Security Guide

Xerox® VersaLink® C7120/C7125/C7130 Multifunction Products

Xerox® VersaLink® B7125/B7130/B7135 Printers

xerox™

Document Version: 1.0 (December 2021).

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

Target Audience

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

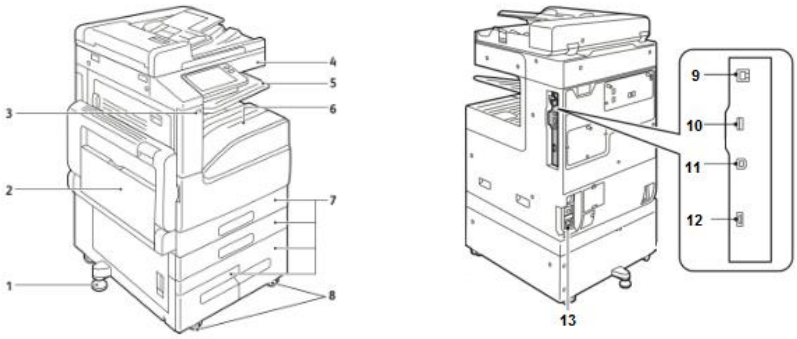
Disclaimer

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

2. Product Description

Physical Components

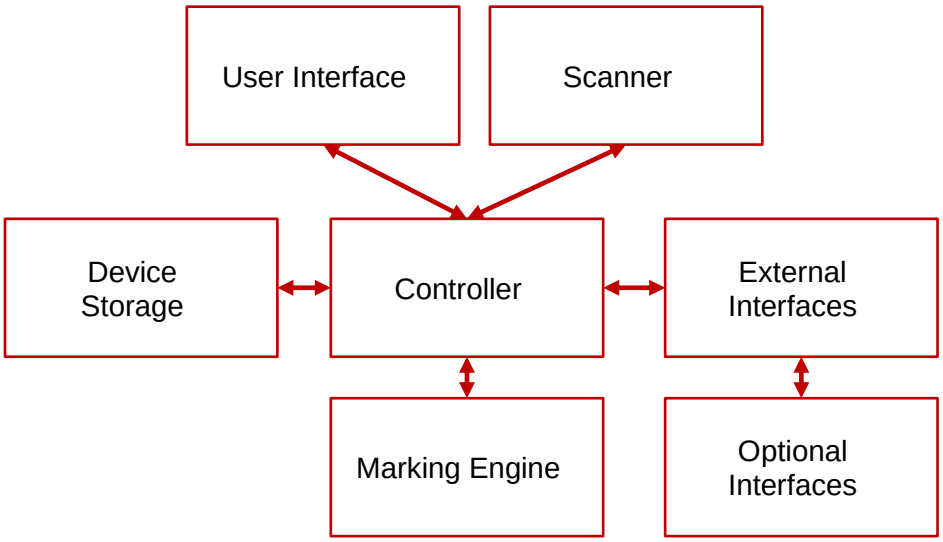
VersaLink® products consist of an input document handler and scanner, marking engine, controller, and user interface. A typical configuration is depicted below. Please note that options including finishers, paper trays, document handers, etc. may vary configuration, however, they are not relevant to security and are not discussed.



1. **Stabilizer.**
2. **Bypass paper feed tray.**
3. **Front USB Port(s)***
4. **Touch screen user interface.**
5. **Upper paper tray.**
6. **Lower paper tray.**
7. **Paper feed trays.**
8. **Caster wheels.**
9. **Rear USB Port(s)***
10. **Optional Wi-Fi dongle port***
11. **RJ45 Ethernet connection***
12. **Service port (May require disassembly to access).**
13. **AC Power**
14. ***Denotes a security related component**

Architecture

VersaLink® 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 7 Identification, Authentication, and Authorization

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.

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, xerographics, 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.

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. VersaLink® 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.

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 DOC, 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 NFC or 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 optional 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

VersaLink® products accept an optional wireless module via a proprietary port.

NEAR FIELD COMMUNICATIONS (NFC) READER

The system supports an installable RFID reader for authentication and convenience in certain configurations. VersaLink® products accept the RFID reader via USB on the front of the product. This communication cannot write or change any settings on the system. The data exchanged is not encrypted and may include information including system network status, IP address and product location. NFC functionality can be disabled using the embedded web server of the product. NFC functionality requires a software plugin that can be obtained from Xerox sales and support. NFC functionality is supported via optional touch screen user interface or optional dedicated NFC USB dongle.

Information shared over NFC includes: IPv4 Address, IPv6 Address, MAC Address, UUID (a unique identifier on the NFC client), and Fully qualified domain name

SMART CARD – CAC/PIV

All VersaLink® products support CAC/PIV login by enabling the VersaLink® 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 VersaLink® 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.

