Security Guide

Xerox® PrimeLink® B9100/9110/9125/9136 Copier/Printers

Document Version: 1.01 (May 2020).

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

Table of Contents

1. Introduction

Purpose

The purpose of this document is to disclose information for the PrimeLink® B9100/9110/9125/9136 Copier/Printer (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.

2. Product Description

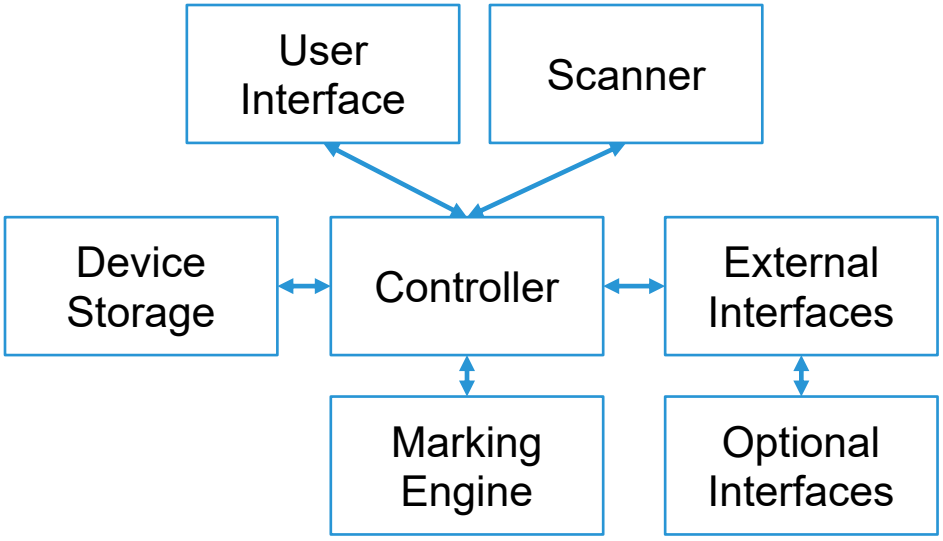
Physical Components

PrimeLink® Copier/Printer products consist of an input document handler and scanner, marking engine, controller, and user interface. 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. Bypass paper feed tray (tray 5).	**6. Front Cover.**
2. Duplex Automatic Document Feeder.	**7. Dry Ink/Toner Cover.**
3. Document Platen Scanner Cover.	**8. Dry Ink/Toner Waste Bottle Door.**
4. User Interface.	**9. Trays 1- 4.**
5. Optional Standard Finisher.	**10. High Capacity Feeder (Tray 6).**

Architecture

PrimeLink® Copier/Printer products share a common architecture which is depicted below. The following sections describe components in detail.



User Interface

The user interface detects soft and hard button actuations and provides text and graphical prompts to the user. The user interface is sometimes referred to as the Graphical User Interface (GUI) or Local UI (LUI) to distinguish it from the remote web server interface (WebUI).

The user interface allows users to access product services and functions. Users with administrative privileges can manage the product configuration settings. User permissions are configurable through Role Based Access Control (RBAC) policies, described in section 6: Identification, Authentication, and Authorization.

User image data in the memory on Controller is accessible (Preview Thumbnail feature).

Scanner

The scanner converts documents 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.

The scanner does not have its own control processor. The scanner attribute information is written in the SEEPROM and the control is performed by the controller.

Name	Purpose/Explanation
SEEPROM	This non-volatile memory has no user data stored in it. This memory contains: Mode setting information on image processing and mechatronics control, and data on the parts usage status associated with recycling.

Marking Engine

The Marking Engine performs copy/print paper feeding and transport, image marking, fusing, and document finishing. The marking engine is comprised of paper supply trays and feeders, paper transport, LED scanner, xerographic, and paper output and finishing. The marking engine is only accessible to the Controller via inter-chip communication with no other access and does not store user data.

Name	Purpose/Explanation
Flash ROM	All operating system and application executable control code related to Marking Engine resides here (e.g. boot loader, paper path, and xerographic).
SRAM **(Static RAM)**	This is a Work RAM used to develop the program and parameters in the above-mentioned Flash ROM. No user data is stored in this memory.

Controller

The controller manages document processing using proprietary hardware and algorithms to process documents into high-quality electronic and/or printed reproductions. Documents may be temporarily buffered in RAM during processing. Some models may be equipped with additional storage options such as magnetic Hard Disk Drive (HDD), Solid State Disk (SSD), SD Card, or Flash media. For model specific details please see Appendix A: Product Security Profiles. PrimeLink® products encrypt user data and include media sanitization (overwrite) options that ensure that erased data cannot be recovered, described further in section 3: User Data Protection.

In addition to managing document processing the controller manages all network functions and services. Details can be found in section Network Security

The controller handles all I/O communications with connected products. The following section provides a description of each interface. Please note that not all interfaces are supported on all models; details about each model can be found in Appendix A: Product Security Profiles.

The details of the memory devices in the Controller are:

Name	Purpose/Explanation
DRAM	The executable software is loaded in this memory and is run. This memory is also used for temporary storage of user data such as data files and images. Such data is not backed up and is deleted when a job is completed. And the all data is lost when the power to the device is removed.
Flash ROM	This Flash memory contains the code necessary to boot the system, all executable code (operating system, PostScript interpreter, network protocols, document scheduler, etc.), and the installed fonts. A power-on self-test is performed and the bootstrap OS is loaded. This memory never contains any user data or document data. Operating system and application executable control code resides here. All codes except for the code of boot loader are compressed and are extracted into DRAM to be executed. No user image data is stored in this memory.
NVRAM	This non-volatile memory has no image data stored in it. User data such as system setting information, mailbox information, job memory, user management information, and various types of logs are recorded in it. The data is written in the memory after it is encrypted.
Controller Hard Disk	This device contains numerous types of data including user data: 1. Data of the documents scanned in upon copying. 2. Data of spooled documents in PDL format from the network. 3. Data of the documents used in security print, sample print, and delayed—start print. 4. Data of the scanned-in documents 5. Job logs. 6. Downloaded fonts and forms. For the formatting of the hard disk, the file system included in Linux is used. The format, however, is not accessible even when the hard disk is connected to PC. When a job is completed, its reference in the directory table is deleted but the image data remains on the disk until overwritten by a subsequent job. Image Overwrite feature enables an overwrite of the used data with meaningless data. Also, Data Encryption feature enables a data encryption of the HDD data.
Page Memory	This is a volatile memory used to store image data temporarily.
SEEP ROM	This memory contains the system's setting information.

Controller External Interfaces

Front Panel USB (Type A) port(s)

One or more USB ports may be located on the front of the product, near the user interface. Front USB ports may be enabled or disabled by a system administrator. The front USB port supports the following:

- Walk-up users may insert a USB thumb drive to store or retrieve documents for scanning and/or printing from a FAT formatted USB device. The controller will only allow reading/writing of a limited set of known document types (such as PDF, PNG, JPEG, TIFF, etc.). Other file types including binary executables are not supported.

  Note: features that use the front USB ports (such as Scan To USB) can be disabled independently or restricted using role-based access controls.

- Connection of optional equipment such as CAC readers.

Firmware updates may be submitted through the front USB ports. (Note that the product must be configured to allow local firmware updates, or the update will not be processed.

10/100/1000 MB Ethernet RJ-45 Network Connector

This is a standard RJ45 Ethernet network connector and confirms to IEEE Ethernet 802.3 standards.

Rear USB (Type B) Target Port

A USB type B port located on the controller board at the rear of the product. This port supports the following:

- USB target connector used for printing

Note: This port cannot be disabled completely by a system administrator.

Optional Equipment

RJ-11 Analog Fax and Telephone

The analog fax module connects to the controller. The fax connection supports the Fax Modem T.30 protocol only and will not accept data or voice communication attempts. An external (EXT) is available to connect an external handset. In this configuration, the FAX card acts as a passive relay.

Wireless Network Connector

PrimeLink® Copier/Printer products do not offer a wireless connector option.

Near Field Communications (NFC) Reader

PrimeLink® Copier/Printer products do not support Near Field Communications (NFC) Reader

SMART CARD – CAC/PIV

PrimeLink® products support CAC/PIV login by enabling the Plug-in feature and then enabling the appropriate plug-in. Additional plug-ins can be downloaded from Xerox.com in the product Support area online.

All PrimeLink® products support SIPR network access through a plug-in. The SIPR network plug-in is restricted only to users who have purchased the SIPR kit from Xerox. Contact your Xerox sales representative for details.

