Version 1.1

Xerox® AltaLink® B8045/B8055/B8065/B8075/B8090 Multifunction Printer

Document Version: 1.1 (July 2017).

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

1. Introduction

This document describes the locations, capacities and contents of volatile and non-volatile memory devices within the AltaLink® B8045, B8055, B8065, B8075 and B8090 multifunctional printers.

1.1. Purpose

The purpose of this document is to disclose information for the products with respect to device security. Device security, for this paper, is defined as how image data is stored and transmitted, how the product behaves in a networked environment, and how the product may be accessed, both locally and remotely. Please note that the customer is responsible for the security of their network and the AltaLink® products B80xx do not establish security for any network environment.

The purpose of this document is to inform Xerox customers of the design, functions, and features of the AltaLink® B80xx products relative to Information Assurance (IA).

This document does NOT provide tutorial level information about security, connectivity, PDLs, or AltaLink® systems features and functions. This information is readily available elsewhere. We assume that the reader has a working knowledge of these types of topics. Additional information is also available in the AltaLink® B8045/B8055/B8065/B075/B8090 Systems Administrator Guide.

1.2. Target Audience

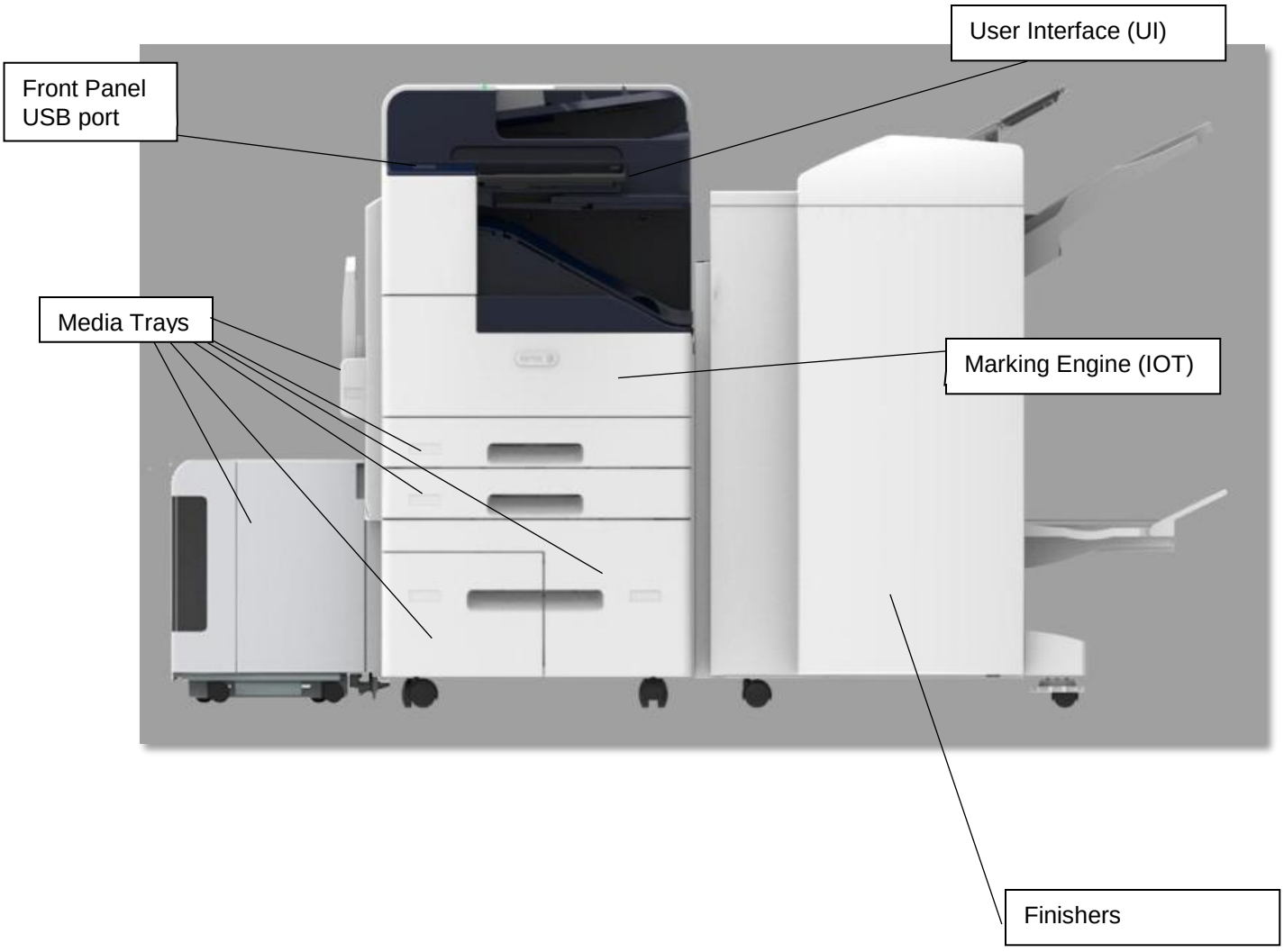
The target audience for this document is Xerox field personnel and customers concerned with IT security.

1.3. Disclaimer

The information in this document is accurate to the best knowledge of the authors, and is provided without warranty of any kind. In no event shall Xerox Corporation be liable for any damages whatsoever resulting from user's use or disregard of the information provided in this document including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Xerox Corporation has been advised of the possibility of such damages.

2. Device Description

This product consists of an input document handler and scanner, marking engine including paper path, controller, finishing device, optional fax, keyboard, card readers and user interface.



