Security Guide

Xerox® Instant Print Kiosk

Document Version: 1.0 (September 2019).

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

Table of Contents

This document describes the locations, capacities and contents of volatile and non-volatile memory devices within the Xerox® Instant Print Kiosk.

Purpose

The purpose of this document is to disclose information for the Xerox® VersaLink® Multifunction devices and printers (hereinafter called as “the product” or “the system”) with respect to product security. Product Security, for this paper, is defined as how image data is stored and transmitted, how the product behaves in a network environment, and how the product may be accessed both locally and remotely. The purpose of this document is to inform Xerox customers of the design, functions, and features of the product with respect to Information Assurance. This document does not provide tutorial level information about security, connectivity, or the product’s features and functions. This information is readily available elsewhere. We assume that the reader has a working knowledge of these types of topics.

Target Audience

The target audience for this document is Xerox field personnel and customers concerned with IT security.

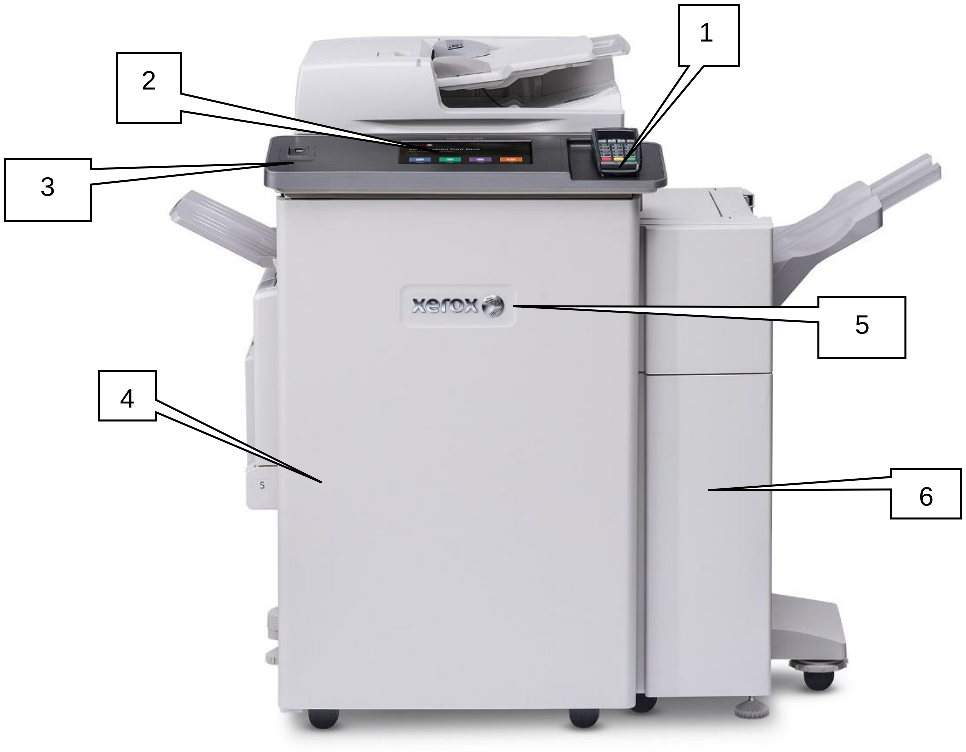
Disclaimer

The content of this document is provided for information purposes only. Performance of the products referenced herein is exclusively subject to the applicable Xerox Corporation terms and conditions of sale and/or lease. Nothing stated in this document constitutes the establishment of any additional agreement or binding obligations between Xerox Corporation and any third party.

1. Product Description

Physical Components

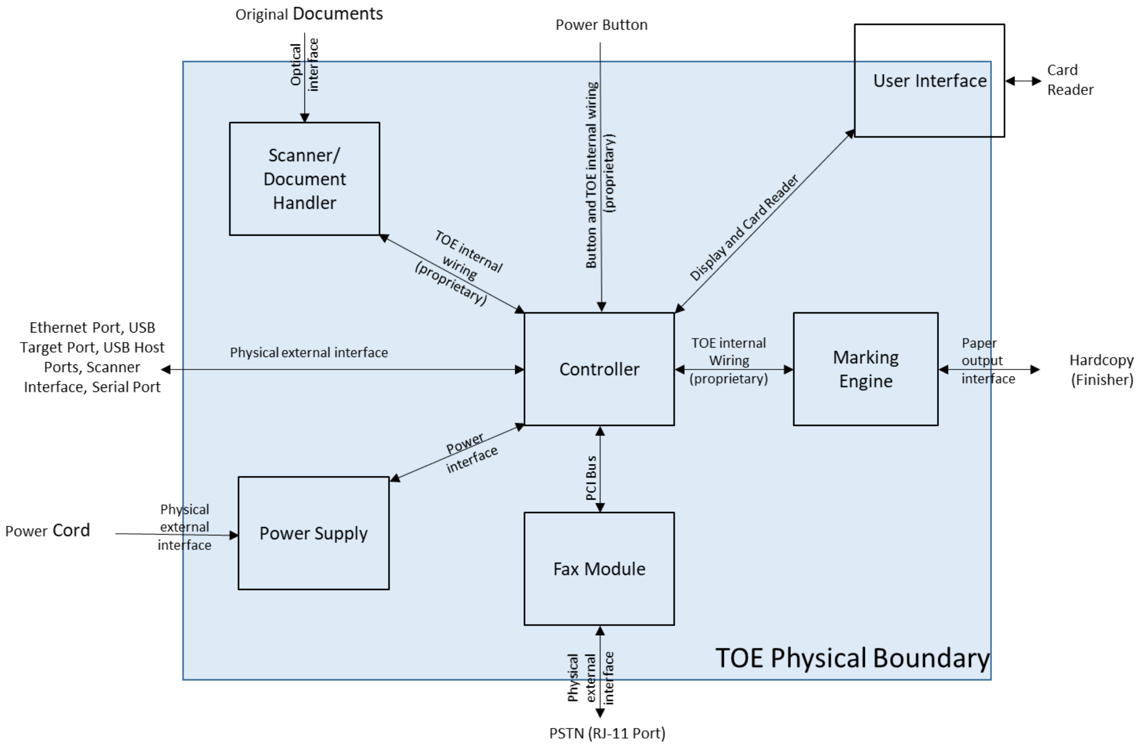
The product consists of an input document handler and scanner, marking engine, controller, and user interface. A PCI-DSS approved credit card reader is used for payment processing. A typical configuration is depicted below. Please note that options including finishers, paper trays, document handers, etc. may vary configuration, however, they are not relevant to security and are not discussed.



1. **Card Reader.**
2. **Graphical User Interface (GUI)**
3. **Front Panel USB Port***
4. **Paper Trays**
5. **Marking Engine (IOT)**
6. **LX Finisher**

Architecture

The security-relevant subsystems of the product are partitioned as shown below:


Original Documents
Optical interface
Power Button
User Interface
Card Reader
Scanner/ Document Handler
Button and TOE internal wiring (proprietary)
Display and Card Reader
TOE internal wiring (proprietary)
Ethernet Port, USB Target Port, USB Host Ports, Scanner Interface, Serial Port
Physical external interface
Controller
TOE internal Wiring (proprietary)
Marking Engine
Paper output interface
Hardcopy (Finisher)
Power interface
PCI Bus
Power Cord
Physical external interface
Power Supply
Fax Module
TOE Physical Boundary
Physical external interface
PSTN (RJ-11 Port)

Controller

The kiosk provides both network and direct-connect external interfaces and enables copy, print, email, scan and cloud fax functionality. The controller contains the image path, which uses proprietary hardware and algorithms to process the scanned images into high-quality reproductions. Scanned images may be temporarily buffered in DRAM to enable electronic pre-collation, sometimes referred to as scan-once/print-many. When producing multiple copies of a document, the scanned image is processed and buffered in the DRAM in a proprietary format. Extended buffer space for very large documents is provided on disk media. The buffered bitmaps are then read from DRAM and sent to the Image Output Terminal (IOT) for marking on hardcopy output. Image Overwrite, which is included as a standard feature, enables both Immediate and On-Demand overwrite of any temporary image data created on disk.