Foreign Product Interface

This port is used to connect optional equipment to control access to the machine. A typical application is a coin-operated product where a user must deposit money to enable the machine to print. The information available via the Foreign Product Interface is limited to optically-isolated pulses that can be used to count impressions marked on hardcopy sheets. No user data is transmitted to or from this interface.

3. User Data Protection

Xerox printers and multifunction products receive, process, and may optionally store user data from several sources including as local print, scan, fax, or copy jobs or mobile and cloud applications, etc. Xerox products protect user data being processed by employing strong encryption. When the data is no longer needed, the Image Overwrite (IIO) feature automatically erases and overwrites the data on magnetic media, rendering it unrecoverable. As an additional layer of protection, an extension of IIO called On-Demand Image Overwrite (ODIO) can be invoked to securely wipe all user data from magnetic media.

User Data Protection While Within Product

This section describes security controls that protect user data while it is resident within the product. For a description of security controls that protect data in transit please refer to the following section that discusses data in transit; also, the Network Security section of this document.

Encryption

All user data being processed or stored to the product is encrypted by default. Note that encryption may be disabled to enhance performance on PrimeLink® products (though this is not recommended in secure environments).

The algorithm used in the product is AES-256. The encryption key is automatically created at start up and stored in the RAM. The key is deleted by a power-off, due to the physical characteristics of the RAM.

Trusted Platform Module (TPM Chip)

PrimeLink® products does contain a TPM. Please refer to Appendix A: Product Security Profiles for model specific information.

Media Sanitization (Image Overwrite)

PrimeLink® Copier/Printer equipped with magnetic hard disk drives are compliant with NIST Special Publication 800-88 Rev1: Guidelines for Media Sanitization. User data is securely erased using a three-pass algorithm as described in the following link:

https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-88r1.pdf

Note: Solid-State storage media such as Solid-State Disk, eMMC, SD-Card, and Flash media cannot be completely sanitized by multi-pass overwriting methods due to the memory wear mapping that occurs. (Additionally, attempts to do so would also greatly erode the operational lifetime of solid-state media). Solid State media is therefore not recommended for use in highly secure environments. Please refer to NIST-800-88r1 “Table A-8: Flash Memory-Based Storage Product Sanitization” for technical details.

Overwriting Immediate Image Overwrite

When enabled, Immediate Image Overwrite (IIO) will overwrite any temporary files that were created on the magnetic hard disk that may contain user data. The feature provides continuous automatic of sensitive data with minimal impact to performance, robust error reporting, and logging via the Audit Log.

On-Demand Image Overwrite

Complementing the Immediate Image Overwrite is On-Demand Overwrite (ODIO). While IIO overwrites individual files, ODIO overwrites entire partitions. The ODIO feature can be invoked at any time and optionally may be scheduled to run automatically.

User Data in Transit

This section focuses on the protection of user data (print/scan/other jobs) in transit as they are submitted to the product for processing and/or are sent from the product to other systems. Additional protections are also discussed in the Network Security section of this document.

Inbound User Data (Print Job Submission)

In addition to supporting network level encryption including IPSec and WPA Xerox products also support encryption of print job data at the time of submission. This can be used to securely transmit print jobs over unencrypted connections or to enhance existing network level security controls.

Encrypted Transport	Description
IPPS (TLS)	Submit print jobs via Secure Internet Printing Protocol. This protocol is based on HTTP and utilizes the TLS suite to encrypt data.
HTTPS (TLS)	Securely submit a print job directly to product via the built-in web server.

- Servers that utilize TLS1.0, TLS1.1, and TLS1.2 with Cipher-Block-Chaining mode enabled are susceptible to man in the middle attacks that exploit MAC padding.
- To mitigate this vulnerability on print systems that support disabling CBC ciphers, configure the servers communicating with the print system to disallow use of CBC mode.

Scanning to Network Repository, Email, Fax Server (Outbound User Data)

PrimeLink® Copier/Printer support scanning of hardcopy documents to external network locations including file repositories and email and facsimile services. In addition to supporting network level encryption including IPSec Xerox products support the following.

Protocol	Encryption	Description
HTTP	N/A	Unencrypted HTTP protocol.
HTTPS (TLS)	TLS	HTTP encrypted by TLS
FTP	N/A	Unencrypted FTP.
SFTP (SSH)	SSH	FTP encrypted by SSH through “EIP” ONLY
SMBv3	N/A	Unencrypted Available
SMBv2	N/A	Unencrypted SMB

SMBv1	N/A	(Not used as a transport protocol. Used for network discovery only)
SMTP (email)	S/MIME	The product uses SMTP to transmit data to the email server. Email authentication, encryption, and signing are supported. Please refer to the Network Security section of this document for details.

Note: Random UDP ports are open due to Device SMB client requirement. These UDP ports need to remain Open as long as SMB Client is enabled.

Scanning to User Local USB Storage Product (Outbound User Data)

Scan data is transferred directly to the user's USB product. Filesystem encryption of user products are not supported.

Add on Apps – Cloud, Google, DropBox, and others (Outbound User Data)

The Xerox App Gallery contains several additional applications that extend the capabilities of Xerox products. Discussion of App security is beyond the scope of this document. Xerox Apps utilize the security framework provided by the third-party vendor. (For example, Microsoft O365 or Google apps would utilize Microsoft and Google's security mechanisms respectively). Please consult documentation for individual Apps and third-party security for details.

Local Data Encryption (HDD)		AES-256
Federal Information Protection Standard 140-2		Yes
Media Sanitization NIST 800-171 (Image Overwrite)		Models with magnetic HDD. See Appendix A: Product Security Profiles.
Print Submission		
	IPPS (TLS)	Supported
	HTTPS (TLS)	Supported
	Xerox Print Stream Encryption	Not Supported
Scan to Repository Server		
	HTTPS (TLS)	1.2
	SFTP (SSH)	Not Supported
	SMB (unencrypted)	v1, v2, v3
	SMB (with share encryption enabled)	Not Supported
	HTTP (unencrypted)	Supported
	FTP (unencrypted)	Supported
Scan to Fax Server		
	HTTPS (TLS)	1.2
	SFTP (SSH)	Not Supported
	SMB (unencrypted)	v1, v2, v3
	SMB (with share encryption enabled)	Not Supported
	S/MIME	Supported
	HTTP (unencrypted)	Supported
	FTP (unencrypted)	Supported
	SMTP (unencrypted)	Supported
Scan to Email		
	S/MIME	Supported
	SMTP (unencrypted)	Supported

4. Network Security

Xerox products are designed to offer a high degree of security and flexibility in almost any network environment. This section describes several aspects of the product related to network security.

TCP/IP Ports and Services

Xerox devices are robust, offering support for a wide array of services and protocols. The devices are capable of hosting services as well as acting as a client for others. The diagram below presents a high-level overview of inbound communications (from other hosts on the network into listening services on the device) and outbound connections initiated by the device (acting as a client to external network services).

Inbound (Listening Services)		Out Bound (Network Client)
Print Services LPR, IPP, Raw IP, etc. **Management Services** SNMP, Web interface, WebServices, etc. **Infrastructure and Discovery Services** IPSEC, SSDP, WSD, mDNS, NetBIOS, etc.		**Built-in Scan Services** FTP, HTTP & HTTPS (TLS), SMB, CIFS, SMTP & SMTPS, POP3 and POPS, etc. **Authentication Services** LDAP & LDAPS, SMB, Kerberos. **Infrastructure** ISAKMP (IPSec), DHCP and DHCPv6, etc. Dropbox, Google Drive, OneDrive, and several others.

Listening Services (inbound ports)

The following table summarizes all potentially open ports on the product. These ports can be enabled/disabled within the product configuration.

Port	Type	Service Name
20	TCP	• FTP data (Active) – Client –
20	TCP	• FTP data (FreeFlow)
21	TCP	• FTP – Client –
21	TCP	• FTP data (FreeFlow)
25	TCP	• SMTP
53	TCP/UDP	• DNS – Client –
67	UDP	• BOOTP/DHCP – Client
80	TCP	• HTTP(CWIS)
80	TCP	• HTTP(UPnP Discovery)
80	TCP	• HTTP(WSD)
80	TCP	• HTTP(WebDAV)
80	TCP	• HTTP(IPP added port)
88	UDP	• Kerberos – Client
110	TCP	• POP3 – Client
123	UDP	• SNTP – Client
137	UDP	• NETBIOS – Name Service
138	UDP	• NETBIOS – Datagram Service
139	TCP	• NETBIOS
161	UDP	• SNMP
162	UDP	• SNMP trap
389	TCP	• LDAP – Client
427	TCP/UDP	• SLP
443	TCP	• HTTP(CWIS)
443	TCP	• HTTP(IPP)
443	TCP	• HTTP(WebDAV)
443	TCP	• HTTP(Authentication Agent)
445	TCP	• Direct Hosting
465	TCP	• SMTPS – Client
500	UDP	• ISAKMP
515	TCP	• LPR
524	TCP	• NetWare NCP – Client
547	UDP	• DHCPv6 – Client
631	TCP	• IPP (FreeFlow)
636	TCP	• LDAPS – Client
1824	TCP	• HTTPS(OffBox Validation) – Client –

Port	Type	Service Name
1824	TCP	• Xerox Secure Access
1900	UDP	• SSDP
3702	UDP	• WSD Discovery
5353	UDP	• Mdns
9100	TCP	• raw IP
15000	TCP	• Loopback port for the control of SMTP server
20001	TCP	• Loopback port for HTTP Server
1024	TCP	• NetWare, SLP

“- Client -“: The port number is not for the port on the controller side, but for the port of the connecting destination. Unless the port number for the controller side is specified, the port number for the controller side is unknown. Also, the port is not open on the controller all the time but will open only at time of accessing the remote server.