USB Port(s)	
USB port and location	**Purpose**
Front panel – 1 Host port	User retrieves print ready files from Flash Media or stores scanned files on Flash Media. Physical security of this information is the responsibility of the user or operator. Upload of software upgrades, download of network logs, download and upload of machine settings for setup cloning.
Rear panel – 2 Host ports	User retrieves print ready files from Flash Media or stores scanned files on Flash Media. Physical security of this information is the responsibility of the user or operator. Upload of software upgrades, download of network logs, download and upload of machine settings for setup cloning. Optional security devices, such as a CAC reader, and /or keyboard communicate with the machine via this port. No job data is transmitted across this interface when an optional security device is connected.
Rear panel – 1 Target port	User PC direct connection for printing, Xerox Customer Service Engineer PWS connection for problem diagnosis. The optional Copy Assistant kit communicates with the machine via this port. No job data is transmitted across this interface.
Additional Information A number of devices can be connected to the 3 USB Host ports. Once information has been copied (either as a back-up data set or as a transfer medium, physical security of this information is the responsibility of the user or operator.)	

Ethernet Port(s)	
Fax port and location	**Purpose**
Rear panel – 1 port RJ45	Connection to the internet
Wi Fi dongle via USB on the rear panel	Connection to Wi-Fi networks

FAX Port(s)	
Fax port and location	**Purpose**
Rear panel – 1 port RJ11	Transmission and receiving of fax jobs
Rear panel – 1 port RJ11	Transmission and receiving of fax jobs

Configuration Overview

45/55

65/75/90

Document Input:

200 Sheet SPDH

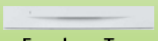
Paper Input:

2X 500 Sheet A3/ Ledger Trays, 100 Sheet Bypass

Trays 3&4 (2000/1600 A4/Ltr)

May Choose:

Tray Lock Kit



Envelope Tray

45-90ppm PFP (optional: PFP oversize media kit and PFP SEF media kit for 65..90ppm)

Output:

Must Choose:

OCT (45 to 75ppm) or Finisher Transport (45 to 90ppm)

May Choose

Pro Finisher
May choose for 65-75 ppm
Must choose for 90ppm

45-75ppm Office Finisher (Optional Hole Punch)

45-75ppm LVF – BKM Finisher (Optional Hole Punch)

Options: May Choose

- Keyboard
- 1L or 2L Fax
- Wi Fi
- Xerox PrintSafe Software
- Work Surface
- FDI
- CAC card reader
- Secure Access Card readers
- Conv. Stapler
- Near field communication device interface
- CAC Reader
- Unicode kit

2.1. Security-relevant Subsystems

2.1.1. Physical Partitioning

The security-relevant subsystems of the product are partitioned as shown in Figure 2-1.

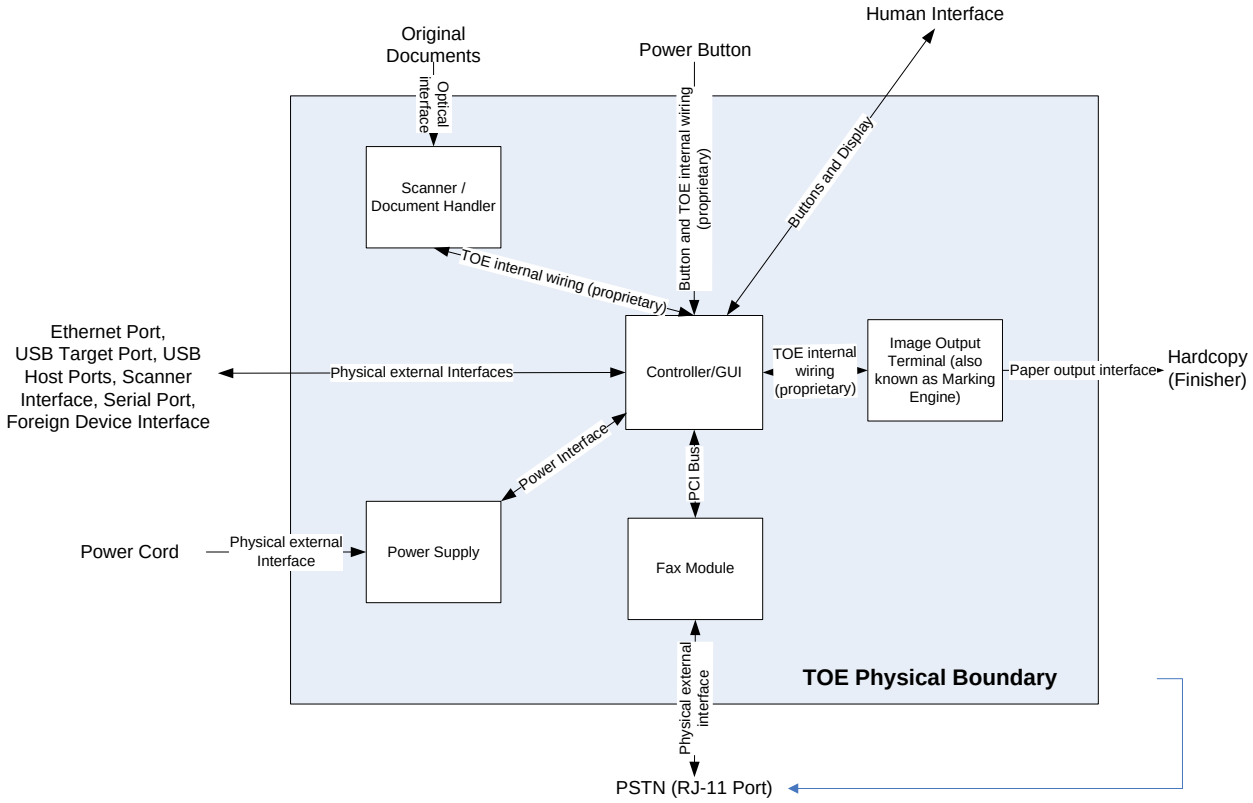


Figure 2-1 System functional block diagram

2.2. Controller

2.2.1. Purpose

The controller provides both network and direct-connect external interfaces, and enables copy, print, email, network scan, server fax, internet FAX, and LanFAX functionality. Network scanning, server fax, internet fax, and LanFax, are standard features. 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 also incorporates an open-source web server (Apache) that exports a Web User Interface (WebUI) through which users can submit jobs and check job and machine status, and through which system administrators can remotely administer the machine.