The controller works with the Graphical User Interface (GUI) assembly to provide system configuration functions. A System Administrator has the ability to access these functions.

Memory Components

Volatile Memory

All volatile memory listed is cleared after power is removed (decay occurs generally within 20 seconds at room temperature). All volatile memory listed is required for normal system operation and during service and diagnostic procedures.

Removal of any volatile memory will void the warranty.

Non-Volatile Memory

All non-volatile memory listed is required for normal system operation and during service and diagnostic procedures. Non-volatile memory in the system cannot be accessed by accidental keystrokes.

Removal of any non-volatile memory will void the warranty.

Volatile Memory for the MFD

Type (SRAM, DRAM, etc.)	Size	User Modifiable (Y/N)	Function or Use	Process to Clear:
DDR3 SDRAM non ECC – System Memory	4GB	N	Executable code, Printer control data, temporary storage of job data	Power Off System

Additional Information: There is one main block of Volatile memory in the controller and that is the System memory. System memory contains a mixture of executable code, control data and job data. Job data exists in System memory while the job is being processed. Once the job is complete, the memory is reused for the next job.

Non-Volatile Memory for the MFD

Type (SRAM, DRAM, etc.)	Size	User Modifiable (Y/N)	Function or Use	Process to Clear:
SEEPROM	256bytes	Via Diagnostics	Serial Presence Detect Config (for 4Gb DDR3 system memory)	NA
Flash	8MB	Via Diagnostic	BIOS Flash – Contains BIOS code for processor	NA
Flash	8MB	Via Diagnostic	Boot Flash – Contains Ethernet config settings and MAC address	NA
Battery Backed SRAM	242bytes	Via Diagnostic	Stores and maintains Time and Date	NA
SEEPROM	8Mb	Via Diagnostics	Programs Balinese FPGA	NA

Additional Information: All memory listed above contains code for execution and configuration information. No user or job data is stored in these locations.

Non-Volatile Hard Disk Memory for the MFD

Type (SRAM, DRAM, etc.)	Size	User Modifiable (Y/N)	Function or Use	Process to Clear:
System Disk / System partition	No	24GB	N with normal operation	Operating System, Fonts, configuration file storage.
System Disk / Image partition	No	24GB	N with normal operation	Job Images

Additional Information: The System disk contains the Linux Operating System and stores executables, fonts, and settings files. During normal operation, job files do not remain stored on this disk. One exception is "Print From" "Saved Jobs" feature. Customer jobs saved on the machine's hard disk using this feature must be manually deleted by the customer. If full On Demand Overwrite is selected all saved jobs will be erased.

The Image partition stores images in a proprietary encoded format in non-contiguous blocks. Customer image data is only stored to the image partition if EPC memory is full. User data and image data may be completely erased with a full Overwrite using a three-pass algorithm which conforms to U.S. Department of NIST Special Publication 800-88 Rev1, and the entire image partition is erased and checked.

RFID Devices

No RFD devices are contained in this device.

Media and Storage Descriptions

There are no disk drives, tape drives, CF/SD/XD memory cards, etc. in this device.

Marking Engine Module Volatile Memory

Type (SRAM, DRAM, etc.)	Size	User Modifiable (Y/N)	Function or Use	Process to Clear:
DRAM (MCU PWBA)	32M x 16 bit	N	Temporary Storage of variables	Power Off System
RAM (UI PWBA)	1kbyte	N	Temporary Storage of variables	Power Off System

Marking Engine Module Non-Volatile Solid State Memory

Type (SRAM, DRAM, etc.)	Size	User Modifiable (Y/N)	Function or Use	Process to Clear:
Flash (MCU PWBA)	16Mbit	N	Permanent storage of program. User image data are not stored.	Not customer alterable.
EEPROM (LED Driver, PWBA, K)	128Kbit	N	Permanent storage of setup data.	Not customer alterable.
EEPROM (MM PWBA)	128Kbit	N	Permanent storage of parameters and setup data. User image data are not stored.	Not customer alterable.
EEPROM (UI PWBA)	1kbit x 2	N	Permanent storage of setup data. Storage of UI error log data	Not customer alterable.
EEPROM (DADF PWBA) LOW (PF2.01) or HIGH(PF2.02)	16Kbit	N	Permanent storage of DADF configuration code. User image data are not stored.	Not customer alterable.
EEPROM (TM PWBA)	2kbit	N	Permanent storage of TM configuration code. User image data are not stored.	Not customer alterable.
Flash or ROM (UI PWBA)	32kbyte	N	Permanent storage of UI executable code. User image data are not stored.	Not customer alterable.
ROM (DADF PWBA) LOW (PF2.01) or HIGH(PF2.02)	256kbit	N	Permanent storage of DADH configuration code. User image data are not stored.	Not customer alterable.
EEPROM (IIT)	16Kbit	N	Permanent storage of setup data	Not customer alterable

Feeder and Finisher Modules

All memory inside the feeder/finisher devices listed below is used for configuration settings and normal operation. Removal of any memory will void the warranty. Access to any memory is by system programs or diagnostics only. This document lists the available options. Depending on the configuration purchased, your system will contain on or more of these devices. NOTE: None of these devices stores any job data or Personally Identifiable Information in electronic form.

Feeder Modules

High Capacity Tandem Tray Module

Finisher Modules

Office Finisher LX

Scanner

The purpose of the scanner is to provide mechanical transport to convert hardcopy originals to electronic data. The scanner converts the image from hardcopy to electronic data. A document handler moves originals into a position to be scanned. The scanner provides enough image processing for signal conditioning and formatting. The scanner does not store scanned images.

Graphical User Interface (GUI)

The GUI detects soft button actuations and provides text and graphical prompts to the user. Images are captured by the GUI and submitted to the final destination (scan location or marking engine) but are not stored in the GUI. The GUI also displays screens for service and diagnostic purposes.

Graphic User Interface Module Volatile Memory

Type (SRAM, DRAM, etc.)	Size	User Modifiable (Y/N)	Function or Use	Process to Clear:
RAM	2 GB	N	Executable code, logs, temporary storage of job data	End of session

Additional Information: Job data exists while the job is being processed. Once the job is complete, the memory is reused for the next job.

Graphic User Interface Module Non-Volatile Memory

Type (Flash, EEPROM, etc.)	Size	User Modifiable (Y/N)	Function or Use	Process to Clear:
Flash	16MB	N	Executable code, configuration	NA

Additional Information: No user or job data is stored in these locations.

External Connections

An SD card slot is located beneath the GUI for software upgrades and collecting logs. This location is protected by a locked, metal plate and so it is not customer accessible.

Credit / Debit Card Terminal

The Instant Print Kiosk includes a PCI-DSS approved PIN Transaction Security device. PIN Transaction Security (PTS) devices are used by a merchant at the point-of-interaction for capturing payment card data and validating approval of its use for a transaction. The PCI Council validates the conformance of PTS devices to the PCI PTS standard and provides a list of approved devices.

