Focus On Security
Xerox Remote Services Security White Paper

Table of Contents

February 18, 2009

Xerox Engineering Services

Xerox Corporation

A Proactive And Innovative Strategy

Introduction

NOTE: This document refers to Remote Services as a collection of tools used on various Xerox products. The features and information contained in this document refer to the Production Remote Services, prInteract and SMart eSolutions tools.

Xerox is responsive to the security concerns of our customers. Xerox Remote Services are designed to avoid making networks more susceptible to viruses. Remote Services transactions always originate from the device, based on authorizations made by the customer. Remote Services can only communicate with a secure server at Xerox that conforms to the stringent requirements of the internal Xerox Corporation information management infrastructure. Customers do not need to make any changes to Internet firewalls, proxy servers, or other security infrastructure.

Xerox systems are designed to integrate within customer workflows. They connect to the network and push machine data to Xerox Communication servers where the information can be reviewed and analyzed to be used to evaluate service issues as well as to automate billing and supplies replenishment. This built-in knowledge-sharing feature of Xerox systems is what makes Xerox Remote Services viable and its approach unique.

"Transmitting machine data translates to more productivity and less customer attention required."

Xerox Remote Services helps differentiate Xerox machine performance and support from other equipment suppliers. While other vendors may remotely monitor some of their machines, Xerox has developed integrated systems and remote tools, and coupled them with highly skilled Xerox support teams who are tasked with working to make Xerox customers more productive and satisfied. This combination creates a high value Remote Services capability that provides proactive problem resolution, and a robust underlying knowledge of the customer's needs.

A key enabler for creating these support processes is the ability to transmit machine performance data back to the Xerox infrastructure.

The Results Are Tangible

- Transmitting machine data translates to faster preventative maintenance, predicts machine failure and reduces the cycle time to fix problems.
- A multitude of engineering tools leverage data to monitor your machine's health and performance, diagnose problems and recommend corrective actions to your service and support team.
- Active remote monitoring enhances customer experience by using your machine's data to understand your environment and set thresholds and action plans to accommodate your production needs.
- Automated Meter Reading can save customer time as well as insuring accuracy over manually retrieving billing information.
- Automated Supplies Replenishment can allow for ordering of supplies when needed without customer interaction.
- On certain models, automatic downloading of software patches is supported to fix problems and add features.
- The expertise of hundreds of Xerox engineers is available.

The Purpose Of This White Paper

The goal of this document is to ensure that Xerox customers understand and feel confident that Remote Services are performed and machine data is transmitted to Xerox in a secure and accurate manner. This White Paper provides additional background on Remote Services capabilities, and specifically focuses on the security aspects of Xerox Remote Services.

It is recommended that you read the document in its entirety and take appropriate actions consistent with your information technology security policies and practices. It is also important that you maintain the integrity of any security measures taken. Each customer has many issues to consider as it develops and deploys a security policy within its organization. Since these requirements will vary from customer to customer, the customer has the final responsibility for any and all implementations, re-installations, testing of security configurations, patches, and modifications.

Remote Services Overview

Increasingly, Xerox products implement services that communicate back to Xerox. Xerox Remote Services capabilities are based on a technology platform that provides a flexible end-to-end system for connecting products to our post-sale solutions offerings.

There are two main architectural elements of the Remote Services system. These two elements work together in a seamless manner to enable a extensive set of services and to provide for additional services to be added in the future. These elements are:

"On certain models, automatic downloading of software patches is supported to fix problems and add features."

Remote Services Client software This is a software module embedded in Xerox products or installed in the customer's environment to provide the client-side infrastructure that enables secure transactions back to Xerox.

Xerox Communication Server a common connectivity server to which the client software transmits system data.

Remote Services Design Goals

Xerox views security as a key requirement of the overall Remote Services architecture. The security related goals were derived from the following sources:

- Inputs and feedback from extensive Voice of the Customer continuing studies conducted by the Xerox Innovation Group (XIG). These studies are focused on determining customer preferences and their remote services needs.
- Xerox Customer Service and Support Organizations across the world.
- Security guidelines published by the Xerox Information Management (XIM) organization.

Xerox Remote Services include capabilities designed to address the following concerns about security:

Identification and Authentication. The process of uniquely and reliably identifying a device.

Authorization The process of granting the device remote access services based on our customer's security needs and product acquisition decisions.

Data Integrity The ability to verify that data has not been subjected to unauthorized modification.

Audit Capabilities The ability to track all communication between a machine and Xerox.

Customer Confidentiality The prevention of access to unauthorized parties by making use of encryption techniques (i.e. https).

"The Remote Services Client allows a secure connection from the device to Xerox"

Within the end-to-end Remote Services system, the system design goals respond to network security concerns in two main catergories.

Customer Network Category

The first category is security concerns related to the connection of the client software to the end-user's network and to the transmission of data across the Internet to Xerox. Xerox Remote Services incorporate the following controls:

- The customer must authorize communications between the device and Xerox.
- Communications from the device shall not include Personally Identifiable Information (PII) **unless** authorized by the customer.
- The transmission of job data is **not** possible without express independent permission and initiation by the customer (approval to send diagnostic, supplies usage, and billing data is separate from approval to send job data).
- Job data is separately encrypted and is not generally available to the back-end systems or personnel which are not specifically designated.
- The **Remote Services Client Software** allows a secure connection from the device to Xerox. It is not possible to use this connection to access the customer's network or data beyond what is pushed to Xerox by the customer.
- The integrity and authentication of any information (data or code) downloaded from the Communications Server to the device by the **Remote Services Client** is verified prior to installation.