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 the network disk. The buffered bitmaps are then read from DRAM and sent to the Image Output Terminal (IOT) for marking on hardcopy output. For long documents, the production of hardcopy may begin before the entire original is scanned, achieving a level of concurrency between the scan and mark operations.

The controller operating system is Wind River Linux. Unnecessary services such as rsh, telnet and finger are disabled in the Operating System. FTP is used in client-only mode by the network-scanning feature for the filing of scanned images and the retrieval of Scan Templates; however, the controller does not contain an FTP server.

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.

2.2.2. Memory Components

General Memory Information

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.

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

Non-volatile memory in the system cannot be accessed by accidental keystrokes.

Detailed information on the memory, can be found in the Statement of Volatility document on www.xerox.com

2.2.3.External Connections

The controller printed wiring boards are physically mounted in a tray with external connections available at the right rear of the machine. The tray contains a single controller board. An optional fax board may also be installed. A disk is mounted on the underside of the tray. Below the controller tray are other connectors that distribute power and communications to external options such as a finisher or high-capacity paper tray.

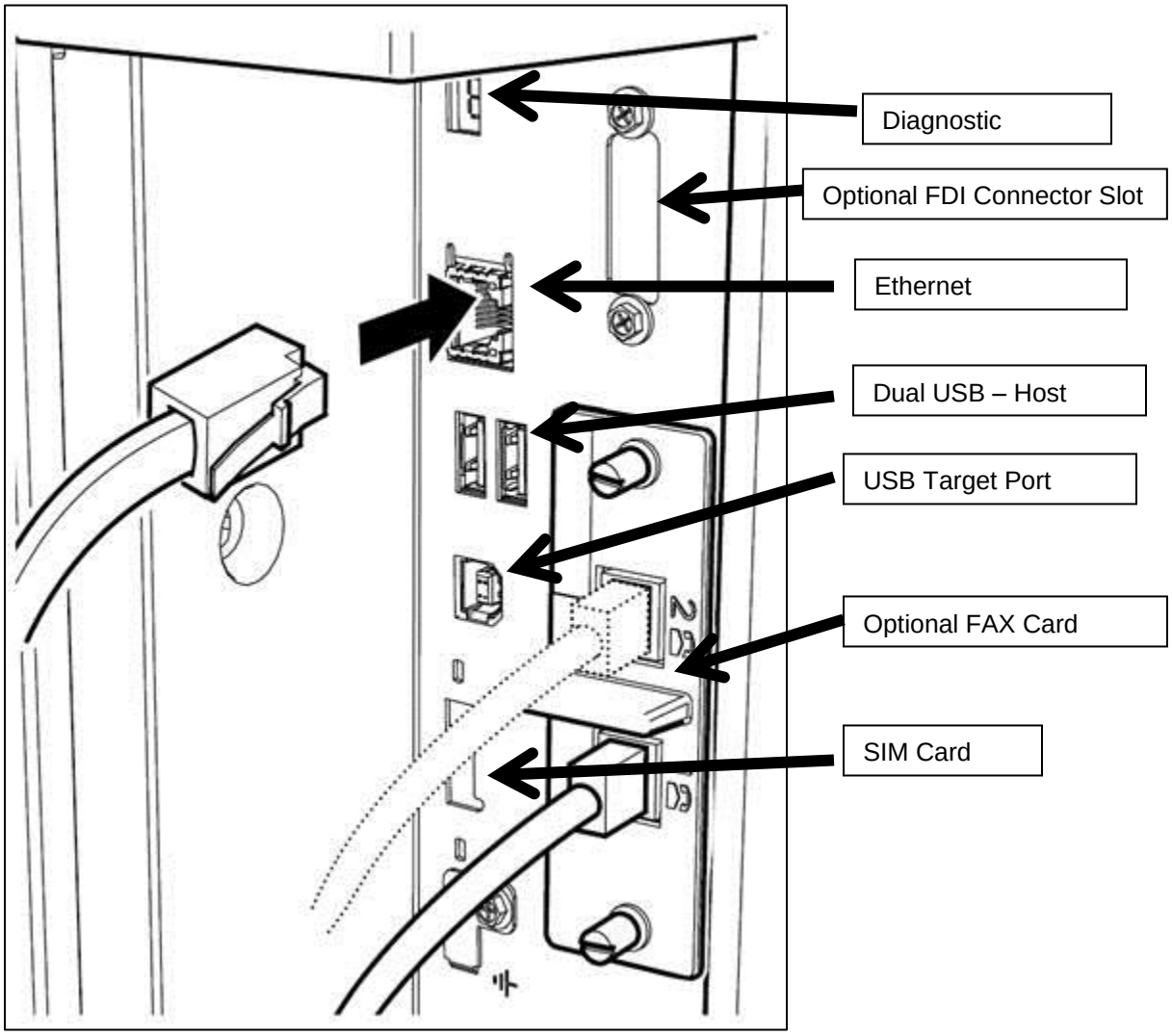


Figure 2-2 AltaLink® B80xx Back panel connections

Interface	Description / Usage
USB Target Port	Diagnostics and service; Xerox Copier Assistant
Dual USB Host Ports	Card readers; SW upgrade; USB Printing; Scan to USB
Ethernet Port	Network Connectivity
Diagnostic LED Readout	Displays status codes for Diagnostics
Foreign Device Interface (FDI)	Allows connection of optional access control hardware.
Optional FAX (Single or Dual)	Allows insertion of optional “Land Line” Fax card
SIM Card Slot	Options enablement

Table 1 Controller External Connections

2.2.4.USB Ports

The AltaLink® system contains a host connector for a USB flash drive, enabling upload of software upgrades and download of network logs or machine settings files and scan jobs.