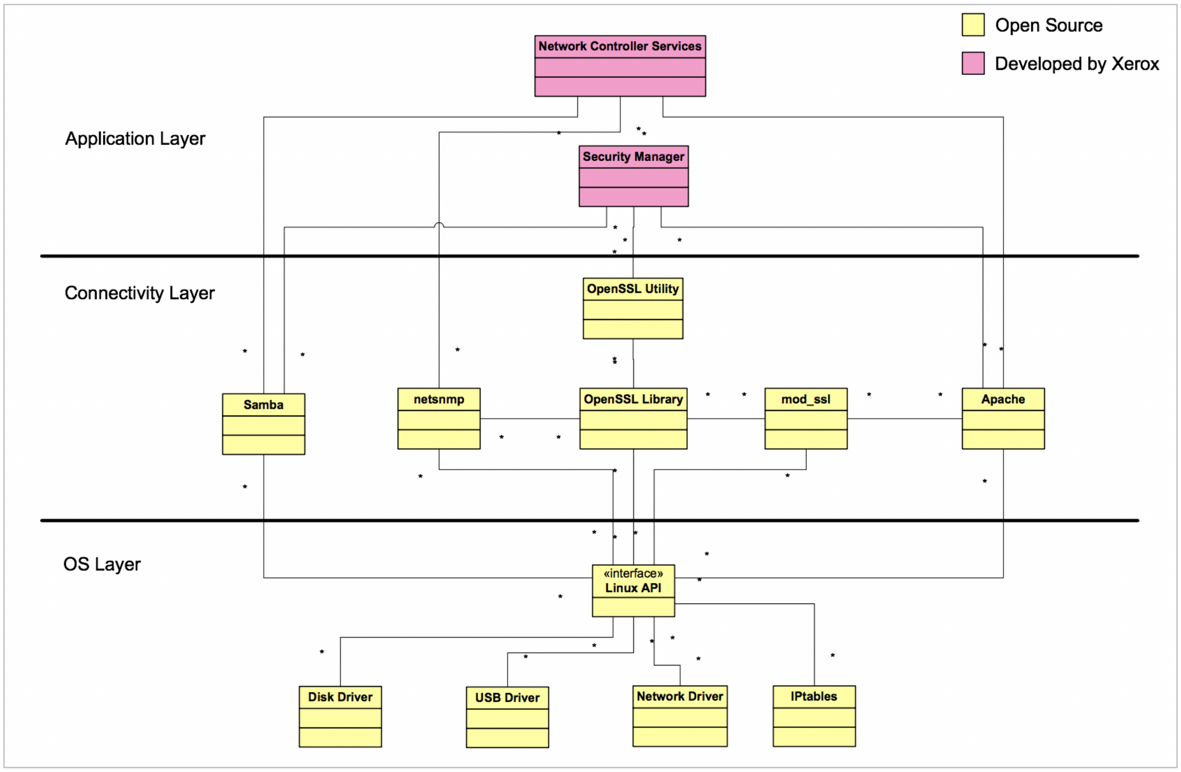
Marking Engine (Image Output Terminal or IOT)

The Marking Engine performs copy/print paper feeding and transport, image marking and fusing, and document finishing. Images are not stored at any point in these subsystems. The marking engine is comprised of paper supply trays and feeders, paper transport, LED scanner, xerographics, and paper output and finishing. The marking engine contains a CPU, BIOS, RAM and Non-Volatile Memory.

System Software Structure

Operating System Layer in the Controller

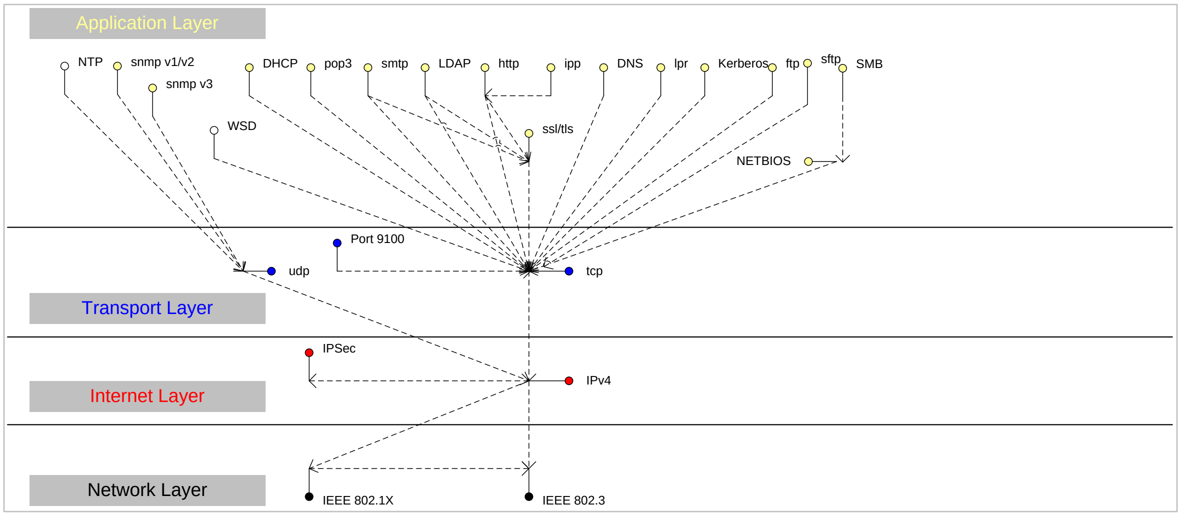
The OS layer includes the operating system, network and physical I/O drivers. IP Filtering is provided by the kernel.



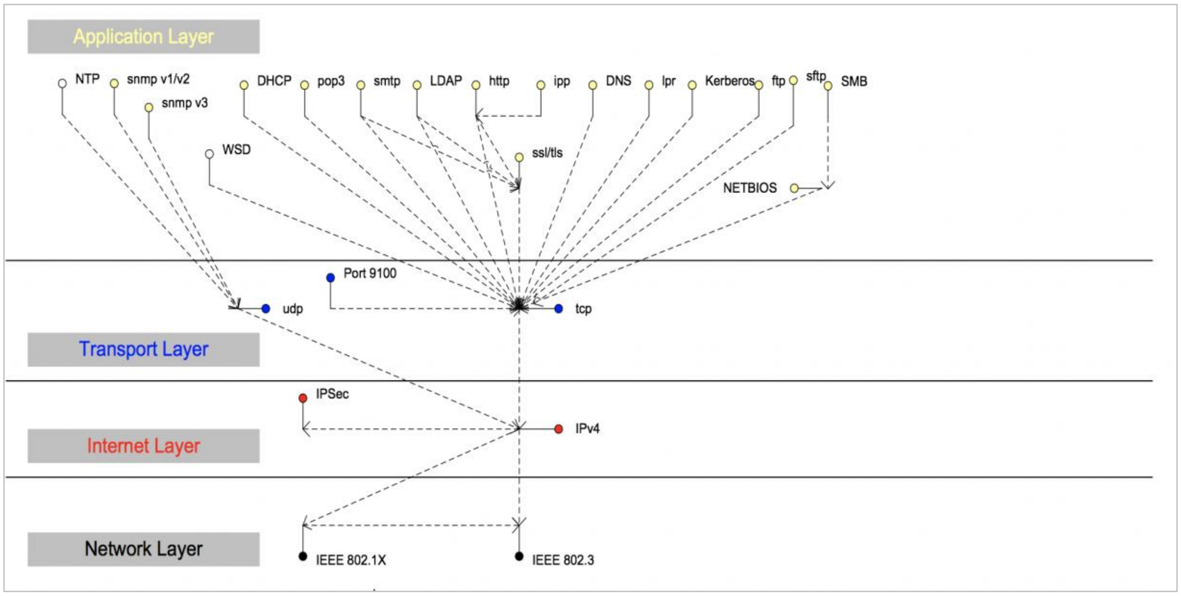
Network Protocols

The network context of the system is illustrated in the diagram below:

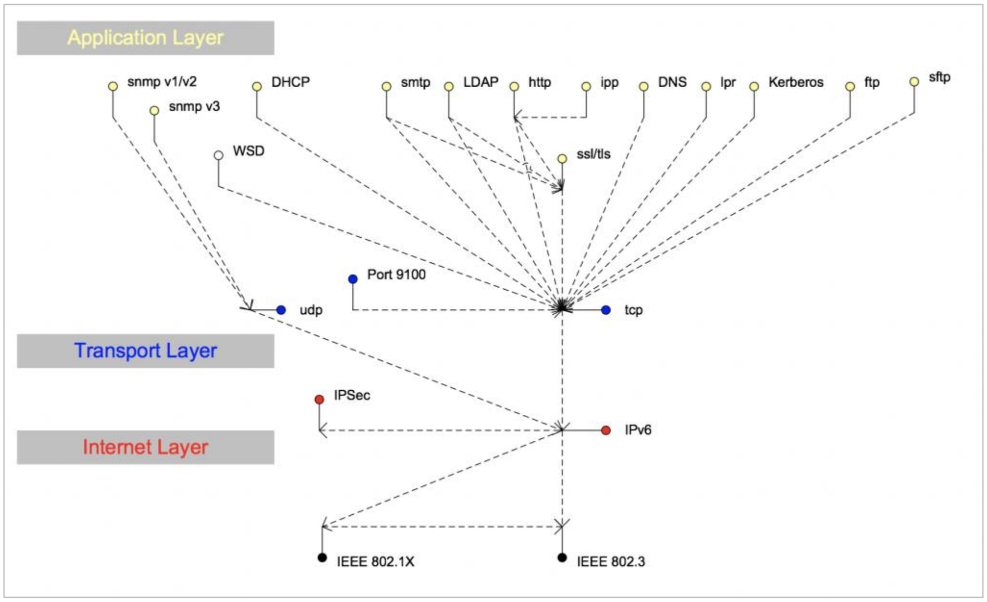
Interface diagrams depicting the IPv4 and IPv6 protocol stacks supported by the device, annotated according to the DARPA model.



Network Protocol Stack



IPv6 Network Protocol Stack



Logical Access Network Security

A variety of network protocols are supported. There are no ‘Xerox unique’ additions to these protocols.

IPSec

The device supports IPSec tunnel and transport mode. The print channel can be secured by establishing an IPSec association between a client and the device. A shared secret is used to encrypt the traffic flowing through a tunnel.

802.1x

IEEE 802.1X is a security standard for port based network access control. It secures Ethernet and/or Wi-Fi networks against unauthorized access by requiring device authentication with a central server before network access and data transmissions are allowed.

IP Filtering

The devices contain a static host-based firewall that provides the ability to prevent unauthorized network access based on IP address and/or port number. Filtering rules can be set by the SA using the WebUI. An authorized SA can create rules to (Accept / Reject / Drop) for ALL or a range of IP addresses. In addition to specifying IP addresses to filter, an authorized SA can enable/disable all traffic over a specified transport layer port

Logical Access Ports

The device has no exposed services.

2. System Access

Kiosk Configuration and Management

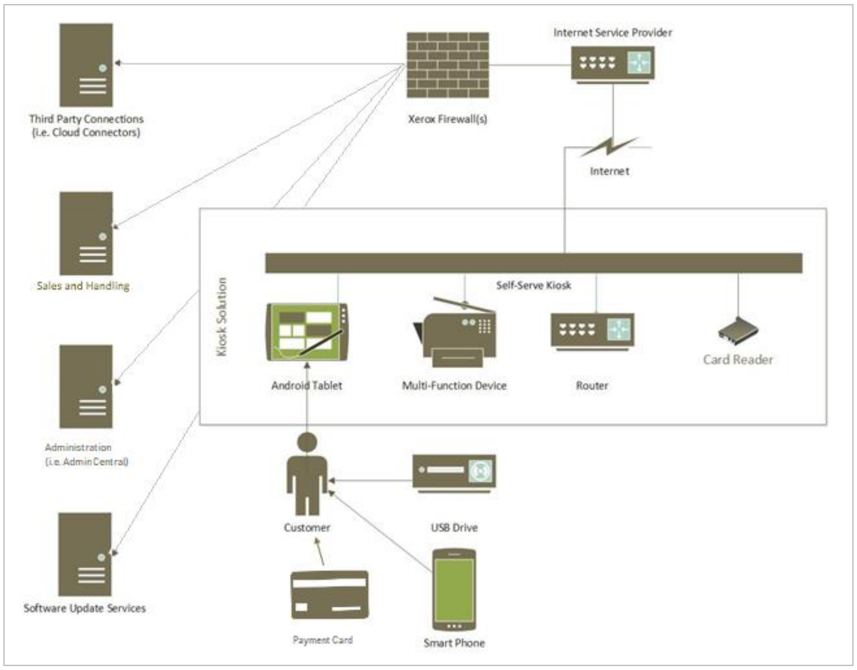
The Kiosk includes three built in accounts. The tables below describe the accounts and their access rights.

Role	Description
Administrator	Used by site administrators for software upgrades and to view all software version information in addition to Associate tasks.
Associate	Used by site staff members to help with normal operational issues.
Xerox CSE	Used only by Xerox Customer Service Engineers.

	Administrator	Xerox CSE	Associate
Device Management	X	X	X
Embedded Web Server	X	X	X
View Configuration	X	X	
Software Updates	X	X	
Debug	X	X	X
User Accounts	X		
Continue Bootup		X	
Skip Bootup	X		X

Customer Transaction Processing

The Xerox® Instant Print Kiosk is typically deployed in a public or common area. Consumers approach the device, select the desired services, initiate the transaction, and provide payment using a credit card. The following diagram illustrates the various components and services the device may interact with during a transaction.



Walkup User Workflow

Below is a brief example of a typical transaction:

A customer wishes to print a file from Google Drive:

1. Customer selects Print and then selects the Google Drive option.
2. Customer inserts or swipes a credit card into the card reader. The card reader communicates with the PCI appliance to authorize payment.
3. Customer provides Google signin credentials. The device communicates with Google over HTTPS port 443 to authenticate and receives a token. Once authenticated, the device will display the Google Drive contents.
4. Customer selects the desired file to print and specifies options (paper size, number of copies, finishing, etc). The device communicates with the payment server to calculate total job cost and displays it to the customer.
5. Customer approves the total job cost and the Kiosk prints the customer’s file.

   Once the job completes, the customer chooses to Checkout. The card reader communicates with the PCI appliance which manages tokenization and payment processing.

Note: The card reader is the only component that processes PCI data. All PCI communications are encrypted directly by the card reader and the hosts within the PCI processing infrastructure with which it communicates.

Use of Customer Credentials

Some apps may require the user credentials to login to a server. The instances where the device logs into a server are detailed in the following table:

Feature	Device Behavior
Print from Google Drive; Scan to Google Drive	The user enters personal credentials to access their Google account.
Print from Dropbox, Scan to Dropbox	The user enters personal credentials to access their Dropbox account.
Cloud Fax (XMEDIUS)	The device logs in to the Fax Server with the credentials set up by the system administrator.
Print from Email; Scan to Email	The user enters a code received from the print from email provider for Print from Email; the user enters email address(es) for Scan to Email.
Print from SharePoint; Scan to SharePoint	The user enters personal credentials to access their SharePoint account.
Print from One Drive; Scan to One Drive	The user enters personal credentials to access their One Drive account.

The usernames and passwords are sent over the network encrypted. The credentials are passed through the device to the network but are not stored on the device. The system follows the best security practices of the 3rd party services used. The system provides authentication tokens (rather than sending usernames and passwords).

3. Security Aspects of Selected Features

McAfee Enhanced Security / Integrity Control

Xerox has partnered with industry leader McAfee to include the Enhanced Security feature which uses McAfee Embedded Control. The McAfee agent is included with the device software which enables communication with McAfee tools such as the ePolicy Orchestrator.