Ports 20, 21: FTP

There are cases where this port is used as an FTP client feature or as an FTP server feature.

When it is used as an FTP client feature, this port is not open all of the time. This port is open only when sending image data to the FTP server to perform ScanToFTP and MailboxToFTP functions, or when accessing the FTP server to search for Scan Job Flow Sheets (i.e. Scan job Flow Sheets). In other cases, no ports are connected to the FTP server.

FTP server feature is activated only when FreeFlow feature is enabled. Port 21 is open at all times and Port 20 opens only when receiving image data from the FTP client. A service engineer can configure these port numbers. A system administrator can disable these ports and service (turn FTP ports OFF/ON) from Embedded Web Services.

NOTE: FTP server feature is only activated when Freeflow Protocol (port 631) is enabled.

If you disable FTP Protocol (port 21) you will also need to disable Freeflow Protocol when performing security port scans.

Access to disable Protocols/Ports can be found in the Embedded Web Server under the following paths:

“Properties/Connectivity/Port Settings”

“Properties/Connectivity/Protocols”

Port 25: SMTP

This port enables E-mail Print feature, and is open all of the time when the receive protocol is set to SMTP. Also, this port is open when sending image or message to SMTP server in Scan to E-mail, or Email Alert feature. When “SMTP Authentication” is set, authentication to the server is performed. In such case, a password is sent in plain text or as encrypted according to the information notified by the server. A system administrator can change the port number from Embedded Web Services.

Port 53: DNS

This port is used for DNS. This port is used for name queries to the DNS server when the product accesses the device designated by the device name. This port is also used to register device names in DNS server (authoritative server) to update the DNS dynamically. A system administrator can disable only DNS dynamic update service from Embedded Web Services.

Port 67: DHCP

This port is used only when performing DHCP, and is not open all of the time. To permanently close this port, DHCP must be explicitly disabled. This is done via the Local User Interface or Embedded Web Services by a system administrator.

Port 80: HTTP (EWS)

This port is used to access embedded web pages through browser. The port number can be changed from Embedded Web Services by a system administrator.

The embedded web pages are used for the following purposes:

- to give information on device status to users.
- to enable confirmation of the job logs and job queue in the device, and operation of the jobs.
- to allow users to download print ready files and program Scan Job Flow Sheets.
- to enable management of Mailboxes and operation on the documents in Mailboxes.
- to enable import/export of Address Book and import of device certificate.
- to allow remote administration of the device. User may view the properties but not change them without logging into the product with system administrator privileges. When authentication of a system administrator fails for the specified number of times consecutively, rebooting of the entire product is required.

A read/write of partial system setting information is possible through the unique protocols on the HTTP port.

The HTTP server can only host the web pages in the device, but cannot substitute for the proxy server. Through HTTP, the file system of the product cannot be accessed directly.

The embedded HTTP server is a unique implementation.

A system administrator can disable this service (and the port) via Local User Interface or from Embedded Web Services.

Port 80: HTTP (WebDAV)

This port is a WebDAV server port that supports features to access Mailbox. The port number is configurable, and a system administrator can disable this service (and the port) via local UI or from Embedded Web Services.

Port 88: Kerberos

The product employs Kerberos client function that is used to access this product from Local UI.

The product supports Kerberos V5 and uses CBC (Cipher Block Changing) of DES (Data Encryption Standard). The Kerberos code is not used for document encryption.
The authentication data of the user permitted by the product is set in the Kerberos server, and

address information and realm information of the Kerberos server used by the product is set in the Controller NVRAM.

The following show the difference from the standard Kerberos packaging.

7. **Ticket cache** – In the product, tickets are stored only in a memory, and are deleted automatically by a user log-off or an automatic log-off due to time-out. When power is turned off during log-on, the tickets will be deleted.
8. **Validity of the ticket** – In the product, only the initial ticket is obtained; authentication is considered as successful when the initial ticket is obtained. Thus, invalidation of the initial ticket is not judged.

Port 110: POP3

This port enables E-mail Print feature and is open at the specified intervals set when receive protocol is set to POP3. Also, when “POP Before SMTP” is set, POP access is always performed before sending data such as image to the SMTP server. Usually the POP User ID and the password are sent in plain text, but the password is encrypted to be sent when “APOP authentication” is selected. A system administrator can change the port number from Embedded Web Services.

Port 123: SNTP

This port is used to access the server at the specified intervals when time synchronization with the external time is set on the Local User Interface. The setting can be changed by a system administrator.

Ports 137, 138, 139, 445: NETBIOS

Port 137 is the standard NetBIOS Name Service port and mainly used by WINS. Port 138 supports the CIFS browsing protocol. Port 445 is a standard direct host port and is used for communication using SMB protocol that does not use NetBIOS over TCP. A system administrator can disable each of the 4 ports via Local User Interface or from Embedded Web Services. To use the SMB feature for Scan, all of the above ports need to be available. For Scan, image is sent to Port 139 or Port 445, both of which are on the remote server. SMBV1, V2 and V3 are supported for ScanToSMB / MailboxToSMB, ScanToHome and ScanToPC as SMB client.

Ports 161, 162: SNMP

These ports support the SNMPv1, SNMPv2c, and SNMPv3 protocols. SNMPv1 and SNMPv2c control access to device’s MIB information by using write community string and read community string. Since these community strings are transmitted on network in plain text, users should note that the community strings can be read if packets are dumped. It is highly recommended that the customer changes the community string from the default upon product installation. To solve the above problem, for SNMPv3, packets on network are authenticated and encrypted, which realizes safe access. Therefore, users who place importance on security should use SNMPv3. A system administrator can set enable/disable of the SNMP from the local UI or Embedded Web Services.

Port 389: LDAP

This is the standard LDAP port used for Address Book queries in LDAP authentication and the Scan to Email feature.

Port 427: SLP

In the product, this port is used to search the NetWare server on the network, on the IP protocol. This function operates only when the NetWare print function is set to be used on the IP protocol.

Port 443: HTTPS

This port operates as a secure channel for HTTP server, and supports TLSv1.1 and TLSv1.2. When SSL/TLS is enabled, HTTP connections to Embedded Web Services are redirected to HTTPS. Since communication through this port is encrypted, interception on the network can be avoided. A system administrator can change the port number and/or disable the port via local UI or from Embedded Web Services.

Port 443: HTTPS (IPP)

This port operates as a secure channel for internet print protocol, and supports TLSv1.1 and TLSv1.2. Since communication through this port is encrypted, interception on the network can be avoided. A system administrator can change the port number and/or disable the port via local UI or from Embedded Web Services.

Port 443: HTTPS (WebDAV)

This port operates as a secure channel for Web DAV server, and supports TLSv1.1 and TLSv1.2. When SSL/TLS is enabled, HTTP connections to WebDAV server are redirected to HTTPS. Since communication through this port is encrypted, interception on the network can be avoided. The port number is configurable, and a system administrator can disable this service (and the port) via local UI or from Embedded Web Services.

Port 465, SMTPS

This is the secure channel port used to access the SMTP server using SMTPS (SMTP over TLS) for Scan to Email and Email Alert.

Port 500: ISAKMP

This port is used for IKE in order to establish an IPSec SA (Security Association), and is open all of the time for IKE communication. When the product communicates to an external device as a client, the port number of the product and that of the external device are both 500. A system administrator can disable IPSec via local UI or from Embedded Web Services.

Port 515: LPR

This is the standard LPR printing port, which only supports IP printing. The port number is configurable, and a system administrator can disable this service (and the port) via Local User Interface or from Embedded Web Services.

Port 524: NetWare NCP

This is a port on the NetWare server side, and is used to provide print service through IP connection to NetWare server. After connection, the port is used until the power is turned off. The port number cannot be changed. A system administrator can disable the service via local UI or from Embedded Web Services.