Autorun is disabled on this port. No executable files will be accepted by the port.

Modifying the software upgrade, network log or saved machine settings files will make the files unusable on an AltaLink® system.

The data in the network log file is encrypted and can only be decrypted by Xerox service personnel at a Xerox location.

USB Port(s)	
USB port and location	**Purpose**
Front panel – 1 Host port	User retrieves print ready files from Flash Media or stores scanned files on Flash Media. Physical security of this information is the responsibility of the user or operator. Upload of software upgrades, download of network logs, download and upload of machine settings for setup cloning. Optional security devices, such as a CAC reader, access cards, and /or keyboard communicate with the machine via this port. No job data is transmitted across this interface when an optional security device is connected.
Rear panel – 2 Host ports	User retrieves print ready files from Flash Media or stores scanned files on Flash Media. Physical security of this information is the responsibility of the user or operator. Upload of software upgrades, download of network logs, download and upload of machine settings for setup cloning. Optional security devices, such as a CAC reader, and /or keyboard communicate with the machine via this port. No job data is transmitted across this interface when an optional security device is connected.
Rear panel – 1 Target port	User PC direct connection for printing, Xerox Customer Service Engineer PWS connection for problem diagnosis. The optional Copy Assistant kit communicates with the machine via this port. No job data is transmitted across this interface.
Additional Information A number of devices can be connected to the 3 USB Host ports. Once information has been copied (either as a back-up data set or as a transfer medium, physical security of this information is the responsibility of the user or operator.)	

Table 2 USB Ports

2.3. Optional Fax Module

2.3.1. Purpose

The optional embedded FAX service uses the installed embedded fax card to send and receive images over the telephone interface. The FAX card plugs into a custom interface slot on the controller.

2.3.2. Hardware

The Fax Card is a printed wiring board assembly containing a fax modem and the necessary telephone interface logic. It connects to the controller via a serial communications interface. The Fax Card is responsible for implementing the T.30 fax protocol. All remaining fax-specific features are implemented in software on the controller. The fax telephone lines are connected directly to the Fax Card via RJ-11 connectors.

2.4. Scanner

2.4.1. Purpose

The purpose of the scanner is to provide mechanical transport to convert hardcopy originals to electronic data.

2.4.2. Hardware

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. All other image processing functions are in the copy controller.

2.5. Graphical User Interface (GUI)

2.5.1. Purpose

The GUI detects soft and hard button actuations, and provides text and graphical prompts to the user. The GUI is sometimes referred to as the Local UI (LUI) to distinguish it from the WebUI, which is exported by the web service that runs in the controller. Images are not transmitted to or stored in the GUI.

2.6. Marking Engine (Image Output Terminal or IOT)

2.6.1. Purpose

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.

2.6.2. Hardware

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.

2.7. System Software Structure

2.7.1. Operating System Layer in the Controller

The OS layer includes the operating system, network and physical I/O drivers. The controller operating system is Wind River Linux. Xerox may issue security patches for the OS, in which case the Xerox portion of the version number (i.e. after the '+' sign) will be incremented.