The McAfee Enhanced Security features use “whitelisting” technology to protect your Xerox devices from attack. On the Xerox device, there are critical files and directories designated read-only and some designated write-only. If attempts are made to write to a read-only or read from a write-only file or directory, in addition to being prevented, this creates an event which will be recorded in the device Audit Log. Further, if e-mail alerts were configured on the Xerox device, an e-mail would be sent to the configured address with details of the event.

Software upgrades are handled by designating the software upgrade process as a trusted updater. Once the digital signature is verified, the new software is installed and with it, a new whitelist for the new version. The digital signature prevents corrupted files from being installed by verification that the file is genuine Xerox software and has not been modified.

The use of digital signatures and the whitelisting technique, to stop unauthorized reads, writes, and optionally execution, prevents malicious code from harming your device, regardless of where the attack originated.

Audit Log

Device Audit Log

The device maintains a security audit log. This feature is enabled by default and is required if McAfee protection is enabled, but can be disabled by the SA. The audit log is implemented as a circular log containing a maximum of 15000 event entries, meaning that once the maximum number of entries is reached, the log will begin overwriting the earliest entry. Only a device administrator is authorized to download the log from the device. The log may be downloaded on demand over a secure http connection, or transmitted to a remote secure sftp server on demand or via a daily scheduled action. The log may also be retrieved at the LUI into a USB storage device. The log is exported as a tab-delimited file, and then into a compressed (.zip) file format. The log does not clear when it is disabled, and will persist through power cycles and software upgrades.

The audit log can contain personally identifying information (PII) and should be treated appropriately.

Device Protocol Log

The device has the ability to track secure communication session information for IPSec, TLS, SSH and HTTPS. When enabled, these logs are each written to separate files and included in the zipped download file.

Audit Log File Format

When the audit log file is downloaded, the administrator receives a zipped archive which includes the audit log file (and protocol log files if enabled). The naming convention is serial number_date_time_offset from GMT_auditfile.zip.

The following table lists the events that are recorded in the log:

Event ID	Event Description	Entry Data
1	System startup	Device name
2	System shutdown	Device name Device serial number
3	Manual ODIO Standard started	Device name Device serial number
4	Manual ODIO Standard complete	Device name Device serial number Overwrite Status
5	Print job	Job name User Name Completion Status IIO status Accounting User ID Accounting Account ID
6	Network scan job	Job name User Name Completion Status IIO status Accounting User ID Accounting Account ID total-number-net-destination net-destination.
7	Server fax job	Job name User Name Completion Status IIO status Accounting User ID Accounting Account ID Total-fax-recipient-phone-numbers fax-recipient-phone-numbers net-destination.

Event ID	Event Description	Entry Data
8	IFAX	Job name User Name Completion Status IIO status Accounting User ID Accounting Account ID total-number-of-smtp-recipients smtp-recipients
9	Email job	Job name User Name Completion Status IIO status Accounting User ID Accounting Account ID total-number-of-smtp-recipients smtp-recipients
10	Audit Log Disabled	Device name Device serial number
11	Audit Log Enabled	Device name Device serial number
12	Copy	Job name User Name Completion Status IIO status Accounting User ID Accounting Account ID Total-fax-recipient-phone-numbers fax-recipient-phone-numbers
13	Efax	Job name User Name Completion Status IIO status Accounting User ID Accounting Account ID Total-fax-recipient-phone-numbers fax-recipient-phone-numbers

Event ID	Event Description	Entry Data
14	Lan Fax Job	Job name User Name Completion Status IIO status Accounting User ID Accounting Account ID Total-fax-recipient-phone-numbers fax-recipient-phone-numbers
15	Data Encryption enabled	Device name Device serial number
16	Manual ODIO Full started	Device name Device serial number
17	Manual ODIO Full complete	Device name Device serial number Overwrite Status
18	Data Encryption disabled	Device name Device serial number
20	Scan to Mailbox job	Job name or Dir name User Name Completion Status IIO status
21	Delete File/Dir	Job name or Dir name User Name Completion Status IIO status
23	Scan to Home	UserName Device name Device serial number Completion Status (Enabled/Disabled)
24	Scan to Home job	Job name or Dir name User Name Completion Status (Normal/Error) IIO status Accounting User ID-Name Accounting Account ID-Name total-number-net-destination net-destination

Event ID	Event Description	Entry Data
25	Copy store job	Job name or Dir name User Name Completion Status (Normal/Error) IIO status
26	PagePack login	Device name Device serial number Completion Status: Success: (if Passcode is ok) Failed: (if Passcode is not ok) Locked out (if Max Attempts Exceed 5) Time Remaining: Hrs (Remaining for next attempt) Min (Remaining for next attempt)
27	Postscript Passwords	Device name Device serial number StartupMode (enabled/disabled) System Params Password changed Start Job Password changed
29	Network User Login	UsereName Device name Device serial number Completion Status (Success, Failed)
30	SA login	UsereName Device name Device serial number Completion Status (Success or Failed)
31	User Login	UserName Device name Device serial number Completion Status (Success or Failed)
32	Service Login	Service name Device name Device serial number Completion status (Success or Failed).
33	Audit log download	UserName Device name Device Serial Number Completion status (Success or Failed).

Event ID	Event Description	Entry Data
34	IIO feature status	UserName Device name Device serial number IIO Status (enabled or disabled)
35	SA pin changed	UserName Device name Device serial number Completion status
36	Audit log Saved	UserName Device name Device serial number Completion status
37	SSL	UserName Device name Device serial number Completion Status (Enabled/Disabled/Terminated)
38	X509 certificate	UserName Device name Device serial number Completion Status (Created/uploaded/Downloaded).
39	IP sec Enable/Disable/Configure	UserName Device name Device serial number Completion Status (Configured/enabled/disabled/Terminated)
40	SNMPv3	UserName Device name Device serial number Completion Status (Configured/enabled/disabled).
41	IP Filtering Rules	UserName Device name Device serial number Completion Status (Configured/enabled/disabled).

Event ID	Event Description	Entry Data
42	Network Authentication Enable/Disable/Configure	UserName Device name Device serial number Completion Status (Enabled/Disabled)
43	Device clock	UserName Device name Device serial number Completion Status (time changed/date changed)
44	SW upgrade	Device name Device serial number Completion Status (Success, Failed)
45	Cloning	Device name Device serial number Completion Status (Success, Failed)
46	Scan Metadata Validation	Device name Device serial number Completion Status (Metadata Validation Success or Failed)
47	Xerox Secure Access Enable/Disable/Configure	Device name Device serial number Completion status (Configured/enabled/disabled)
48	Service login copy mode	Service name Device name Device serial number Completion Status (Success, Failed)
49	Smartcard (CAC/PIV) access	UserName (if valid Card and Password are entered) Device name Device serial number Process Name
50	Process terminated	Device name Device serial number Process name

Event ID	Event Description	Entry Data
51	ODIO scheduled	Device name Device serial number ODIO type (Full or Standard) Scheduled time ODIO status (Started/Completed/canceled) Completion Status (Success/Failed/Canceled)
53	CPSR Backup	File Name User Name Completion Status (Normal / Error) IIO Status
54	CPSR Restore	File Name User Name Completion Status (Normal / Error) IIO Status
55	SA Tools Access Admin	Device serial number Completion Status (Locked/Unlocked)
57	Session Timer Logout	Device Name Device Serial Number Interface (Web, LUI) User Name (who was logged out) Session IP (if available)
58	Session Timer Interval Change	Device Name Device Serial Number Interface (Web, LUI)(Timer affected by change) User Name (who made this change) Session IP (if available) Completion Status
59	Feature Access Control Enable/Disable/Configure	User Name Device Name Device Serial Number Completion Status (Enabled/Disabled/Configured) Interface (Web, Local, CAC, SNMP) Session IP address (if available)