Ports 546, 547: DHCPv6

These ports are used for DHCPv6. When querying the IPv6 DNS server address, the product accesses port 547 of DHCPv6 server and receives the result from DHCPv6 server at port 546. The

product can query the IPv6 DNS server address when the auto acquisition of IPv6 DNS server address is enabled, and a system administrator can disable it from Embedded Web Services.

Ports 80, 631: IPP (FreeFlow)

These ports support the Internet Print protocols(IPP). 631 is the standard port number for IPP and 80 is an added port number. The added port number is configurable. A system administrator can disable this service and port 80 (turn IPP port OFF/ON) via Local User Interface or from Embedded Web Services. IPP is also used in FreeFlow print. In FreeFlow print, only port 631 is used. A system administrator can disable this port and service (turn FreeFlow port OFF/ON) from Embedded Web Services.

NOTE: Both IPP Protocol and Freeflow Protocol share common port 631. If you disable IPP Protocol (port 631) you will also need to disable Freeflow Protocol when performing security port scans.

Access to disable Protocols/Ports can be found in the Embedded Web Server under the following paths:

“Properties/Connectivity/Port Settings”

“Properties/Connectivity/Protocols”

Port 636: LDAPS

This is the secure channel port used to access LDAP server using LDAPS (LDAP over TLS) for LDAP authentication and for Address Book queries in the Scan to Email feature.

Port 1824: HTTPS (OffBox Validation)

This port is used to communicate with OffBox Validation server. The protocol and port number can be changed by a system administrator on the OffBox Validation server side and cannot be changed via local UI or from Embedded Web Services.

Port 1900: SSDP

This port provides the discovery feature that complies with SSDP (Simple Service Discovery Protocol). This port number cannot be changed. Whether this port opens depends on whether the UPnP discovery feature is/are enabled or disabled.

Port 3702, WSD Discovery

This port provides the WSD (Web Services on Devices) discovery feature. This port number cannot be changed. Whether this port opens depends on whether the WSD print feature is enabled or not.

Port 5353: mDNS

This port provides the discovery feature using Multicast DNS. The port number is fixed to 5353. A system administrator can disable this service via local UI or from Embedded Web Services.

Port 9100: raw IP

This port has a bidirectional function (via pjl back channel), and only allows printing. The port is a configurable port and a system administrator can disable this service (and the port) via Local User Interface or from Embedded Web Services.

Port 15000: Loopback Port

This port is the loopback port for the control of the common server that operates the SMTP server, and is activated when SMTP receive is enabled. A system administrator can disable this loopback port by disabling SMTP receive via Local User Interface or from Embedded Web Services.

Network Encryption

IPSec

Internet Protocol Security (IPsec) is a network security protocol capable of providing encryption and authentication at the packet level. PrimeLink® Copier/Printer products support IPSec for both IPv4 and IPv6 protocols.

IPSec	
Supported IP Versions	IPv4, IPv6
Key exchange authentication method	Preshared Key and digital signature, device authentication certificate, server validation certificate
Transport Mode	Transport mode only
Security Protocol	ESP only
ESP Encryption Method	AES256
ESP Authentication Methods	None SHA1/SHA256/SHA384/SHA512

Wireless 802.11 Wi-Fi Protected Access (WPA)

PrimeLink® Copier/Printer products do not offer a wireless network connector option.

TLS

PrimeLink® Copier/Printer products support TLS 1.2.

TLS Version Supported	
Product Web Interface	1.2, 1.1, 1.0
Product Web Services	1.2, 1.1, 1.0
Product IPPS printing	1.2, 1.1, 1.0
Remote control	Not Supported

Encryption Suites

TLS Protocol	Supported Encryption Suites
TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA
TLS 1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA
TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA256

Note: Ensure that applications or services are configured to reject SSLv3, SSLv2 and TLSv1.0 communications. Disabling weak protocols is a defense-in-depth measure against vulnerabilities that could allow SSL version downgrade attacks

Public Key Encryption (PKI)

A digital certificate is a file that contains data used to verify the identity of the client or server in a network transaction. A certificate also contains a public key used to create and verify digital signatures. To prove identity to another product, a product presents a certificate trusted by the other product. The product can also present a certificate signed by a trusted third party and a digital signature proving that it owns the certificate.

A digital certificate includes the following data:

- Information about the owner of the certificate
- The certificate serial number and expiration date
- The name and digital signature of the certificate authority (CA) that issued the certificate
- A public key
- A purpose defining how the certificate and public key can be used
- There are four types of certificates:
- A Product Certificate is a certificate for which the printer has a private key. The purpose specified in the certificate allows it to be used to prove identity.
- A CA Certificate is a certificate with authority to sign other certificates.
- A Trusted Certificate is a self-signed certificate from another product that you want to trust.

- A domain controller certificate is a self-signed certificate for a domain controller in your network. Domain controller certificates are used to verify the identity of a user when the user logs in to the product using a Smart Card.

For protocols such as HTTPS, the printer is the server, and must prove its identity to the client Web browser. For protocols such as 802.1X, the printer is the client, and must prove its identity to the authentication server, typically a RADIUS server.

Device Certificates

PrimeLink® products support both CA signed and self-signed certificates. Product certificates support a bit length of up to 3072bits.

A CA signed certificate can be created by generating a Certificate Signing Request (CSR), and sending it to a CA or a local server functioning as a CA to sign the CSR. An example of a server functioning as a certificate authority is Windows Server 2008 running Certificate Services. When the CA returns the signed certificate, install it on the printer.

Alternatively, a self-signed certificate may be created. When you create a Product Certificate, the product generates a certificate, signs it, and creates a public key used in SSL/TLS encryption.

Device Certificates	
Certificate Length	2048, 3072
Supported Hashes	SHA2, SHA256, SHA384, SHA512
Product Web Server	Supported
IPPS (TLS) Printing	Supported
802.1X Client	Supported
Email Signing	Supported
Email Encryption	Supported
OCSP Signing	Supported
IPSec	Supported
SFTP	Not Supported

Trusted Certificates

Public certificates may be imported to the product's certificate store for validation of trusted external products. The following categories are supported:

- A Trusted Root CA Certificate is a certificate with authority to sign other certificates. These certificates usually are self-signed certificates that come from another product or service that you want to trust.
- An Intermediate CA Certificate is a certificate that links a certificate to a Trusted Root CA Certificate in certain network environments.
- Other Certificates are certificates that are installed on the printer for solution-specific uses.

An administrator can specify the minimum encryption key length required for certificates. If a user attempts to upload a certificate that contains a key that does not meet this requirement, a message appears. The message alerts the user that the certificate they are attempting to upload does not meet the key length requirement.

Trusted Certificates	
Minimum Length Restriction Options	2048, 3072
Maximum Length	4096
Supported Hashes	SHA2/224/256/384/512
Supported Formats	.cer, .der, PKCS#7, PKCS#12 (.pfx, .p12)
IPSec	Supported
LDAP	Supported
Scanning (HTTPS/TLS)	Supported
Scanning (FTP/SSH)	Supported
802.1X Client	Supported
Email Signing	Supported
Email Encryption	Supported
OCSP Signing	Supported

Certificate Validation

PrimeLink® Copier/Printer support certificate validation with configurable checks for OSCP and CRL.

Validation checks include:

- Validation of certificate path
- Certificate expiration
- Validation of trusted CA
- Signature validation

Email Signing and Encryption using S/MIME

S/MIME (Secure/Multipurpose Internet Mail Extensions) provides Authentication, Message integrity, Non-repudiation, and encryption of email.

Email S/MIME	
Versions	v3
Digest	SHA1, SHA256, SHA384, SHA512 *MD5 receives S/MIME signed e-mail only, S/MIME signed e-mail send cannot be selected.
Encryption	3DES, RC2-40/64/128, AES128, AES192, AES256

SNMPv3

SNMPv3 is the current standard version of SNMP defined by the Internet Engineering Task Force (IETF). It provides three important security features:

- Message integrity to ensure that a packet has not been tampered with in transit
- Authentication to verify that the message is from a valid source
- Encryption of packets to prevent unauthorized access

SNMPv3	
Digest	Supported - MD5/SHA-1
Encryption	Supported - DES/AES128

Cisco Identity Services Engine (ISE)

Cisco ISE is an intelligent security policy enforcement platform that mitigates security risks by providing a complete view of which users and what products are being connected across the entire network infrastructure. It also provides control over what users can access your network and where they can go. Cisco's ISE includes over 200 Xerox product profiles that are ready for security policy enablement. This allows ISE to automatically detect Xerox products in your network. Xerox products are organized in Cisco ISE under product families, such as Primelink® Copier/Printer products, enabling Cisco ISE to automatically detect and profile new Xerox products from the day they are released. Customers who use Cisco ISE find that including Xerox products in their security policies is simpler and requires minimal effort.

