitored monthly.

Discovery Total

4 cycles/month x 1,000 printers x 50 KB/printer = 200,000 KB ≈ 0.19 GB/month

Discovery Traffic to Non-print Devices during a Sweep

4 cycles/month x 65,534 IP Address x 1 KB/printer = 262,136 KB ≈ 0.25 GB/month

Status Polling Total

30 days x 24 polls/day x 1,000 printers x 19 KB/printer = 13,680,000 KB/month ≈ 13 GB/month

Overall (Exaggerated) Total

0.19 GB + 0.25 GB + 13 GB ≈ 13.44 GB/month

Manufacturer Applicability

You can configure Xerox® Device Agent to support only Xerox® network printers (Xerox and Fuji Xerox) or all printers (any discoverable Xerox® or non Xerox® network printer) that communicate via SNMP. This configuration is governed by policies configured in the application. This setting affects non Xerox® printers in three ways: discovery, export of discovered printers to Xerox® Services Manager server, and scheduled export of meters for found printers. When you configure manufacturer applicability, the scheduled device discovery will attempt to find all Xerox® and non Xerox® network printers and will send printer information and meters to Xerox® Services Manager server.

Additionally, the policies configured in Xerox® Services Manager may allow you to change this value within Xerox® Device Agent. If Xerox® Device Agent is configured to allow for this setting change, it may be set to restrict discovery of non Xerox® printers. To do so, manufacturer applicability must be set to Only Xerox® Network Printers and All Queue Connected Printers.

Note: This section only applies to Xerox® Print Services and Xerox® Partner Print Services.

Manufacturer Applicability does not apply to directly connected printers. Printers of all manufacturers will be discovered when you use queue-based discovery.

Recovery Services to Monitor for Errors

Xerox® Device Agent can monitor for the following error conditions:

- Service has crashed
- Service has locked up

In addition, you can choose what action to take after an error from the following options:

- Restart the service, or
- Do Nothing (if recovery is disabled)

You can create a diagnostic file of the database and log files that will be saved to a location where they will not be overwritten. This ensure that even if the Xerox® Device Agent is uninstalled or upgraded enough information is saved to allow Xerox Support be able to determine the cause of an issue. The diagnostic file is sent to an Azure server over HTTPS and contains install logs, event logs and other errors logs from the Xerox® Device Agent/Bin directory.

RUNNING RECOVERY SERVICES

You can generate a Recovery File of Database and Log files by running a command line utility in the Xerox® Device Agent installation /Bin directory. You must be an administrator to run this utility. By default,

a Recovery File will be generated in a default location and is sent to Xerox.

The following files are uploaded to Xerox in the diagnostic upload:

- Windows Application Event Log
- Discovery Event Log
- Xerox DM (Device Management) Event Log
- Schedule Event Log
- Database Files
- XDA Installer Log

Note:

- Only Xerox Support representatives have access to these diagnostic recovery files.
- Diagnostic recovery files are password protected and transmitted over a secure connection.
- The recovery files are deleted after the problem has been diagnosed.

DISABLING RECOVERY SERVICES AUTOMATIC UPLOAD

To disable the automatic upload of log files add the -c switch to the Xerox Device Agent Service in Service and Applications / Services.

1. Double click **Xerox Device Agent Service** in Service and Applications / Services.
2. Select the **Recovery** tab.
3. Under Command line parameters, replace the "-r" with "-r -c".

Xerox® Services Manager Integration

Note: This section only applies to Xerox® Print Services and Xerox® Partner Print Services.

The application communicates directly to Xerox through the Internet, transferring associated printer and device information through a secure Web services transfer mechanism automatically (Refer to the Security section for more information.) Xerox uses this device information to update device status and meter reads. The data exchange between the application and Xerox is compressed to conserve bandwidth.

The interaction with Xerox® Services Manager can be broken down into the following categories:

- Data exchange as part of the Startup Wizard
  - Registration
  - Site status export
  - Site settings export
  - Device list import
  - Export devices that have been newly discovered
- Daily synchronization operation (the frequency is user-configurable)
  - Device list import
  - Export of devices
  - Site status export

  - Site Settings import
- Remote command checks
- Check for commands on Xerox® Services Manager
  - Process and send results

REGISTRATION

Xerox® Device Agent is required to register with Xerox® Services Manager. This involves a Web service-based transaction in which Xerox® Device Agent sends a unique Xerox® Device Agent install/site identifier and the Xerox® Services Manager registration key. This data packet is negligible (< 2 KB) and is performed only when the Startup Wizard is run to register Xerox® Device Agent with Xerox® Services Manager.