Event ID	Event Description	Entry Data
60	Device Clock NTP Enable/Disable	Device Name Device serial number Enable/Disable NTP NTP Server IP Address Completion Status (Success/Failed)
61	Grant / Revoke Admin	Device Name Device Serial Number User Name (of target user) Grant or Revoke (the admin right) Completion Status (Success/Failed)
62	Smartcard (CAC/PIV) Enable/Disable/Configure	UserName Device Name Device Serial Number Completion Status (Success/Failed)
63	IPv6 Enable/Disable/Configure	UserName Device Name Device Serial Number Completion Status (Success/Failed)
64	802.1x Enable/Disable/Configure	UserName Device Name Device Serial Number Completion Status (Success/Failed)
65	Abnormal System Termination	Device Name Device Serial Number
66	Local Authentication	UserName Device Name Device Serial Number Completion Status (Enabled/Disabled)
67	Web User Interface Authentication (Enable Network or Local)	UserName Device Name Device Serial Number Authentication Method Enabled (Network/Local)

Event ID	Event Description	Entry Data
68	FIPS Mode Enable/Disable/Configure	UserName Device name Device Serial Number Enable/Disable/Configure
69	Xerox Secure Access Login	UserName Device Name Device Serial Number Completion Status (Success/Failed)
70	Print from USB Enable/Disable	User Name Device Name Device Serial Number Completion Status (Enabled/Disabled)
71	USB Port Enable/Disable	User Name Device Name Device Serial Number USB Port (Front/Rear) Completion Status (Enabled/Disabled)
72	Scan to USB Enable/Disable	User Name Device Name Device Serial Number Completion Status (Enabled/Disabled)
73	System Log Download	Username IP of requesting device (if available) File names downloaded Destination (IP address or USB device) Completion status (Success/failed)
74	Scan to USB Job	Job Name User Name Completion Status IIO Status Accounting User ID-Name Accounting Account ID-Name

Event ID	Event Description	Entry Data
75	Remote UI feature	User Name Device Name Device Serial Number Completion Status (Enabled/Disabled/Configured)
76	Remote UI session	User Name Device Name Device Serial Number Completion Status (Initiated/Terminated) Remote Client IP Address
77	Remote Scan Feature Enable/Disable (TWAIN driver)	User Name Device Name Device Serial Number Competion Status (Enable/Disable)
78	Remote Scan Job Submitted (TWAIN driver)	UserName (at client if available) IP address of submitting client Device name Device serial number Job name (if accepted) Completion status (accept/reject request)
79	Scan to Web Service Job (Remote Scan Job Competed) (TWAIN driver)	Job name UserName Accounting User ID-Name Accounting Account ID-Name Completion status Destination
80	SMTP Connection Encryption	UserName Device name Device serial number Completion Status (Enabled for STARTLS / Enabled for STARTLS if Avail / Enabled for SSL/TLS / Disabled)

Event ID	Event Description	Entry Data
81	Email Domain Filtering Rule	User name Device Name Device Serial Number Completion Status (Feature Enabled/Feature Disabled, Rule Added / Rule Deleted)
82	Software Self Test Started	Device Name Device Serial Number
83	Software Self Test Complete	Device Name Device Serial Number Completion Status(Success/Failed/Cancelled)
84	McAfee Security State NOTE: ColorQube 8900 ONLY	UserName Device name Device serial number Security Mode (Enhanced Security / Integrity Control) Completion Status (Enabled / Disabled / Pending)
85	McAfee Security Event NOTE: ColorQube 8900 ONLY	Device name Device serial number Type (Read / Modify / Execute / Deluge) McAfee message text
87	McAfee Agent NOTE: ColorQube 8900 ONLY	User name Device name Device serial number Completion Status (Enabled / Disabled)
88	Digital Certificate Import Failure	Device name
89	User Name Add/Delete	Device serial number
90	User Name Password Change	Security Mode

Event ID	Event Description	Entry Data
91	EFax Job Secure Print Passcode	UserName (managing passcodes) Device name Device serial number Completion Status (Passcode Created/Changed)
92	Scan2Mailbox Folder Password Change	UserName (managing passwords) Device name Device serial number Folder Name Completion Status (Password was Changed)
93	EFax Mailbox Passcode	UserName (managing passcodes) Device name Device serial number Completion Status (Passcode Created/Changed)
94	FTP/SFTP Filing Passive Mode	User Name Device Name Device Serial Number Completion Status (Enabled / Disabled)
95	EFax Forwarding Rule	User Name Device Name Device Serial Number Fax Line 1 or 2 (if applicable) Completion Status (Rule Edit / Rule Enabled / Rule Disabled)
96	EIP Weblets Allow Install	UserName Device name Device serial number Completion Status (Enable Installation / Block Installation)
97	EIP Weblets Install	UserName Device name Device serial number Weblet Name Action (Install / Delete) Completion (Success / Fail)

Event ID	Event Description	Entry Data
98	EIP Weblets Enable / Disable	UserName Device name Device serial number Weblet Name Completion Status (Enable / Disable)
99	Network Connectivity Enable / Disable	UserName Device name Device serial number Completion Status (Enable Wireless / Disable Wireless (Enable Wired /Disable Wired)
100	Address Book Permissions	UserName Machine Name Machine serial number Completion Status (SA Only/Open Access Enabled WebUI) / (SA Only/Open Access Enabled LocalUI)
101	Address Book Export	UserName Machine Name Machine serial number
102	SW upgrade enable / disable	UserName Device name Device serial number Completion Status (Enable Installation / Disable Installation)
103	Supplies Plan Activation	Device name Device serial number Completion Status: Success: (if Passcode is ok) Failed: (if Passcode is not ok) Locked out (if Max Attempts Exceed 5) Time Remaining : Hrs (Remaining for next attempt) Min (Remaining for next attempt)

Event ID	Event Description	Entry Data
104	Plan Conversion	Device name Device serial number Completion Status: Success: (if Passcode is ok) Failed: (if Passcode is not ok) Locked out (if Max Attempts Exceed 5) Time Remaining : Hrs (Remaining for next attempt) Min (Remaining for next attempt)
105	IPv4 Enable/Disable/Configure	UserName Device name Device serial number Completion Status (Enabled Wireless/Disabled Wireless/ Configured Wireless) (Enabled Wired/Disabled Wired/ Configured Wired)
106	SA PIN Reset	Device serial number Completion Status (Success/Failed)
107	Convenience Authentication Login	UserName Device name Device serial number Completion Status (Success or Failed)
108	Convenience Authentication Enable/Disable/Configure	UserName Device name Device serial number Completion Status (Enabled/Disabled/Configured)
109	Efax Passcode Length	UserName (managing passcodes) Device name Device serial number Completion Status (Passcode Length Changed)

Event ID	Event Description	Entry Data
110	Custom Authentication Login	UserName Device name Device serial number Completion Status (Success or Failed)
111	Custom Authentication Enable/Disable/Configure	UserName Device name Device serial number Completion Status (Enabled/Disabled/Configured)
112	Billing Impression Mode	UserName Device name Device serial number Mode Set to (A4 Mode, A3 Mode Completion Status (Success, Failed Impression data
113	Airprint Enable/Disable/Configure	UserName Device name Device serial number Completion Status (Enabled/Disabled/Configured)
114	Device cloning enable / disable	UserName Device name Device serial number Completion Status Enable / Disable
115	Save for reprint job	UserName Device name Device serial number Completion Status (Standard Access, Open Access, Restricted)

Event ID	Event Description	Entry Data
116	Web UI Access/Configure	UserName Device name Device serial number Completion Status (Standard Access, Open Access, Restricted)
117	System log push to Xerox	Username if authenticated Server destination URL Log identifier string (filename) Completion Status (Success / Failed)
119	Scan to WebDAV Job	Job name User Name Completion Status IIO status Accounting User ID-Name Accounting Account ID-Name WebDAV destination.
120	Mopria Print enable / disable	UserName Device name Device serial number Completion Status Enable / Disable
121	PoS credit card API enable / disable	UserName Device name Device serial number Completion Status Enable / Disable
122	PoS CC data transfer data transfer	Job name or number? Machine Name Machine serial number Destination server Completion status (Success / Fail)