Cisco ISE Profiling Services provides dynamic detection and classification of endpoints connected to the network. ISE collects various attributes for each network endpoint to build an endpoint database. The classification process matches the collected attributes to prebuilt or user-defined conditions, which are then correlated to an extensive library of product profiles. These profiles include a wide range of product types, including tablets, smartphones, cameras, desktop operating systems (for example, Windows®, Mac OS® X, Linux® and others), and workgroup systems such as Xerox printers and MFPs.

Once classified, endpoints can be authorized to the network and granted access based on their profile signature. For example, guests to your network will have different level of access to printers and other end points in your network. As an example, you and your employees can get full printer

access when accessing the network from a corporate workstation but be granted limited printer access when accessing the network from your personal Apple® iPhone®.

Cisco ISE allows you to deploy the following controls and monitoring of Xerox products:

- Automatically provision and grant network access rights to printers and MFPs to prevent inappropriate access (including automatically tracking new printing products connecting to the network):
  - Block non-printers from connecting on ports assigned to printers
  - Prevent impersonation (aka spoofing) of a printer/MFP
  - Automatically prevent connection of non-approved print products
  - Smart rules-based policies to govern user interaction with network printing products
- Provide simplified implementation of security policies for printers and MFPs by:
  - Providing real time policy violation alerts and logging
  - Enforcing network segmentation policy
  - Isolating the printing products to prevent general access to printers and MFPs in restricted areas
- Automated access to policy enforcement
  - Provide extensive reporting of printing product network activity

Network Access Control	
Cisco ISE	Supported

Contextual Endpoint Connection Management

Traditionally network connection management has been limited to managing endpoints by IP address and use of VLANs and firewalls. This is effective, but highly complex to manage for every endpoint on a network. Managing, maintaining, and reviewing the ACLs (and the necessary change management and audit processes to support them) quickly become prohibitively expensive. It also lacks the ability to manage endpoints contextually.

Connectivity of PrimeLink® Copier/Printer devices can be fully managed contextually by Cisco TrustSec. TrustSec uses Security Group Tags (SGT) that are associated with an endpoint's user, device, and location attributes. SG-ACLs can also block unwanted traffic so that malicious reconnaissance activities and even remote exploitation from malware can be effectively prevented.

FIPS140-2 Compliance Validation

When enabled, the product will validate its current configuration to identify cryptographic modules in use. Modules which are not FIPS 140-2 (Level 1) compliant will be reported.

PrimeLink® products include FIPS compliant algorithms of Kerberos, however an exception can be approved to run these in non-FIPS compliant mode when configured for non-FIPS algorithms.

PrimeLink® products use encryption algorithms for Kerberos, SMB, and PDF Direct Print Service that are not approved by FIPS140-2. They can however operate in FIPS140-2 approved Mode in order to maintain compatibility with conventional products after an exception is approved by a system administrator. They do not use FIPS compliant algorithms when in this configuration.

Additional Network Security Controls

Endpoint Firewall Options

Firewall	IP Whitelisting
Stateful Firewall	Not Supported
IP Whitelist	Supported

IP Whitelisting (IP Address Filtering)

PrimeLink® products support IP Whitelisting only.

When enabled all traffic is prohibited regardless of interface (wired/wireless) unless enabled by IP filter rule. IPv4 and IPv6 are enabled separately. If IP Filter and IPsec are both enabled, IPsec is evaluated first. Up to 25 addresses can be enabled for IPv4 and an additional 25 for IPv6. Addresses include IP and subnet allowing individual system or subnets to be enabled. A system administrator can disable this feature using the embedded web server.

Stateful Firewall (Advanced IP Filtering)

PrimeLink® Copier/Printer products do not support stateful packet inspection.

5. Device Security: BIOS, Firmware, OS, Runtime, and Operational Security Controls

PrimeLink® products have robust security features that are designed to protect the system from a wide range of threats. Below is a summary of some of the key security controls. The Marking Engines for the product contains the μ-iTRON 4.0 operating system. These systems have no networking capability. The Controller uses the Linux operating system. Typical Unix functions such as rsh, telnet and finger do not operate under the OS. User must note that the Linux operating system is not accessible. All logons to the product are to application software and not to the Linux OS. Hence the Linux OS is not accessible to the user.

Pre-Boot BIOS Protection

BIOS

- The BIOS is inaccessible and cannot be cleared or reset.
- The BIOS can only be modified by a firmware update, which is digitally signed.
- BIOS will fail secure, locking the system if integrity is compromised.

Embedded Encryption

- Configuration Settings (including security settings) and User Data are encrypted by AES.
- Each device is encrypted using its own unique key.

Boot Process Integrity

Firmware Integrity & Verification

- Firmware is digitally signed.
- Firmware is verified against a whitelist using cryptographic hashing.

Event Monitoring & Logging

- The Audit Log feature records security-related events.

Continuous Operational Security

Firmware and Diagnostic Security Controls

- Firmware installation controls limit who can install firmware and from where.
- Customer defined service technician (CSE) restrictions add an additional layer of protection to prevent unauthorized access and/or modification of PrimeLink® products.
- Continuous logging

Fail Secure Vs Fail Safe

PrimeLink® products are designed to fail secure.

When a security control is compromised, the control is no longer trustworthy, and a system is at risk of further compromise. In such a scenario, security products may either fail safe [open] or fail secure [closed].

An example from physical security is a door. If power is lost the door may either:

- Unlock and 'fail safe' to an open state (likely for safety reasons such as in a public building).
- Lock and 'fail secure' for security reasons (such as a bank vault).

Pre-Boot Security

BIOS

PrimeLink® Copier/Printer products is embedded and cannot be accessed directly. Unlike devices such as Desktop and Laptop computers that have a BIOS that can be accessed via a keystroke on startup, the BIOS of PrimeLink® products it's not accessible.

Many devices can be cleared to factory defaults (including passwords and security settings) by depressing a reset button using a paperclip or similar method. For security reasons, PrimeLink® products do not offer such a method to clear or reset the BIOS. (Note that configuration settings may be reset to factory defaults by an authorized administrator, however this does not impact BIOS settings).

BIOS updates are not applied by device firmware updates. Firmware is protected from tampering by use of digital signatures (discussed later in this section).

The BIOS is designed to fail secure. An integrity check is performed immediately when power is applied. If verification is successful, the system proceeds with OS kernel boot. If the integrity check fails, the system will fail secure.

Embedded Encryption

AES encryption is used to protect the system, user data, and configuration (including security settings) from being retrieved or modified. Each device uses its own unique key that is securely generated. Encryption is enabled by default. Media encryption and sanitization are discussed in Section 3: User Data Protection.

Boot Process Security

Firmware Integrity

Unlike open operating systems such as servers and user workstations in which software may be installed by users, Xerox products are based on embedded systems and the contents are managed by Xerox. The only means of modifying the contents of a device is by applying a firmware update package.

Firmware updates use a special format and each firmware update is digitally signed to protect the integrity of the contents. Firmware that is corrupt or has been illicitly modified will be rejected. **This security control cannot be disabled.**

PrimeLink® products include a built-in firmware software validation. This is a file integrity monitor that compares the security hashes of currently installed firmware to a secured whitelist that was installed when the signed firmware was installed.

Event Monitoring and Logging

Audit Log

The Audit Log feature records security-related events. The Audit Log contains the following information:

Field	Description
Index	A unique value that identifies the event.
Date	The date that the event happened in mm/dd/yy format.
Time	The time that the event happened in hh:mm:ss format.
ID	The type of event. The number corresponds to a unique description.
Description	An abbreviated description of the type of event.
Additional Details	Columns 6–10 list other information about the event, such as: Identity: User Name, Job Name, Computer Name, Printer Name, Folder Name, or Accounting Account ID display when Network Accounting is enabled. Completion Status Image Overwrite Status: The status of overwrites completed on each job. Immediate Image must be enabled.

Events targeted for audit log are recorded to the NVRAM with timestamps. When the number of events reaches 50, they are stored in the hard disk of the product. Up to 15,000 events can be stored in the hard disk. When the number of events exceeds 15,000, audit log files will be deleted in order of timestamp, and then new events will be recorded.

The audit log be exported at any time by a user with administrative privileges. Note that as a security precaution, audit log settings and data can only be accessed via HTTPS.

Operational Security

Firmware Restrictions

The list below describes supported firmware delivery methods and applicable access controls.