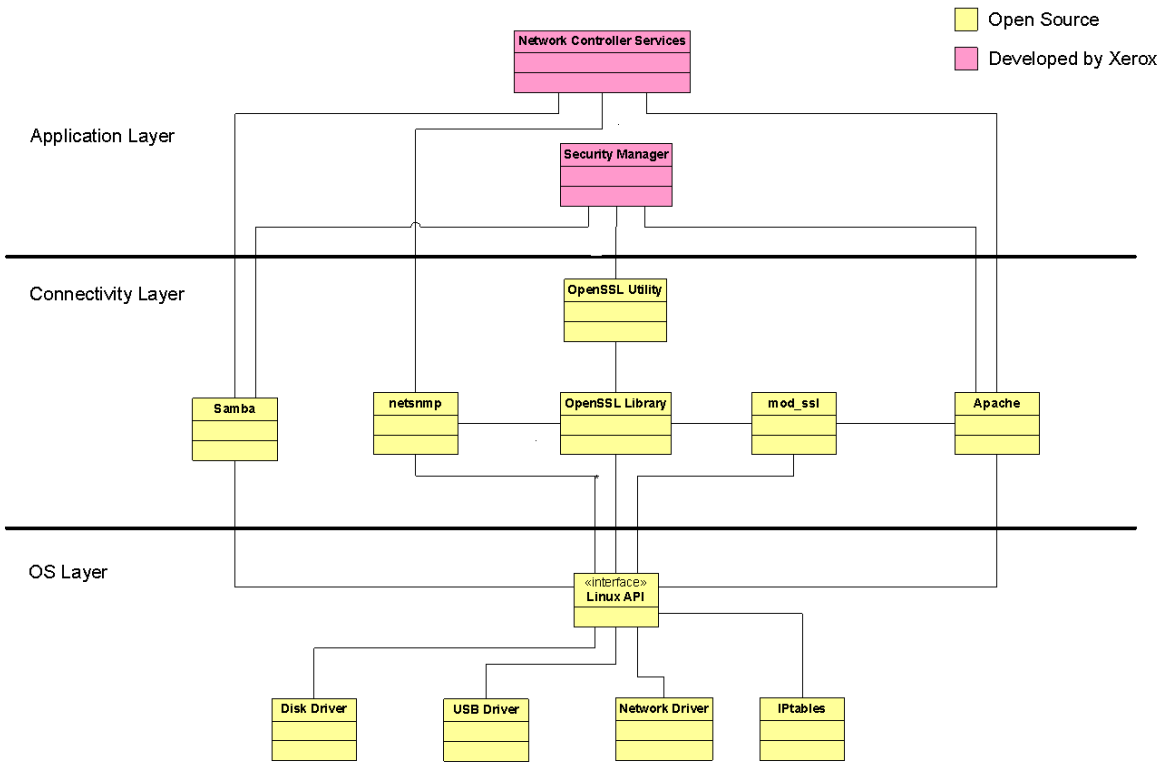


Figure 2-3 Controller Operating System layer components

2.7.2.Network Protocols

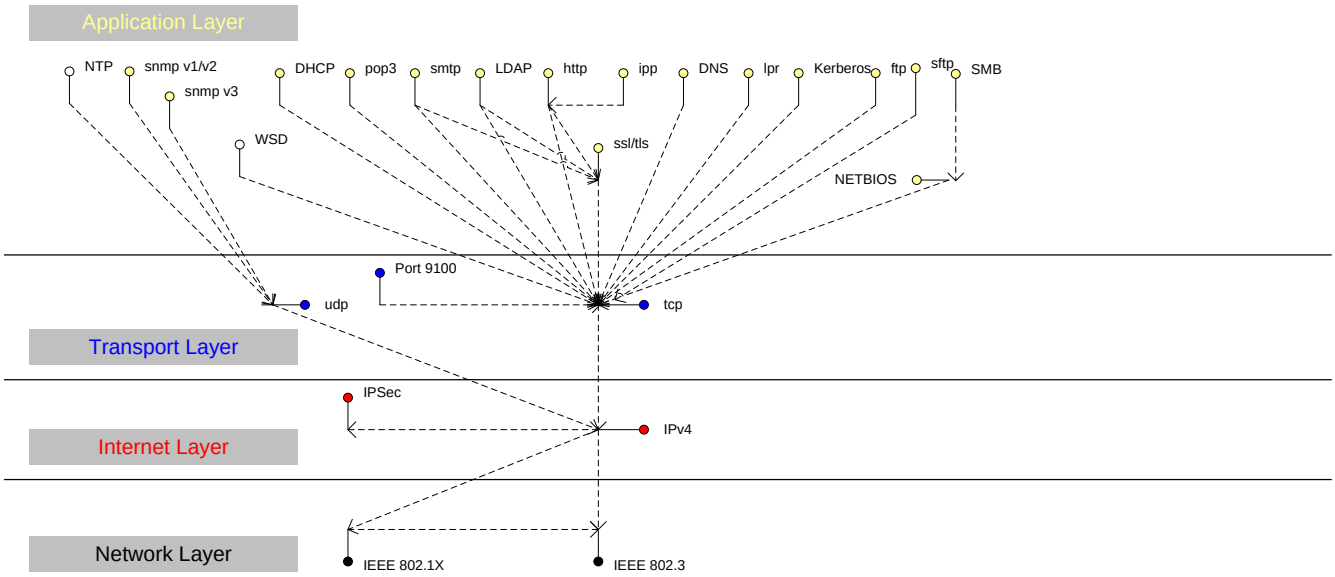


Figure 2-4 and Figure 2.6 are interface diagrams depicting the IPv4 and IPv6 protocol stacks supported by the device, annotated according to the DARPA model.