Event ID	Event Description	Entry Data
124	Invalid Login Attempt Lockout	Device name Device serial number Interface (Web UI, Local UI) Session IP Address if available
125	Protocol audit Log enable/Disable	UserName Device Name Device serial number Completion Status Enable / Disable
126	Display Device information configure	UserName Device Name Device serial number Completion Status (Configured)
127	Invalid Login Lockout Expires	Device name Device serial number Interface (Web UI) Session IP Address if available Count of invalid attempts: "attempts xx" where xx = the number of attempts.
128	Erase Customer Data	Erase Customer Data Device serial number Success / Failed
129	Audit log SFTP scheduled Configure	UserName Device Name Device serial number Completion status (Enable/Disable/Configured)
130	Audit Log SFTP Transfer	UserName Device Name Device serial number Destination server Completion Status (File Transmitted)

Event ID	Event Description	Entry Data
131	Remote Software Download Enable Disable	UserName Device name Device serial number Completion Status (Enable/Disable)
132	Airprint & Mopria Scanning Enable/Disable/Configure	UserName Device Name Device serial number Completion Status (Enable/Disable/Configured)
133	Airprint & Mopria Scan Job Submitted	Job name (if accepted) UserName (if available) IP address of submitting client Device name Device serial number Completion status (accept/reject request)
134	Airprint & Mopria Scan Job Completed	Job name UserName (if available) Completion status
136	Remote Services NVM Write	Device Name Device Serial Completion Status (Success-Fail)
137	Remote Services FIK Install	Device Name Device Serial Completion Status (Success-Fail) User-readable names for the features being installed
138	Remote Services Data Push	Device Name Device Serial Completion Status (Success-Fail)
139	Remote Services	User Name, Device Name, Device Serial Status: (“Enabled” / “Disabled”)

Event ID	Event Description	Entry Data
140	Restore enable/disable	User Name Device name Device serial number Completion status Enable / Disable
141	Backup-Restore file downloaded	File Name User Name Interface (WebUI) IP Address of the destination (if applicable) Completion Status (Success or Failed)
142	Backup-Restore restore installed	File Name User name Device name Device IP address Interface (WebUI) Completion Status (Success or Failed)
143	Google Cloud Services	User name Device name Device serial number Completion Status-(Enabled / Disabled / Configured)
144	User or Group Role Assignment	User name Device name Device serial number User or group name (assigned) Role name Action (added/removed)
145	User Permission Role	User name Device name Device serial number Role name Completion status (Created / Deleted / Configured)

Event ID	Event Description	Entry Data
146	Admin Password Policy Configure	User name Device name Device serial number
147	Local user account password policy	User name Device name Device serial number
148	Restricted admin login	User name Device name Device serial number Completion status: “Success” or “Failed”
149	Grant / revoke restricted admin rights	User name (of user making the change) Device name Device serial number User name (of target user) Action: “Grant” or “Revoke”
150	Manual session logout	Device Name Device Serial Number Interface (Web, LUI, CAC) User Name (who was logged out) Session IP (if available)
151	IPP Enable/Disable/Configure	User name Device name Device serial number Completion status: (“Enabled” / “Disabled” / “Configured”)
152	HTTP Proxy Server Enable/Disable/Configure	User name Device name Device serial number Completion status: (“Enabled” / “Disabled” / “Configured”)
153	Remote Services Software Download	Device Name Device Serial number File Name

Event ID	Event Description	Entry Data
154	Restricted Admin Permission Role	User name Device name Device serial number Restricted admin role name Completion status (Created / Deleted / Configured)
155	EIP Weblet Installation Security Policy	User name Device name Device serial number Policy: (“allow installation of encrypted Weblets” / ” allow installation of both encrypted and unencrypted Weblets”
159	Send Engineering Logs on Data Push	User name (if available) Device name Device serial number Current setting (“Enabled” / “Disabled”)

Remote Services

Remote Services provides the ability to transmit data to Xerox to be used for billing and, when contracted, supplies replenishment. It also has the ability to send status information for self-help diagnosis. Remote Services provides the ability for Xerox to remotely update the device with new software, licenses, and internal settings (NVM). Xerox Support may request the device System Administrator to send logging information in order to diagnose a problem. This level of logging information may contain personally identifying information (PII) and should only be authorized by a System Administrator with appropriate authority and consents.

The System Administrator may make configuration changes to Remote Services via the Web UI, including enable/disable participation in Remote Services, permissions for remote updates, and time of day for daily polling to the Xerox Remote Services Datacenter. The device can be set to communicate to the Xerox Datacenter via a proxy server on the customer's network. Proxy server settings may be auto-detected or manually set on the Web UI.

Encryption

Print, copy, fax, scan and any job that needs file conversion are written to the SSD nonvolatile memory. These are deleted at the completion of the job, but there is no provision for immediate image overwrite (IIO) of SSD memory, so to protect user data the data is encrypted before writing to the drive.

The Data Encryption Feature will be available to ensure data is protected for all user / job sensitive data. Read and write accesses to the disk(s) will pass through the encryption subsystem on the way into and out of the disk(s) during all operations. All user / job sensitive data will be encrypted.

User account passwords are encrypted.

Encrypted Partitions

All hard disk partitions that store customer data are encrypted with AES256, which utilizes a FIPS 140-2 certified module and algorithm. Encryption keys are encrypted and stored per current relevant US government standards, specifications and guidelines.

.

4. Software Security

Xerox Approved Apps

Only Apps with valid signature approved by Xerox/Partners are allowed to be installed. The system verifies the validity of the signature from Xerox Corporation (or an approved partner) of apps before allowing them to be installed.

Graphical User Interface Upgrades

Remote Software Upgrade

Software upgrades for the graphical user interface can be accomplished remotely by using Xerox CentreWare Web (CWW). CWW is a cloud based software tool for identifying supported devices and managing user interface updates. When software is available on CWW, the user interface will download the software and install the update. Software that is not digitally signed will not be installed.

Local Software Upgrade

Xerox Customer Service Engineers can perform local upgrades using an SD card slot located beneath the user interface panel (after unlocking the metal plate protecting access to the slot).

Printer Upgrades

Remote Printer Upgrade

The printer firmware upgrades are done automatically via the Remote Configuration Tool (RCT). When firmware is available for that device on RCT, the printer will download the firmware and install the update. Firmware that is not digitally signed will be rejected.

Image Overwrite

The Image Overwrite Security feature provides both Immediate Job Overwrite (IJO) and On-Demand Image Overwrite (ODIO) functions. Immediately before a job is considered complete, IIO will overwrite any temporary files associated with print, network scan, internet fax, network fax, or e-mail jobs that had been created on the controller Hard Disk. The ODIO feature can be executed at any time by the SA and will overwrite the entire document image partitions of the controller Hard disk. Scheduled ODIO may also be configured to run at specific times.

A standard ODIO will overwrite all image data from memory and disks except for Jobs and Folders stored in the Reprint Saved Jobs feature; Jobs stored in the Scan to Mailbox feature (if installed); Fax Dial Directories (if fax card is installed); and Fax Mailbox contents (if fax card is installed). A full ODIO will overwrite all image data from memory and disks as well as the items excluded from a standard ODIO.

Algorithm

The overwrite mechanism for both IJO and ODIO conforms to the NST Special Publication 800-88 Rev1.

The algorithm for the Image Overwrite feature is:

Step 1: Pattern #1 is written to the sectors containing temporary files (IIO) or to the entire spooling area of the disks (ODIO). (hex value 0x35 (ASCII “5”)).