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)

Some models include a Trusted Platform Module (TPM). The TPM is compliant with ISO/IEC 11889, the international standard for a secure crypto processor, dedicated to secure cryptographic keys. The TPM is used to securely hold the product storage encryption key. Please refer to Appendix A: Product Security Profiles for model specific information.

MEDIA SANITIZATION (IMAGE OVERWRITE)

VersaLink® products 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-800-88 “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.

Data in Transit

This section focuses on the protection of 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.

ENCRYPTED FIRMWARE

For the newest VersaLink® products including the Xerox® VersaLink® C7120/C7125/C7130 and Xerox® VersaLink® B7125/B7130/B7135, all versions of firmware are encrypted.

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.
Xerox Print Stream Encryption	The Xerox Global Print Driver® supports document encryption when submitting Secure Print jobs to enabled products. Simply check the box to Enable Encryption when adding the Passcode to the print job.

SCANNING TO NETWORK REPOSITORY, EMAIL, FAX SERVER (OUTBOUND USER DATA)

VersaLink® multifunction products 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	Encryption may be enabled on a Windows share. VersaLink® products do not currently support SMB encryption.
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.

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.

		VersaLink® Multifunction C7120/C7125/C7130	VersaLink® Printers B7125/B7130/B7135
Local Data Encryption (HDD, SDD, IC, SD Card)		AES-256	AES-256
Federal Information Protection Standard 140-2		Yes	Yes
Media Sanitization NIST 800-171 (Image Overwrite)		Models with magnetic HDD. See Appendix A: Product Security Profiles	Models with magnetic HDD. See Appendix A: Product Security Profiles
Print Submission			
	IPPS (TLS)	Supported	Supported
	HTTPS (TLS)	Supported	Supported
	Xerox Print Stream Encryption	(Not currently supported)	(Not currently supported)
Scan to Repository Server			
	HTTPS (TLS)	(Not currently supported)	(Not Applicable)
	SFTP (SSH)	(Not currently supported)	(Not Applicable)
	SMB (unencrypted)	v3	(Not Applicable)
	SMB (with share encryption enabled)	(Not currently supported)	(Not Applicable)
	HTTP (unencrypted)	(Not currently supported)	(Not Applicable)
	FTP (unencrypted)	(Not currently supported)	(Not Applicable)
Scan to Fax Server			
	HTTPS (TLS)	(Not currently supported)	(Not Applicable)
	SFTP (SSH)	(Not currently supported)	(Not Applicable)
	SMB (unencrypted)	v3	(Not Applicable)
	SMB (with share encryption enabled)	(Not currently supported)	(Not Applicable)
	S/MIME	Supported	(Not Applicable)
	HTTP (unencrypted)	(Not currently supported)	(Not Applicable)
	FTP (unencrypted)	(Not currently supported)	(Not Applicable)
	SMTP (unencrypted)	Supported	(Not Applicable)
Scan to Email			
	S/MIME	Supported	(Not Applicable)
	SMTP (unencrypted)	Supported	(Not Applicable)

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. **Cloud Services** 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
80 or 443	TCP	HTTP including: Web User Interface UPnP Discovery Web Services for Products (WSD) WebDAV
631 or 443	TCP	HTTP (IPP)
137	UDP	NETBIOS (Name Service)
138	UDP	NETBIOS (Datagram Service)
161	UDP	SNMP
427	TCP/UDP	SLP
445	TCP	CIFS
500 & 4500	UDP	IPSec
515	TCP	LPR
631	TCP	IPP
1900	UDP	SSDP
3702	TCP	WSD (Discovery)
5353	UDP	mDNS
9100	TCP	Raw IP (also known as JetDirect, AppSocket or PDL-datastream)
5909-5999	TCP	Remote Access to local display panel. Port is randomly selected and communications encrypted with TLS 1.2.
53202	TCP	WSD Transfer
53303	TCP	WSD Print
53404	TCP	WSD Scan

Network Encryption

IPSEC

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

		VersaLink® Multifunction C7120/C7125/C7130	VersaLink® Printers B7125/B7130/B7135
IPSec			
	Supported IP Versions	IPv4, IPv6	IPv4, IPv6
	Key exchange authentication method	Preshared Key & digital signature	Preshared Key & digital signature
	Transport Mode	Transport mode only	Transport mode only
	Security Protocol	ESP only	ESP only
	ESP Encryption Method	AES-CBC-128 AES-CBC-256 AES-GCM-128 AES-GCM-256	AES-CBC-128 AES-CBC-256 AES-GCM-128 AES-GCM-256
	ESP Authentication Methods	SHA1, SHA256, SHA384, SHA512	SHA1, SHA256, SHA384, SHA512
	DH Group	G14, G19, G20, G24	G14, G19, G20, G24

WIRELESS 802.11 WI-FI PROTECTED ACCESS (WPA)

Products equipped with WiFi support WPA2 Personal, WPA2 Enterprise, and Mixed Mode compliant with IEEE 802.11i. The wireless network adapters used in Xerox products are certified by the Wi-Fi Alliance.