Transaction Security

The second category is the network security concerns related to the exchange of information between the customer and Xerox in executing transactions. The following controls have been established:

- The Xerox Communication Server and the Remote Services Clients mutually identify and authenticate themselves to each other.
- All transactions uploaded by the Remote Services Client to the Xerox Communication Server is able to be audited through the device transaction history log by both the customer and Xerox. A transaction log can be viewed which gives service personnel and privileged users the ability to audit the information shared with Xerox.

Remote Services Architecture

A high-level view of the end-to-end Remote Services architecture would involve communication flow between the Remote Services Client (direct-device and/or proxy-host) and the Xerox Communication Server. Remote Services Clients are embedded either in Xerox devices or in a hosted application (e.g. CentreWare™ Web). The clients are configured to connect with and send messages specifically to the Xerox Communication Server.

Xerox Remote Services use industry standard web services protocols for all communications between Remote Services Clients and the Xerox Communication Server. Web services are accessed via the secured-socket HTTP (HTTPS/SSL) that is common to web browsers and web servers. Use of web services as the underlying mechanism for all Remote Services transactions ensures both interoperability and compatibility with firewalls.

By using HTTP, web services can also take advantage of the Secure Socket Layer (SSL) protocol for security and HTTPS connection management capabilities in order to prevent customer data from being broadcasted over the open Internet.

A proxy server is commonly used in network environments to provide a firewall system between the end-user network and the Internet. Most firewalls/proxies are configured to block requests on all but a few network ports. Firewalls, however, usually allow traffic on port 80 for HTTP and 443 (secured HTTP or HTTPS) so browsers can access the Internet. By using HTTP or HTTPS over standard ports, Remote Services Clients are able to communicate through firewalls. The Remote Services Clients act like any web browser (over standard ports) requiring no "holes in the customer firewall" or changes to other equipment at the customer site. Remote Services Clients support the 128 bit SSL encryption.

"All transaction content between the Remote Services Client and the Xerox Communication Server is auditable through the device transaction history log"

Customers initiate all interactions between their environment and the Xerox Communication Server. Remote Services Client Software may initiate an interaction with the Xerox Communication Server upon the occurrence of an event (e.g. a customer presses a button on the machine UI, a timer triggers an alarm, etc).

To achieve the effect of two-way connectivity the Remote Services Client Software periodically "checks-in" with the Xerox Communication Server to receive any "instructions" for them. This check is infrequent and very lightweight, avoiding congestion of the customer intranet.

Xerox digitally signs all packages downloaded by the Remote Services Client. The customer benefits from this software integrity because it addresses the following issues:

- **Content Source**: this feature certifies that the packages really come from Xerox.
- **Content Integrity**: this feature confirms that the packages have not been altered or corrupted since they were signed.

Remote Services Frequently Asked Questions (FAQs)

Listed below is a set of FAQs helpful for customers using Xerox Remote Services

1. Will enabling Xerox Remote Services Client Software make my network more susceptible to viruses or hacker attacks?

No. Customers make no changes to their own security infrastructure. Xerox Remote Services only communicate to a specific secure server at Xerox and services are designed specifically to prevent unauthorized data transfers. The secure server at Xerox is regularly scanned for viruses using the latest tools.

2. How do I know that Xerox is not accessing my company's private data off the machine disk?

You may examine the log of what is sent back to Xerox by using the device User Interface. Remote Services features only access machine related data and not customer job images or other customer data. Customer job data can only be sent to Xerox when an authorized user is logged in.

3. How can I be sure that the device data is going to Xerox only?

The secure transmittal process uses HTTPS and VeriSign signed certificates to ensure and verify that the device is sending to Xerox. In addition, all transmission data is sent over a Secure Socket Layer (SSL) connection using 128-bit encryption. Initial configuration of the Client Software "points" to only the Xerox Communication Server.

4. Will my machine interact with or receive information from "non-Xerox" systems?

No. The device always initiates the remote services transfer activity and sets up a Xerox-only, non-intrusive communication path.

5. What is the data used for?

Currently this data is used for one of three purposes:

- **Service** – Service information is collected and sent to allow service personnel to view the state of the device before traveling to the customer site. This saves the customer time by reducing the need to make extra trips to the customer site.
- **Engineering** – Detailed engineering logs allow timely response to critical customer problems and provide valuable feedback for future features.
- **Billing** – Billing information is sent with each data push allowing Xerox to produce accurate customer bills.
- **Supplies** - Consumable information is sent with each data push allowing Xerox to send consumables (toner) when needed.
- **Parts** - Customer Replaceable Unit (CRU) information is sent with each data push allowing Xerox to ship these to customers when needed.

Remote Services Data

The table below details the types and formats of data contained in Remote Services transfers.

File	Format	Description
Billing	XML	Customer Billing Meters
Status	XML	Messages displayed to the operator
Customer Info	XML	Customer contact information
DFE Errors	XML	Errors recorded by the DFE
Diagnostic List	XML	Record of diagnostic procedures performed
Faults	XML	List of faults
Configuration	XML	Configuration of the machine
Events	XML	List of informational events
Diagnostic Data	XML	A set of diagnostic data files
NVM	XML	Systems settings for Image Quality etc.
Engineering	Free Form	Engineering debug information
Supplies Usage	XML	Toner / Ink Usage Levels