Step 2: Pattern #2 is written to the sectors containing temporary files (IIO) or to the entire spooling area of the disks (ODIO). (hex value 0xCA (ASCII compliment of 5)).

Step 3: Pattern #3 is written to the sectors containing temporary files (IIO) or to the entire spooling area of the disks (ODIO). (hex value 0x97 (ASCII “ú”)).

Step 4: 10% of the overwritten area is sampled to ensure Pattern #3 was properly written. The 10% sampling is accomplished by sampling a random 10% of the overwritten area.

User Behavior

Once enabled at either the Local UI or Web UI, IJO is invoked automatically immediately prior to the completion of a print, network scan, embedded fax, internet fax, network fax, or e-mail job. If IIO completes successfully, status is displayed in the Job Queue. However, if IJO fails, a popup will appear on the Local UI recommending that the user run ODIO, and a failure sheet will be printed.

ODIO may be invoked either from the Local UI in Tools Pathway or from the CentreWare Internet Services Web UI. All device functions will be unavailable until the overwrite is completed.

If enabled, a confirmation sheet will be printed at the conclusion of the ODIO process.

Please note that invocation of ODIO will cause currently processing print jobs to be aborted. However, scan jobs will not be cleaned up properly, and so ODIO might fail. The user should insure that all scan jobs have been completed before invoking ODIO. Please refer to the customer documentation for a description on how failures are logged.

Overwrite Timing

The ODIO overwrite time is dependent on the type of hard disk in the product. The overwrite times are generally less than 20 minutes for a Standard ODIO and 60 minutes for a Full ODIO.

IJO is performed as a background operation, with no user-perceivable reduction in copy, print or scan performance.

Immediate Job Overwrite Completion Reporting

When an Immediate Job Overwrite is performed at the completion of each job, the user may view the Completed Jobs Log at the Local UI. In each job entry there will be an indication if the Job was successfully overwritten or not.

All overwrite actions and completion statuses are logged in Audit Log as well.

On Demand Image Overwrite Completion Reporting

Upon completion, an event is written in the Audit Log of the device. This Log may be downloaded by the “admin” user or any user assigned an admin role. The admin may configure whether or not a Confirmation Report will print through the CentreWare Web Ui on the Properties tab, under Security. The options are On, Errors Only, and Off.

All overwrite actions and completion statuses are logged in Audit Log as well.

FIPS 140-2 Compliance

You can enable the printer to check its current configuration to ensure that transmitted and stored data is encrypted as specified in FIPS 140-2 (Level 1). Once FIPS 140 mode is enabled, you can allow the printer to use a protocol or feature that uses an encryption algorithm that is not FIPS-compliant, but you must acknowledge this in the validation process. If FIPS mode is enabled, when you enable a non-compliant protocol such as SMB, a message appears to remind you that the protocol uses an encryption algorithm that is not FIPS-compliant. NOTE: If you enable FIPS 140-2 mode, it may not be able to communicate with other network devices that use protocols that do not employ FIPS 140-2 validated algorithms.

SNMPv3 allows device settings to be managed remotely using FIPS compliant data encryption. SNMPv3 protects the transactions by:

- Checking the integrity of the data (including the message origin, time stamp, and message stream)
- Encrypting the data [AES-128]
- Verifying administrator authorization [SHA1]

When you enable FIPS 140-2 mode, the printer validates its current configuration by performing the following checks:

- Validates certificates for features where the printer is the server in the client-server relationship. An SSL certificate for HTTPS is an example.
- Validates certificates for features where the printer is the client in the client-server relationship. CA Certificates for LDAP and Xerox Extensible Interface Platform (EIP 2.0) are examples.
- Validates certificates that are installed on the printer, but not used. Certificates for HTTPS, LDAP are examples.
- Checks features and protocols for non-compliant encryption algorithms. For example, SMB use encryption algorithms that are not FIPS 140-2-compliant.
- Validates Minimum Certificate Key Length configuration is FIPS compliant (must be 2048 bit).
- Performs CAC, PIV, and .NET card validation.
- Verifies Digital Signing and Encrypted e-mail is FIPS 140-2 compliant.
- IPSec over IPV6 and IPv4 are FIPS 140-2 compliant.

When validation is complete, information and links display in a table at the bottom of the FIPS 140-2 configuration page of the WebUI.

- Click the appropriate link to disable a non-compliant feature, or protocol.
- Click the appropriate link to replace any non-compliant certificates.
- Click the appropriate link to acknowledge that you allow the printer to use non-compliant features and protocols.

5. Additional Information and Resources

Security @ Xerox

Xerox maintains an evergreen public web page that contains the latest security information pertaining to its products. Please see https://www.xerox.com/security.

Responses to Known Vulnerabilities

Xerox has created a document which details the Xerox Vulnerability Management and Disclosure Policy used in discovery and remediation of vulnerabilities in Xerox software and hardware. It can be downloaded from this page: https://www.xerox.com/information-security/information-security-articles-whitepapers/enus.html

Additional Resources

Below are additional resources.

Security Resource	URL
Frequently Asked Security Questions	https://www.xerox.com/en-us/information-security/frequently-asked-questions
Common Criteria Certified Products	https://security.business.xerox.com/en-us/documents/common-criteria/
Current Software Release Quick Lookup Table	https://www.xerox.com/security
Bulletins, Advisories, and Security Updates	https://www.xerox.com/security
Security News Archive	https://security.business.xerox.com/en-us/news/

6. Appendix A: Abbreviations

API	Application Programming Interface
AMR	Automatic Meter Reads
ASIC	Application-Specific Integrated Circuit. This is a custom integrated circuit that is unique to a specific product.
CAT	Customer Administration Tool
CSE	Customer Service Engineer
DADF/DADH	Duplex Automatic Document Feeder/Handler
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server. A centralized database that maps host names to static IP addresses.
DDNS	Dynamic Domain Name Server. Maps host names to dynamic static IP addresses.
DRAM	Dynamic Random Access Memory
EEPROM	Electrically erasable programmable read only memory
EGP	Exterior Gateway Protocol
GB	Gigabyte
HP	Hewlett-Packard
HTTP	Hypertext transfer protocol
IBM	International Business Machines
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IFAX	Internet Fax
IIO	Immediate Image Overwrite
IIT	Image Input Terminal (the scanner)
IT	Information Technology
IOT	Image Output Terminal (the marking engine)
IP	Internet Protocol
IPSec	Internet Protocol Security
IPX	Internet Protocol Exchange
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LDAP Server	Lightweight Directory Access Protocol Server. Typically the same server that is used for email. It contains information about users such as name, phone number, and email address. It can also include a user's login alias.
LED	Light Emitting Diode

LPR	Line Printer Request
MAC	Media Access Control
MIB	Management Information Base
n/a	not applicable
NDPS	Novell Distributed Print Services
NETBEUI	NETBIOS Extended User Interface
NETBIOS	Network Basic Input/Output System
NOS	Network Operating System
NVRAM	Non-Volatile Random Access Memory
NVM	Non-Volatile Memory
ODIO	On-Demand Image Overwrite
PCL	Printer Control Language
PDL	Page Description Language
PIN	Personal Identification Number
PWBA	Printed Wire Board Assembly
PWS	Common alternative for PSW
RFC	Required Functional Capability
SA	System Administrator
SFTP	Secure File Transfer Protocol
SLP	Service Location Protocol
SNMP	Simple Network Management Protocol
SRAM	Static Random Access Memory
SSDP	Simple Service Discovery Protocol
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TIFF	Tagged Image File Format
UI	User Interface
URL	Uniform Resource Locator
UDP	User Datagram Protocol
WebUI	Web User Interface – the web pages resident in the WorkCentre Pro. These are accessible through any browser using the machine’s IP address as the URL.
XCMI	Xerox Common Management Interface
XSA	Xerox Standard Accounting