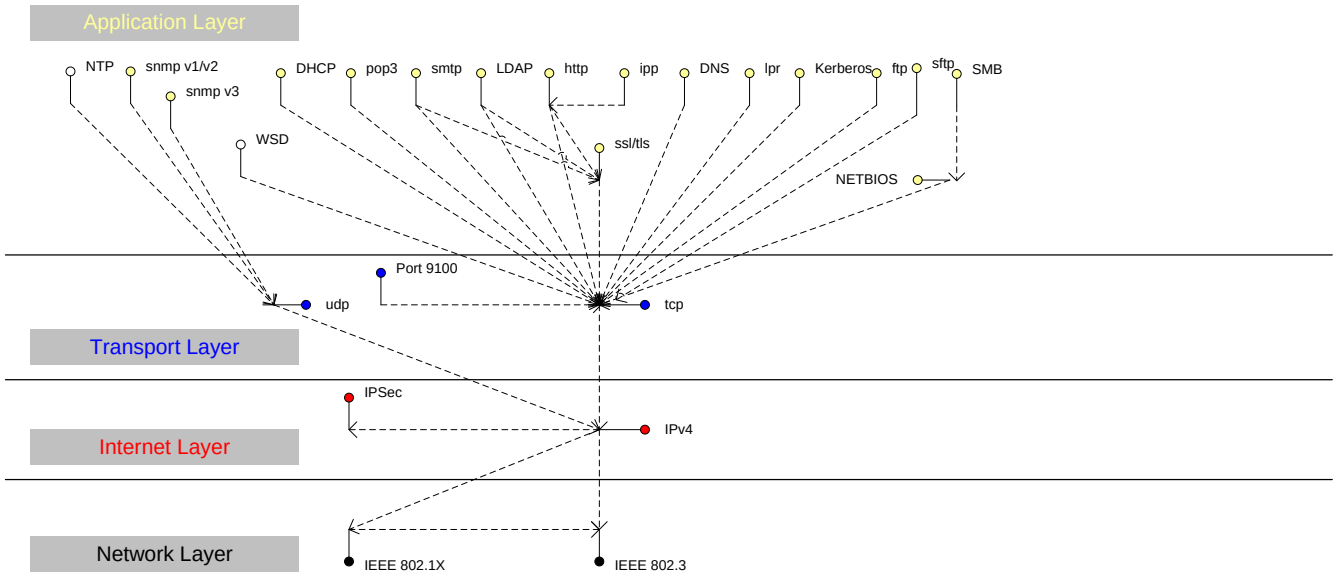


Figure 2-4 IPv4 Network Protocol Stack

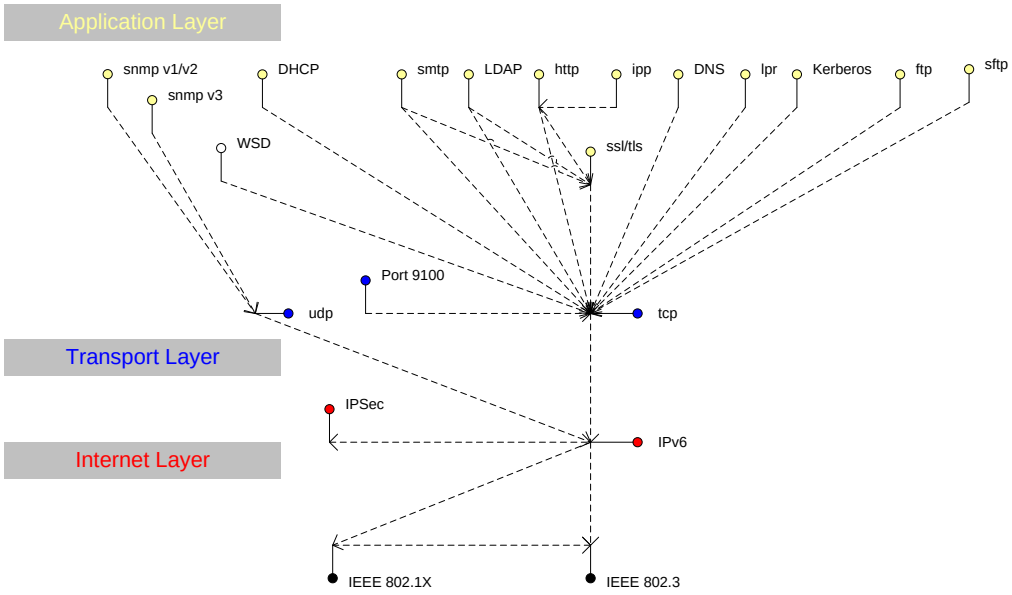


Figure 2-**6** IPv6 Network Protocol Stack

2.8. Logical Access

2.8.1. Network Security

A variety of network protocols is supported. There are no 'Xerox unique' additions to these protocols.

2.8.1.1. 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.

2.8.1.2. 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.

2.8.1.3. 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.

2.8.2.Ports

The following table summarizes all potentially open ports and subsequent sections discuss each port in more detail. All ports can be disabled if not needed under control of the system administrator.

Default Port #	Type	Service name
68	UDP	DHC ACK Response to DHCP
80	TCP	HTTP
88	UDP	Kerberos
110	TCP	POP3 client
137	UDP	NETBIOS- Name Service
138	UDP	NETBIOS-Datagram Service; SMB filing and Scan template retrieval
139	TCP	NETBIOS Session Service - SMB Authentication, SMB filing
161	TCP/UDP	SNMP
162	TCP	SNMPTRAP
427	TCP/UDP	SLP
443	TCP	HTTPS – HTTP over TLS
445	TCP	Microsoft-DS
500	TCP	ISAKMP
515	TCP	LPR
631	TCP	IPP
3702	TCP/UDP	WSD Discovery
4500	TCP/UDP	IKE Negotiation Port for IPSec
5353	TCP/UDP	Multicast DNS
5354	TCP	Multicast DNS Responder IPC
5909-5999	Remote UI	Remote Access to Local UI if feature is enabled. Ports randomized for security.
9100	TCP	raw IP
53202	TCP	WSD Transfer
53303	TCP	WSD Print
53404	TCP	WSD Scan

Table 3 Network Ports

3. System Access

3.1. Authentication Model

The authentication model allows for both local and network authentication and authorization. In the local and network cases, authentication and authorization take place as separate processes: a user must be authenticated before being authorized to use the services of the device.

If the device is set for local authentication, user account information will be kept in a local accounts database (see the discussion in Chapter 4 of Xerox Standard Accounting) and the authentication process will take place locally. The system administrator can assign authorization privileges on a per user basis. User access to services will be provided based on the privileges set for each user in the local accounts database. .

When the device is set for network authentication, the user's network credentials will be used to authenticate the user at the network domain controller.

Users can be authorized on an individual basis to access one or any combination of the available services such as Copy, Fax, Server Fax, Reprint Saved Jobs, Email, Internet Fax, Workflow Scanning Server, and Extensible Interface Platform Services. Authentication can also be achieved via CAC, SIPR, smart access cards.

Also, users can be authorized to access one or any combination of the following machine pathways: Services, Job Status, or Machine Status.

User Permissions, the new authorization method determines your authorization be Role. Roles are stored in the local account database and users are either directly assigned to the roles in the database, or the role is associated with an LDAP/SMB group. Once the device determines what group the user is a member of, it determines what roles in the local database are associated with that group and define access based on the roles. Assignment of users to the System Administrator role or the Accounting Administrator is also managed via User Permissions.

Figure 3-1 provides a schematic view of the authentication and authorization subsystem. Use of the local accounts database or a network database can be set independently for both authentication and authorization, meaning that it is possible to enable network authentication and local authorization, or vice versa. Usually authentication and authorization will be configured to use the same database.