- **Local Firmware Upgrade via USB port**:
  Xerox service technicians can update product firmware using a USB port and specially configured USB thumb drive. This ability can be restricted by enabling the Customer Service Engineer Restriction feature which will require entry of a unique, customer designated password in order to accept the update.
- **Network Firmware Update**:
  Product system administrators can update product firmware using the Embedded Web Server. The ability to apply a firmware update is restricted to roles with system administrator or Xerox service permissions. Firmware updates can be disabled by a system administrator.
- **Xerox Remote Services Firmware Update**:
  Xerox Remote Services can update product firmware securely over the internet using HTTPS. This feature can be disabled, scheduled, and includes optional email alerts for system administrators.

The programs stored in the Flash ROM listed below are downloadable from external sources.

- Controller
- Marking Engine
- Scanner
- Document Feeder
- Finisher (Option for processing printed paper. No description on Finisher is provided in this document because user's image data will not be stored in it.)
- High capacity feeder (No description on High capacity feeder is provided in this document because user's image data will not be stored in it.)
- High capacity stacker (No description on high capacity stacker is provided in this document because user's image data will not be stored in it.)
- Interface Module (No description on interface module is provided in this document because user's image data will not be stored in it.)
  - This program-downloading function can be disabled by a system administrator from the local UI.
  - The header part of file is using software to identify whether the download file is legitimate.

Service Technician (CSE) Access Restriction

The CSE (Customer Service Engineer) Access Restriction allows customers to create an additional password that is independent of existing administrator passwords. This password must be supplied to allow service of the product. This password is not accessible to Xerox support and cannot be reset by Xerox service personnel.

Additional Service Details

Xerox products are serviced by a tool referred to as the Portable Service Workstation (PWS). Only Xerox authorized service technicians are granted access to the PWS. Customer documents or files cannot be accessed during a diagnostic session, nor are network servers accessible through this port. If a network connection is required while servicing a Xerox device, service technicians will remove the device from any connected networks. The technician will then connect directly to the device using an Ethernet cable, creating a physically secure and isolated network during service operations.

Backup and Restore (Cloning)

Certain system settings can be captured in a 'clone' file that may be applied to other systems that are the same model. Clone files are encoded but not encrypted and have the potential to contain sensitive information depending on which product feature setting is selected. Access to both create and apply a clone file can be restricted using role-based access controls. Clone files can only be created and applied through the Embedded Web Server.

EIP Applications

Xerox products can offer additional functionality through the Xerox Extensible Interface Platform® (EIP). Third party vendors can create Apps that extend the functionality of a product. Xerox signs EIP applications that are developed by Xerox or Xerox partners. Products can be configured to prevent installation of unauthorized EIP applications.

XCP (eXtensible Customizable Platform)

PrimeLink® products offer additional functionality through the eXtensible Customizable Platform (XCP) plug-in interface. Plug-ins can alter current functionality and add new functionality that may impact the security of the product. XCP Plug-ins are signed and encrypted by Xerox; products can be configured to reject unsigned plug-ins. XCP plug-ins are used to support USB peripherals and alternative login methods (such as Smart Card login). The XCP plug-in feature is disabled by default and must be manually enabled by a system administrator using the embedded web server

6. Configuration and Security Policy Management Solutions

Xerox Device Manager and Xerox® CentreWare® Web (available as a free download) centrally manage Xerox Devices.

For details please visit Xerox.com or speak with a Xerox representative

(This page intentionally left blank.)

7. Identification, Authentication, and Authorization

PrimeLink® Copier/Printer products offer a range of authentication and authorization options to support various environments.

Single Factor authentication is supported locally on the product or via external network authentication servers (e.g., LDAP, Kerberos, ADS). Multi Factor authentication is supported by addition of card reader hardware. (Where ease of access is desired, open access and simple user identification modes also exist, however these are not recommended for secure environments.)

In all modes, product administrator accounts always require authentication. This cannot be disabled.

PrimeLink® Copier/Printer products support unique roles for Admin, CSE, and Registered Users.

Authentication

PrimeLink® Copier/Printer devices support the following authentication mode:

- Local Authentication
- Network Authentication
- Smart Card Authentication (CAC, PIV, SIPR, .Net)
- Convenience Authentication
- Service Technician Authentication

Local Authentication

The local user database stores user credential information. The printer uses this information for local authentication and authorization, and for Xerox ® Standard Accounting. When you configure local authentication, the printer checks the credentials that a user provides against the information in the user database. When you configure local authorization, the printer checks the user database to determine which features the user is allowed access. Each device has a unique default administrator password which should be changed as soon as possible along with enabling recommended security features to secure the system.

Note: User names and passwords stored in the user database are not transmitted over the network

Password Policy

The following password attributes can be configured:

Password Policy	
Minimum Length	1
Maximum Length	63
Password cannot contain User Name	Supported
Password complexity options (in addition to alphabetic characters)	Require a number

Network Authentication

When configured for network authentication, user credentials are validated by a remote authentication server.

Network Authentication Providers	
Kerberos (Microsoft Active Directory)	Supported
Kerberos (MIT)	Supported
SMB NTLM Versions Supported	NTLMv2
LDAP Versions Supported	Version 3 (including TLS 1.2)

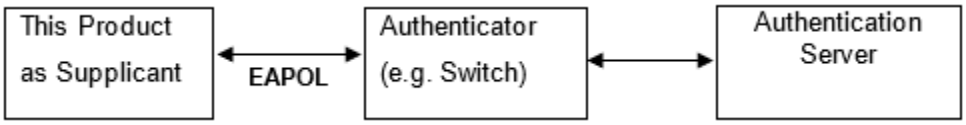
The product provides the device authentication feature that is required for network connection to LAN port where access is controlled.

The following device authentication method is provided.

Device Authentication Method	Operation
802.1X	Wired 802.1X authentication is supported. When the product is activated using the User ID and password set for the product, authentication to the switch device starts in order to connect to the LAN port.

802.1x Authentication

In 802.1X authentication, when the product is connected to the LAN port of Authenticator such as the switch as shown below, the Authentication server authenticates the product, and the Authenticator controls access of the LAN port according to the authentication result.
The product starts authentication processing at startup when the startup settings for 802.1X authentication are enabled.



Of the authentication methods in 802.1X Authentication, the product supports the following.

802.1X Authentication Method	Operation
PEAP/MS-CHAPv2	Performs authentication in the TLS-encrypted channel established between the product and the Authentication server, using the following information: ID information in plain text. Password encrypted in MN-CHAPv2 method.
EAP-TLS	Performs authentication in the SSL-encrypted channel established between the product and the authentication server, using the SSL client certificate of the product. ID information and password are not used.
EAP-TTLS/PAP	Performs authentication in the SSL-encrypted channel established between the product and the Authentication server, using the following information: - ID information in plain text.

802.1X Authentication Method	Operation
	- Password in plain text.
EAP-TTLS/CHAP	Performs authentication in the SSL-encrypted channel established between the product and the Authentication server, using the following information: - ID information in plain text. - Password encrypted in CHAP
EAP-TTLS/MS-CHAPv2	Performs authentication in the SSL-encrypted channel established between the product and the Authentication server, using the following information: - ID information in plain text. - Password encrypted in MS-CHAPv2

Smart Card Authentication

Two-factor security – Smart Card plus User Name/Password combination. Requires optional card reader hardware and software plugin. Authentication is handled by a remote server. Supported remote authentication methods include Kerberos, SMB and LDAP.

Smart Card authentication is considered very secure due to the nature of the Smart Card architecture and potential levels of encryption of data on the card itself.

Support for the SIPR network is provided using the XCP Plug-in architecture and a Smart Card authentication solution created by 90meter under contract for Xerox.

Details regarding 90meter can be found online here: https://www.90meter.com/

Other Smart Card authentication solutions are offered including support for CAC/PIV and .NET compatible cards leveraging XCP Plug-ins.

Smart Cards	
Common Access Card (CAC)	Supported
PIV / PIV II	Supported
Net (Gemalto .Net v1, Gemalto .Net v2)	Supported
Gemalto MD	(Not Currently Supported)

Xerox Secure Access

Convenience authentication offloads authentication to a third-party solution which may offer more or less security than native security implementations. Users swipe a pre-programmed identification card or key fob to access the device.

For example, employees may be issued key fobs for access to facilities. Convenience mode may be configured to allow an employee to authenticate using their fob or require the fob in a multi-factor manor. The level of security provided is dependent upon the chosen implementation.

Some examples of third party convenience authentication providers include:

- Pharos print management solutions: https://pharos.com/
- YSoft SafeQ: https://www.ysoft.com/en

Contact your Xerox sales representative for details and other options.