An Operations Center Administrator can remotely change the registration of a Xerox® Device Agent to another account and or chargeback code in Xerox® Services Manager. The Xerox® Device Agents with another Account / chargeback code (CBC). Xerox® Device Agent registrations can be moved between partners within the same Operations Center and even to another Partner Account / CBC in another Operations Center. This function is documented in the Xerox® Services Manager Administrator Guide.

DEVICE LIST IMPORT

At the end of the Startup Wizard and during the synchronize operation, Xerox® Device Agent imports the list of printers from Xerox® Services Manager. This is a simple transaction with the identifiers for all printers. The data packet is approximately <5 KB for 100 devices.

SITE SETTINGS EXPORT

Xerox® Device Agent sends its settings to Xerox® Services Manager at the end of the Startup Wizard and every time the settings are changed by the user. This includes the discovery settings, synchronization and other schedules, SNMP timeout/retry settings, and SNMP community names. The data size is dependent of the discovery setting, i.e. the number of IP addresses and subnets. This settings packet can be up to 5KB or more in size.

SITE SETTINGS IMPORT

Xerox® Device Agent imports the site settings stored on Xerox® Services Manager as part of the synchronize operation. The data size and the data size variability rules are for the most part the same as that for the Site Settings Export. This import data packet also includes alert profiles.

Note: This section only applies to Xerox® Print Services and Xerox® Partner Print Services.
The count of alert profiles can vary, so the size of this packet can be 5 KB or more.

SITE STATUS EXPORT

Xerox® Device Agent sends the site status information to Xerox® Services Manager to indicate its health. This includes the application's database size and the count of devices. The data size is approximately 3 KB.

DEVICE INFORMATION EXPORT

Xerox® Device Agent exports device information to Xerox via Web services. The device information includes device identity information, status information, and usage information. The data packet size is roughly 35 KB per 100 devices.

REMOTE COMMAND CHECK

Note: This section only applies to Xerox® Print Services and Xerox® Partner Print Services.
Periodically, Xerox® Device Agent will query Xerox® Services Manager if there are any remote commands to execute. Remote commands can be requests for status or reboot for example. Complete list of commands is listed in the Security section.

- Data content will be a negligible if there are no commands to execute. If there is a command to execute, then the response information about the Remote Command will be sent to Xerox® Services Manager.
- Data size depends on the command and number of commands. Just for the check, the packet size will be approximately 2 KB. For example, a troubleshoot device command will result in a response with a transmission size of approximately 9 KB.
- If an Upgrade Device command is queued, Xerox® Device Agent will also retrieve the firmware file from Xerox® Services Manager. Firmware files can be more than 100 MB.
- Default frequency for the command check is once per minute.

AUTO UPDATE

Xerox® Device Agent supports automatic update. When a newer version of Xerox® Device Agent is released, it is loaded on the Auto Update Server available for Xerox® Device Agent to connect to.

There are two actions that utilize network resources to accomplish the Xerox® Device Agent Auto Update function. The two actions include:

- Checking to determine if a newer version of Xerox® Device Agent is available for download.
- Downloading a newer version of Xerox® Device Agent for installation.

Xerox® Device Agent makes changes only on the PC on which it is installed; it does not require network resources like SQL server during the update.

Note: If enabled, automatic updates will also check for CloudFM updates.

Version Check

When Xerox® Device Agent queries the Auto Upgrade Server to determine if a newer version of Xerox® Device Agent is available for download, ~4.2 K of network traffic is generated. This check is performed once a week at the day and time configured in Xerox® Device Agent.

Summary: Monthly total network impact: ~16.8K. Add 4.2K for every time update check is initiated manually.

Update Download

When a newer version of the application is available for download, a composite package of download manager, application installer, and supporting files totaling approximately 30 MB is downloaded to the client machine where the application is currently installed. By default, the auto-upgrade setting is Automatic. Once the download is complete, all installation work is done on the client, and no additional network traffic is generated.

When a Xerox® Workplace Cloud Fleet Management has been licensed and linked to an Xerox® Services Manager account, the Xerox® Device Agent will download files approximately 50 MB in size and install to the client machine in the application directory. This download will only take place if Xerox® Workplace Cloud Fleet Management has been licensed for the associated account and chargeback code.