3.1.1 SIPRNet

SIPRNet support is included as a customer purchasable option

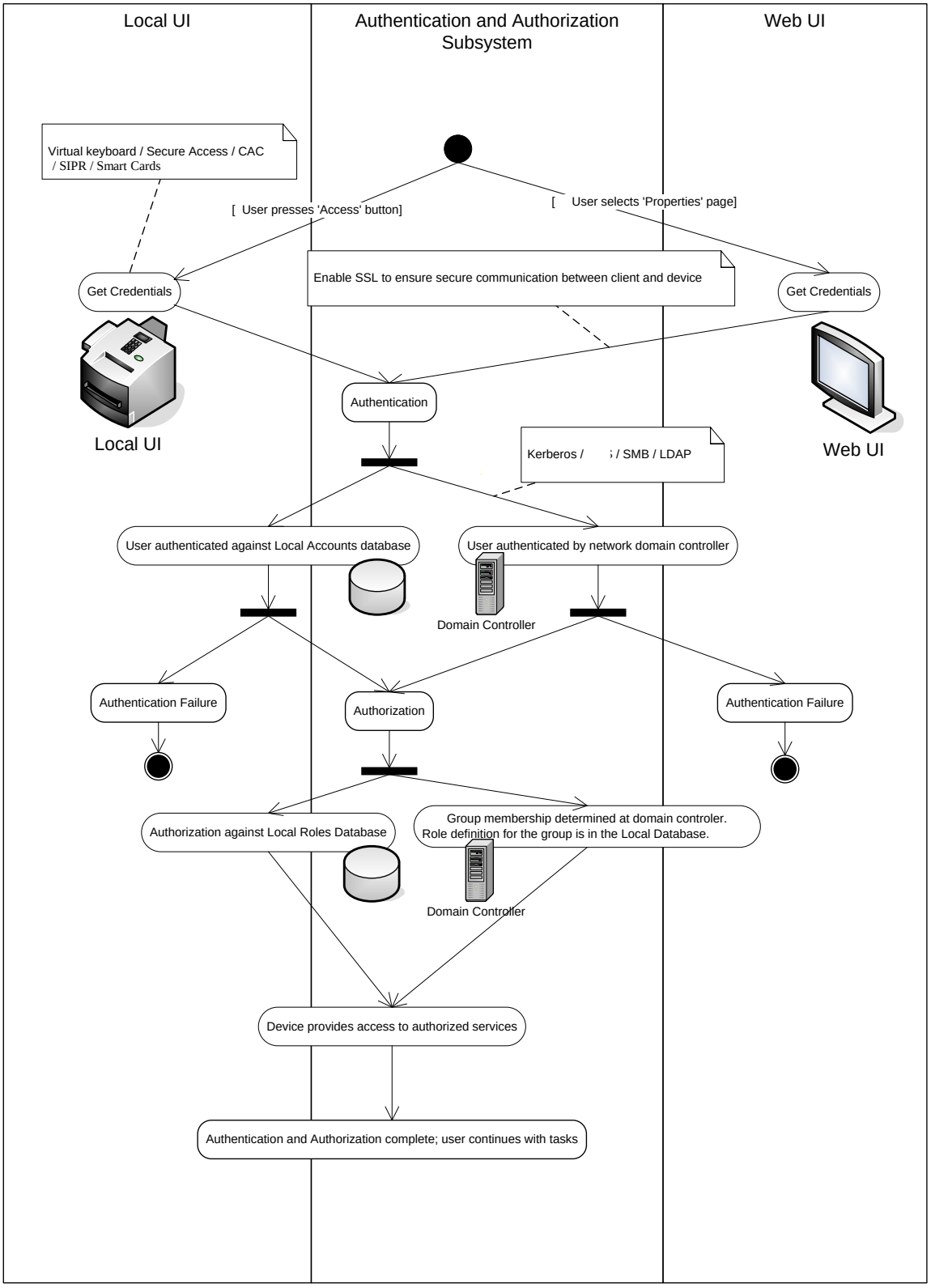


Figure 3-1 Authentication and Authorization schematic

3.2. Login and Authentication Methods

Network Scanning

Network Scanning may require the device to log into a server. The instances where the device logs into a server are detailed in the following table. Users may also need to authenticate for scanning. This authentication is detailed in subsequent sections.

Device log on

Scanning feature	Device behavior
Scan to File, Public Template	The device authenticates to the scan repository as set up by the SA in the Properties tab on the WebUI. The credentials may be the user's credentials or system credentials.
Scan to E-mail, I-Fax	The device logs into an LDAP Server as set up by the SA in User Tools. It will log into the Server when a user is authenticated and the device is configured for Remote Authorization or Personalization is enabled, and when the user attempts to access LDAP based scan-to-email address books. At the time the LDAP server must be accessed, the device will log into (bind to) the LDAP server. The device uses a simple bind to the LDAP server unless the device was able to obtain a TGS for the LDAP server from the Kerberos Server. In this case, a SASL (GSSAPI) bind is performed... A network username and password may be assigned to the device. The device logs in as a normal user, with read only privileges. User credentials may be used if configured by the SA for this authentication step. The device then logs into the SMTP server as set up by the SA in the Properties tab on the WebUI. The credentials may be the user's credentials or system credentials.
Scan to Fax Server	The device logs in to the Fax Server as set up by the SA from the Properties tab on the WebUI. The credentials may be the user's credentials or system credentials.

Please note that when the device logs into any server the device username and password are sent over the network in clear text unless one or more of the following have been enabled:

- HTTPS has been enabled
- IPSec has been configured to encrypt the traffic
- The device is logging into an SMB Server in which case the credentials are hashed.
- The device is using NTLM to login to the SMTP server (the device negotiates the most secure authentication method that both the device and server support).
- The LDAP server is being accessed via SASL.

4. Security Aspects of Selected Features

4.1. 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 and optional Integrity Control 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.

SW Install, Clone, and Weblets files are digitally signed and encrypted with AES256.