Authorization (Role Based Access Controls)

PrimeLink® Copier/Printer products do not offer granular control of user permissions. Users can be assigned to pre-defined roles or customers may design highly flexible custom permissions. A user must be authenticated before being authorized to use the services of the product. Authorization ACLs (Access Control Lists) are stored in the local user database. Authorization privileges (referred to as permissions) can be assigned on a per user or group basis.

Please note that Xerox products are designed to be customizable and support various workflows as well as security needs. User permissions include security-related permissions and non-security related workflow permissions (e.g., walkup user options, copy, scan, paper selection, etc.). Only security-related permissions are discussed here.

Remote Access

Without RBAC permissions defined basic information such as Model, Serial number, and Software Version can be viewed by unauthenticated users. This can be disabled by restricting access to the device website pages for non-logged-in users.

By default, users are allowed to view basic status and support related information, however they are restricted from accessing device configuration settings. Permission to view this information can be disallowed.

Local Access

Without RBAC permissions defined basic information such as Model, Serial number, Software Version, IP address, and Host Name can be viewed without authentication. This can be disabled by disallowing access to device settings for unauthenticated.

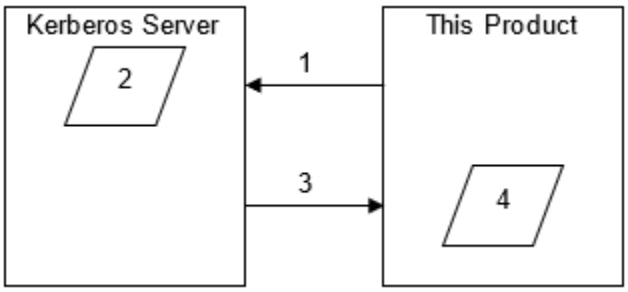
By default, users are allowed to access the local interface, however they are restricted from accessing device configuration settings. Roles can be configured to allow granular access to applications, services, and tools. Users can be also restricted from accessing the local interface completely.

To access the product from the Local User Interface, authentication is required per the authentication method as shown below.

Authentication Method	Operation
No authentication	No authentication is required for general users.
Authentication on the product (without password)	When Authentication on the product is in enabled state, the User ID (PIN) is required for general users.
Authentication on the product (with password)	When Authentication on the product is in enabled state, the User ID and 4 to 12 characters password are required for general users.
External authentication	When external authentication is in enabled state, general users access external authentication function for local access such as for copy / scan. The following are the external authentication functions, and input of the User ID and password is required. 1) Kerberos authentication 2) LDAP authentication 3) SMB authentication Description of each authentication function follows.

Kerberos authentication can avoid password interception and replay attack by using Kerberos protocol. The authentication steps using Kerberos are:

1. A user enters the User ID and password from the Local User Interface on the product. The product encrypts the entered User ID and time stamp into authentication identifier using the password, and sends the authentication identifier to the Kerberos server.
2. The Kerberos server decrypts the authentication identifier using the stored user password, to authenticate and obtain the included time stamp. Then, the server checks the validity of the time stamp. When the time stamp is correct, the Kerberos server creates a Session Key and encrypts it using the user password.
3. The Kerberos server sends back the Initial Ticket that includes the encrypted Session Key to the product.
4. The product decrypts the Session Key included in the Initial Ticket that the product received, using the entered password. When the decryption completes in success, the user is authenticated.



In SMB authentication, through the negotiation with SMB authentication server, the appropriate authentication method is determined by examining from the highest level (i.e. NVLMv2). User selects pre-registered SMB domain name, and executes authentication by entering User ID and password.

SMB Authentication Method	Operation
NTLMv2 authentication	This is supported by Windows OS of WinNT-SP4 and later. By challenge/response, authentication is executed without sending password directly to network. The authentication level is higher than NTLMv1 authentication.
NTLMv1 authentication	This is supported by Windows OS of WinNT and later. By challenge/response, authentication is executed without sending password directly to network.
LM authentication	This is the authentication method adopted on LAN Manager. This is supported by Windows OS of Win95 and later. By challenge/response, authentication is executed without sending password directly to network. This is more vulnerable than NVLMv1 authentication.
PLAIN authentication	This is an authentication using plain text.

The following modes are supported as the authentication methods in LDAP authentication. Since authentication on LDAP server is executed through Simple Bind using plain text, there is a risk of interception of User ID and password on network when LDAP protocol (port 389) is used. When LDAP server supports LDAPS protocol that uses secure channel using TLS, interception of User ID and password on network can be avoided by using LDAPS.

LDAP Authentication Mode	Operation
Direct Login	Executes authentication (ldap_bind) on LDAP server using User ID and password entered by user on local UI.
Search & Login	Searches user's Login ID from LDAP server using the User ID entered by user on local UI as a specific attribute (such as ID number), and executes authentication (ldap_bind) on LDAP server using the searched user's Login ID and entered password.

In Secure Access Authentication, since a secure channel communication using Secure Access Authentication server and TLS is performed, interception of User ID and password on network can be avoided. Communication between Secure Access card reader and Secure Access Authentication server is encrypted by the supplier's unique code (e.g. Equitrac Corporation).

Sequence of authentication performed by inserting card to Secure Access card reader is as follows:

1. The information on the card inserted to Secure Access card reader is read and notified to the Secure Access authentication server. Then, the request for password confirmation is notified to the product from the Secure Access authentication server. When the User ID is entered from the local UI, the User ID is notified to the Secure Access authentication server from the product, and the request for password confirmation is notified to the product from the Secure Access authentication server.
2. The product sends the entered password to the Secure Access Authentication server, and the Secure Access Authentication server sends back the validation result to the product.

To access various features on the product from the remote, authentication is required as follows:

Feature	Operation
Mailbox	To access the Mailbox from the Scanner Driver / Embedded Web Services, Mailbox number and password are required.
Embedded Web Service	With “Authentication on the product (with password)” selected, the User ID and password are required even to access the product from the browser.
Print Auditron	With the Print Auditron enabled, the User ID and password are required to be set on the Printer Driver.

(This page intentionally left blank.)

8. 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/

(This page intentionally left blank.)

9. Appendix A: Product Security Profiles

This appendix describes specific details of each PrimeLink® Copier/Printer product.

PrimeLink® B9100/9110/9125/9136 Copier/Printers

Physical Overview

1. Bypass Tray
2. User Interface
3. Duplex Automatic Document Feeder (Not Included)
4. Offset Catch Tray
5. Dry Ink/Toner Waste Bottle Door
6. Front Door
7. Trays 1 - 4
8. Dry Ink/Toner Cover

Security Related Interfaces

Security Related Interfaces	
Ethernet	10/100/1000 MB Ethernet interface.
Rear USB 3.0 (Type B)	USB target connector used for printing. **Note**: This port cannot be disabled completely by a system administrator.
Front Panel Optional USB2.0 (Type A) port(s)	Users may insert a USB thumb drive to print from or store scanned files to. (Physical security of this information is the responsibility of the user or operator.) Note that features that leverage USB ports (such as Scan To USB) can be disabled independently or restricted using role based access controls. Firmware upgrades may be applied using this port. Connection of optional equipment such as CAC readers. **Note**: This port cannot be disabled completely by a system administrator.
Physical USB Ports	Physical USB ports cannot be disabled.

Encryption and Overwrite

Encryption and Overwrite	
Encryption	AES-256
TPM Chip	Currently Supported
Media Sanitization	Immediate and On-Demand Image Overwrite.

Controller Non-Volatile Storage

	IC	HDD	SSD	SD Card
Contains User Data (e.g., Print, Scan, Fax)	N/A	Yes	N/A	N/A
Encryption Support	N/A	Configurable	N/A	N/A
NIST 800-171 88 rev1 Overwrite Support	N/A	No	N/A	N/A
Contains Configuration Settings	N/A	On Demand	N/A	N/A

Note: Configuration settings may be erased by the reset to factory defaults feature.