		VersaLink® Multifunction C7120/C7125/C7130	VersaLink® Printers B7125/B7130/B7135
Wi-Fi (802.11)			
	No Encryption	Supported	Supported
	WEP	RC4	RC4
	WPA2 Personal (PSK)	CCMP (AES)	CCMP (AES)
	WPA2 Enterprise	PEAP MS-CHAPv2 EAP-TLS EAP-TTLS/PAP EAP-TTLS/CHAP EAP-TTLS/MS-CHAPv2	PEAP MS-CHAPv2 EAP-TLS EAP-TTLS/PAP EAP-TTLS/CHAP EAP-TTLS/MS-CHAPv2
	BSSID Roaming Restriction	(Not Currently Supported)	(Not Currently Supported)

TLS

These VersaLink® products support the latest version, TLS 1.3.

		VersaLink® Multifunction C7120/C7125/C7130	VersaLink® Printers B7125/B7130/B7135
TLS Versions Supported			
	Product Web Interface	1.3,1.2, 1.1, 1.0	1.3,1.2, 1.1, 1.0
	Product Web Services	1.3,1.2, 1.1, 1.0	1.3,1.2, 1.1, 1.0
	Product IPPS printing	1.3,1.2, 1.1, 1.0	1.3,1.2, 1.1, 1.0
	Remote control	1.3,1.2	1.3,1.2

Note: The device supports certain TLS ciphers from the factory. Additional ciphers may be added in later releases of firmware. Additional ciphers may be available through Feature Enablement Key activation on the device. Please contact Xerox Support for assistance.

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

VersaLink® products support both CA signed and self-signed certificates. Product certificates support a bit length of up to 2048 bits.

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.

		VersaLink® Multifunction C7120/C7125/C7130	VersaLink® Printers B7125/B7130/B7135
Device Certificates			
	Certificate Length	RSA/2048, RSA3072, ECC/P-256. ECC/P-384, ECC/P-521	RSA/2048, RSA3072, ECC/P-256. ECC/P-384, ECC/P-521
	Supported Hashes	RSA/SHA1, RSA/SHA256, RSA/SHA384, RSA/SHA512, ECDSA/SHA1, ECDSA/SHA256, ECDSA/SHA384, ECDSA/SHA512	RSA/SHA1, RSA/SHA256, RSA/SHA384, RSA/SHA512, ECDSA/SHA1, ECDSA/SHA256, ECDSA/SHA384, ECDSA/SHA512
	Product Web Server	Supported	Supported
	IPPS (TLS) Printing	Supported	Supported
	802.1X Client	Supported	Supported
	Email Signing	Supported	(Not Applicable)
	Email Encryption	Supported	(Not Applicable)
	OCSP Signing	Supported	Supported
	IPSec	(Not currently supported)	(Not currently supported)
	SFTP	(Not currently supported)	(Not Applicable)

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.

		VersaLink® Multifunction C7120/C7125/C7130	VersaLink® Printers B7125/B7130/B7135
Trusted Certificates			
	Minimum Length Restriction Options	1024, 2048	1024, 2048
	Maximum Length	4096	4096
	Supported Hashes	SHA1/224/256/384/512	SHA1/224/256/384/512
	Supported Formats	.cer, .der, PKCS#7, PKCS#12 (.pfx, .p12)	.cer, .der, PKCS#7, PKCS#12 (.pfx, .p12)
	IPSec	Supported	Supported
	LDAP	Supported	Supported
	Scanning (HTTPS/TLS)	(Not currently supported)	(Not Applicable)
	Scanning (SFTP/SSH)	(Not currently supported)	(Not Applicable)
	802.1X Client	Supported	Supported
	Email Signing	Supported	(Not Applicable)
	Email Encryption	Supported	(Not Applicable)
	OCSP Signing	Supported	Supported

CERTIFICATE VALIDATION

VersaLink® devices 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.