4.1.2 Integrity Control (Optional Feature)

Integrity Control is a purchasable software option that combines the standard Enhanced Security features with the ability to monitor and prevent unauthorized execution of files that were not part of the standard Xerox device software.

4.2. Audit Log

4.2.1 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.

4.2.2 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.

4.2.3 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 Device serial number
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.

Event ID	Event description	Entry Data
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.
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

Event ID	Event description	Entry Data
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
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

Event ID	Event description	Entry Data
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
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)

Event ID	Event description	Entry Data
27	Postscript Passwords	Device name Device serial number StartupMode (enabled/disabled) System Params Password changed Start Job Password changed
29	Network User Login	UserName Device name Device serial number Completion Status (Success, Failed)
30	SA login	UserName 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).
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

Event ID	Event description	Entry Data
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).
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)

Event ID	Event description	Entry Data
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
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)

Event ID	Event description	Entry Data
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)
60	Device Clock NTP Enable/Disable	Device Name Device serial number Enable/Disable NTP NTP Server IP Address Completion Status (Success/Failed)

Event ID	Event description	Entry Data
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)
68	FIPS Mode Enable/Disable/Configure	UserName Device name Device Serial Number Enable/Disable/Configure

Event ID	Event description	Entry Data
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
75	Remote UI feature	User Name Device Name Device Serial Number Completion Status (Enabled/Disabled/Configured)

Event ID	Event description	Entry Data
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 Completion 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)
81	Email Domain Filtering Rule	User name Device Name Device Serial Number Completion Status (Feature Enabled/Feature Disabled, Rule Added / Rule Deleted)

Event ID	Event description	Entry Data
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	UserName Device name Device serial number Security Mode (Enhanced Security / Integrity Control) Completion Status (Enabled / Disabled / Pending)
85	McAfee Security Event	Device name Device serial number Type (Read / Modify / Execute / Deluge) McAfee message text
87	McAfee Agent	User name Device name Device serial number Completion Status (Enabled / Disabled)
88	Digital Certificate Import Failure	Device name Device serial number Email address of requestor (if available) Failure reason (Invalid Address / Invalid Certificate / Invalid Signature)
89	User Name Add/Delete	UserName (managing user names) Device name Device serial number User name added or deleted Completion Status (Created/Deleted)

Event ID	Event description	Entry Data
90	User Name Password Change	Security Mode
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)

Event ID	Event description	Entry Data
97	EIP Weblets Install	UserName Device name Device serial number Weblet Name Action (Install / Delete) Completion (Success / Fail)
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)

Event ID	Event description	Entry Data
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)
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)

Event ID	Event description	Entry Data
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)
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)

Event ID	Event description	Entry Data
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)
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

Event ID	Event description	Entry Data
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)
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

Event ID	Event description	Entry Data
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)
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)

Event ID	Event description	Entry Data
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”)
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)

Event ID	Event description	Entry Data
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)
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)

Event ID	Event description	Entry Data
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
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”)

4.3. User Permissions Role Based Access Control (RBAC)

User Permissions provides permissions based on the authentication of the user through either the Local UI or network authentication. Commonly referred to as Role Based Access Control it assigns

each user the permissions to use the MFP based on a default role, a customized role or a Non-Logged-In User role.

4.4. 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.

4.5. 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.

SD Card Partition Layout

Order	Size (MB)	Name	GPT Type	Mount Path	Common Device Path	File System	Fsck	Perms	Encryption
1	200	flash	ESP	/mnt/flash	/dev/block_flash	FAT32	Std	755	Un
2	1800	persistent	Linux FS Data	/persistent	/dev/block_persistent	Ext4	Std	755	En

Key Management:

All private keys used for encryption or signing are encrypted on the hard drive, either individually encrypted directly, or encrypted by residing on an encrypted partition, or both.

When keying material, such as plaintext secret strings, and private cryptographic keys are destroyed they overwritten with a byte pattern prior to deletion.

4.6. 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, IJO 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.

4.6.1. Algorithm

The overwrite mechanism for both IJO and ODIO conforms to the U.S. Department of Defense Directive SP 800-88 Rev1

The algorithm for the Image Overwrite feature is:

Step 1: Pattern #1 is written to the sectors containing temporary files (IJO) 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 (IJO) 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 (IJO) 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.

4.6.2. 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 IJO 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 AltaLink® Internet Services Web UI. All device functions will be delayed 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.

4.6.3. 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.

4.6.4. Overwrite Completion Reporting

Immediate Job Overwrite

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 status are logged in Audit Log as well.

On Demand Image Overwrite

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 status are logged in Audit Log as well.

4.7. FIPS 140-2

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 optional FIPS 140-2 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 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 uses encryption algorithms that are not FIPS-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 compliant.
- IPSec over IPV6 and IPv4 are FIPS 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.

4.8. Email Signing and Encryption to Self

The device is capable of signing and encrypting emails when the user is authenticated to the device using a CAC, .NET or PIV smart card containing appropriate signing and encryption certificates. The device allows signing to multiple recipients using the SHA256 hash algorithm. The device allows encryption to the authenticated user only, supporting 3DES and AES encryption.
When enabled, the configuration options allow the system administrator the flexibility for the user to choose signing and encryption on a job-by-job basis, or require one or the other for all jobs.
NOTE: The crypto algorithms used for smart card authentication and encryption are FIPS validated, but the signing algorithm is not.

5.1. Responses to Known Vulnerabilities

4.9. Security @ Xerox (www.xerox.com/security)

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

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: http://www.xerox.com/information-security/information-security-articles-whitepapers/enus.html

.

5. APPENDICES

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 system. These are accessible through any browser using the machine's IP address as the URL.
XCMI	Xerox Common Management Interface

XSA Xerox Standard Accounting