IC- Integrated Circuit, soldered to circuit board
HDD- Magnetic Hard Disk Drive
SSD- Solid State Disk
SD Card- Secure Digital Card

Controller Hard Disk Table

Drive / Partition	Removable Y/N	Size	User Modifiable Y/N	Function	Process to Clear
ide0/a	N	3726MB	N	Resources data storage	At the deletion of data
ide0/b	N	5588MB	N	Print data temporary storage	At the completion of job
ide0/c	N	14902MB	N	Private/Mailbox storage	At the deletion of data
ide0/d	N	3726MB	N	PDL/mail data temporary storage	At the completion of job
ide0/e	N	14902MB	N	Copy data temporary storage	At the completion of job
ide0/f	N	1863MB	N	Scan data temporary storage	At the completion of job
ide0/g	N	2794MB	N	Print data temporary storage	At the completion of job
ide0/h	N	6144MB	N	Management data storage	At the deletion of data
ide0/i	N	11176MB	N	Scan-to-URL scan data storage	At the completion of receiving data
ide0/j	N	40960MB	N	Image Log storage	At the completion of transferring image log to server
ide0/l	N	3726MB	N	XCP custom plug-in data storage	At the deletion of plug-in
ide0/o	N	1863MB	N	Debug data storage	None
ide0/p	N	3276MB	N	Firmware backup storage	Never
ide0/z	N	1230MB	N	Security data storage	None

Additional Information:

- If Disk Encryption is ON, all partitions are encrypted.
- If Disk Overwrite is ON, all files are sanitized when it is deleted by NSA recommended method.
- ide0/a: Resources are font, form/logo, SMB folder (config.txt, driver) and Job Template.
- ide0/b: EPC print data which are decomposed and temporarily stored on this partition.
- ide0/c: Private/Mailbox stores scan data, security print data, and proof print data.
- ide0/d: PDL and mail data are received and temporarily stored on this partition.
- ide0/e: EPC copy data are temporarily stored on this partition.
- ide0/f: Scan data are temporarily stored on this partition when Scan To Server, Scan To PC, or Scan To Email is used.

- ide0/g: PDL data are received and temporarily stored on this partition.
- ide0/h: Management data are authentication database, job log, audit log, certificate, address book, development log.
- ide0/i: Scan data stored by Scan to URL process remain on this partition until user retrieves data.

  Xerox® B9100/9110/9125/9136 Copier/Printer does not support the Image Log feature and the partition is not used
- ide0/j: Image Log remains on this partition until Image Log is transferred to server.

  Xerox® B9100/9110/9125/9136 Copier/Printer does not support the Image Log feature and the partition is not used.
- ide0/p: Firmware of previous and current are stored as backup when firmware is upgraded. Data remain until next firmware upgrade.

Controller Volatile Memory Table

Size	Type (SRAM, DRAM, etc)	Function or Use	User Modifiable (Y/N)	Process to Clear	Volatile
4GB (512M x 8bit)x 4	SDRAM (system memory DIMM)	Temporary storage of program, and work area	No	SDRAM is erased when a main switch is turned off.	Yes
8Mbit (1M x 8bit)	Battery-backed SRAM (ESS PWBA)	Permanent storage of machine setting data/job log data. User image data are not stored.	No	SRAM is not erased when a main switch is turned off. Not customer alterable.	Yes
2GB (256M x 16bit) x4	SDRAM (page memory)	Temporary storage of work area	No	SDRAM is erased when a main switch is turned off.	Yes
2GB (128M x 16bit)	SDRAM (Fax PWBA)	Temporary storage of work area	No	SDRAM is erased when a main switch is turned off.	Yes
SDRAM (Fax PWBA) is only available on B9100					

Additional Information: The controller operating system memory manager allocates memory dynamically between OS, running processes, and temporary data which includes jobs in process. When a job is complete, the memory pages in use are freed and reallocated as required by the OS.

Controller Non-Volatile Memory Table

Size	Type (SRAM, DRAM, etc)	Function or Use	User Modifiable (Y/N)	Process to Clear	Volatile
1Mbit (256K x 8bit)	Flash (MCU PWBA)	Permanent storage of Program. User image data are not stored.	No	Not customer alterable	No
8MB 64Mbit	Flash (ESS PWBA)	Permanent storage of program/font data. User image data are not stored.	No	Not customer alterable	No
8Kbit	SEEPROM (BP PWBA	Permanent storage of machine setting data. User image data are not stored.	No	Not customer alterable	No
256Kbit	EEPROM (DADF PWBA	Permanent storage of DADF configuration code. User image data are not stored.	No	Not customer alterable	No
16Kbit	EEPROM (IIT PWBA)	Permanent storage of IIT configuration code. User image data are not stored.	No	Not customer alterable	No
16Kbit	EEPROM (2nd IIT DCDC PWBA)	Permanent storage of 2nd IIT configuration code. User image data are not stored	No	Not customer alterable	No
256Kbyte	Flash with 24Kbyte of data RAM (DADF PWBA)	Permanent storage of DADF executable code. User image data are not stored.	No	Not customer alterable	No
16Mbit	Flash (Fax PWBA)	Permanent storage of Fax executable code.	No	Not customer alterable	No
Flash (Fax PWBA) is only available on B9100					

Additional Information: The controller operating system memory manager allocates memory dynamically between OS, running processes, and temporary data which includes jobs in process. When a job is complete, the memory pages in use are freed and reallocated as required by the OS.

10. Appendix B: Security Events

Security Events

ID	Event	Description
101	Started normally (cold boot)	
101	Started normally (warm boot)	
101	Booting due to forced LOG initialization	
101	Booting due to forced HDD initialization	
101	Shutdown requested	
101	Image Overwriting started	Completion: (“Success” / “Failed”) Scheduled On Demand
101	Image Overwriting finished	Completion: (“Success” / “Failed”)
101	Self-Test	Completion: (“Success” / “Failed”) CheckSum of ROM image 1 CheckSum of ROM image 2
201	Login	User name Completion: (“Success” / “Failed Invalid User ID” / “Failed Invalid Password” / “Failed”) Host Name or IP Address Method: (“Local” / “Remote” / “Convenience” , “Custom”) Role: (“System Administrator” / “Customer Engineer” / “Casual Operator”)
201	Logout	User name Completion: (“Success” / “Failed”)
201	Locked System Administrator Authentication	Count of Remaining Authentication Failures
201	Detected Continuous Authentication Fail	User name Protocol: (“SNMPv3” / “EWS”) Count of Remaining Authentication Failures
301	Audit Log	User name Completion: (“Enabled” / “Disabled”)

ID	Event	Description
401	Print	User name Completion: (“Completed” / “Completed with Warnings” / “Cancelled by User”/ “Cancelled by Shutdown”/ “Aborted”/ “Unknown”) Root Job UUID Relation: (“Related” / “Owned”) Job Accounting ID Action Details Host Name or IP Address File Name
401	Copy	Action Details
401	Scan	Encrypted, Signed, Destination Name, Sender Name
401	Fax	Action Details, Destination Name, Sender Name
401	Mailbox	Action Details
401	Print Reports	
401	Job Flow Service	
401	Jobs other than the above	
501	Adjust Date and Time	Completion: (“Success” / “Failed”)
501	Add User	User name User Role
501	Edit User	User name User Role ID Password CardID Name Permission Role ICCardID Other
501	Delete User	User Name
501	Create Mailbox	Host Name or IP Address Box Number
501	Delete Mailbox	
501	Switch Authentication Mode	Completion: (“Success”) New Setting Previous Setting

ID	Event	Description
501	Change Security Setting	Authentication Accounting Image Overwrite HDD Encryption SSL S/MIME IPSEC SNMPv3 802.1x Certificate Verify Mode Maintainer Password SmartCard FIPS140 Self Test Auto Clear Timer Service Rep. Restricted Operation Print Reports Button External Code Integrity Check Authorization NFC
501	View Security Setting	Access Method: (“Local” / “EWS”) Host Name or IP Address
501	Change Contract Type	User name Completion: (“Success” / “Failed” / “Aborted”)
501	Change Geographic Region	
501	Enter Activation Code	Completion: (“Success”)
501	Change Job Setting	Completion: (“Success”) Function Name: (“Delay Print” / “Private Print”)
501	Change Billing Impression Mode	Completion: (“Success” / “Failed”) Designated Mode (“A3 Mode” / “A4 Mode”) Billing Meter Values
601	Import Certificate	User name Completion: (“Success” / “Failed”) Category: (“RootCA” / “DeviceEE” / “SSCEE”) Key Size Issuer DN Serial Number
601	Delete Certificate	
601	Add Address Entry	Host Name or IP Address Registration Number
601	Delete Address Entry	
601	Edit Address Entry	
601	Import Address Book	Host Name or IP Address

ID	Event	Description
601	Export Address Book	
601	Clear Address Book	Host Name or IP Address
601	Export Audit Log	
601	Install Custom Service	Completion: (“Failed”) Host Name or IP Address Custom Service Name
601	Install Embedded Plug-in	Host Name or IP Address Plugin File Name
601	Export Cloning Data	Completion: (“Success” / “Failed”) Category: (“Apps” / “Contacts” / “Connectivity”/ “Permissions”/ “System”)
601	Import Cloning Data	
701	Important Parts	Completion: (“Replaced”)
701	Hard Disk	Completion: (“Replaced” / “Installed” / “Removed”)
701	ROM Version Change	
801	Communication Reliability	When Reliability Communication Error is detected at the periodical check.