		VersaLink® Multifunction C7120/C7125/C7130	VersaLink® Printers B7125/B7130/B7135
Email S/MIME			
	Versions	v2, v3, v3.2	(Not Applicable)
	Digest	MD5, SHA1, SHA256	(Not Applicable)
	Encryption	3DES, RC2, AES128, AES192, AES256	(Not Applicable)

SNMPV3

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

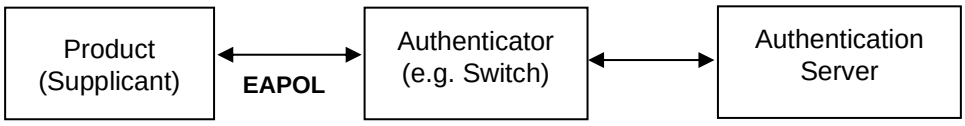
- Message integrity to ensure that a packet has not been tampered with in transit
- Authentication to verify that the message is from a valid source
- Encryption of packets to prevent unauthorized access

		VersaLink® Multifunction C7120/C7125/C7130	VersaLink® Printers B7125/B7130/B7135
SNMPv3			
	Digest	SHA1, MD5	SHA1, MD5
	Encryption	DES, AES128	DES, AES128

Network Access Control

802.1X

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.



		VersaLink® Multifunction C7120/C7125/C7130	VersaLink® Printers B7125/B7130/B7135
Network Access Control			
	802.1x	Supported	Supported
	Authentication Methods	MD5, MS-CHAPv2, PEAP/MS-CHAPv2, EAP-TLS	MD5, MS-CHAPv2, PEAP/MS-CHAPv2, EAP-TLS

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 VersaLink® 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

		VersaLink® Multifunction C7120/C7125/C7130	VersaLink® Printers B7125/B7130/B7135
Network Access Control			
	Cisco ISE	Supported	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 VersaLink® 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.

VersaLink® products use encryption algorithms for Kerberos, SMB, SNMPv3, 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

		VersaLink® Multifunction C7120/C7125/C7130	VersaLink® Printers B7125/B7130/B7135
Firewall		IP Whitelisting	IP Whitelisting
	Stateful Firewall	(Not currently supported)	(Not currently supported)
	IP Whitelist	Supported	Supported

IP WHITELISTING (IP ADDRESS FILTERING)

VersaLink® products support 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)

VersaLink® products do not support Stateful Firewall.

PERSONAL IDENTIFIABLE INFORMATION (PII)

Personal Identifiable Information (PII) can be entered or stored into the device through several means: address book, scan templates, device description, display device information, audit logs, and engineering logs. The PII is encrypted on the device so not readable outside of the operation of the device. The Admin controls the ability of users to enter data, and controls the accessibility of logs, or the deletion of logs. If users wish not to have any PII stored on the device, the Admin has the ability to restrict the features where PII could be stored and has the ability to restrict access to logs. Users do not have access to the internals of the device (memory, hard drive) where PII may be resident.

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

VersaLink® 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.

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.

FIRMWARE INTEGRITY

- Firmware is digitally signed.

Boot Process Integrity

FIRMWARE VERIFICATION

- Firmware is verified against a whitelist using cryptographic hashing.

EVENT MONITORING & LOGGING

- The Audit Log feature records security-related events.

Runtime Security

VersaLink® supports McAfee Embedded Control.

EVENT MONITORING AND 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 VersaLink® products.
- Continuous logging

FAIL SECURE VS FAIL SAFE

VersaLink® 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

The BIOS used in VersaLink® 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 VersaLink® 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, VersaLink® 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.**

VersaLink® 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.

VersaLink® products currently support 52 unique events.

A maximum of 15,000 events can be stored on the device. When the number of events exceeds 15,000, audit log events 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

VersaLink® 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.

7. Identification, Authentication, and Authorization

VersaLink® 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.

A flexible RBAC (Role Based Access Control) security model supports granular to assign of user permissions. Once a user has been authenticated, the product grants (or denies) user permissions based upon the role(s) they have been assigned to. Pre-defined roles that may be used or custom roles may be created as desired.

Authentication

VersaLink® devices support the following authentication mode:

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

NIST 800-171R2 REQUIREMENTS

NIST 800-171r2 requirements can be met on this device through configuration options including but not limited to:

Requirements
Prevent reuse of identifiers for a defined period
Disable identifiers after a defined period of inactivity

Enforce a minimum password complexity and change of characters when new passwords are created
Prohibit password reuse for a specified number of generations
Allow temporary password use for system logons with an immediate change to a permanent password

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 Requires non-alphabetic

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)

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

CONVENIENCE AUTHENTICATION

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.

SIMPLE AUTHENTICATION (NON-SECURE)

Simple authentication is mentioned here for completeness. It is intended for environments where authentication is not required. It is used for customization only. When in this mode, users are not required to enter a password. (The device administrator account always requires a password).

Authorization (Role Based Access Controls)

VersaLink® products 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 allows granular access to applications, services, and tools. Users can be also restricted from accessing the local interface completely.

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.

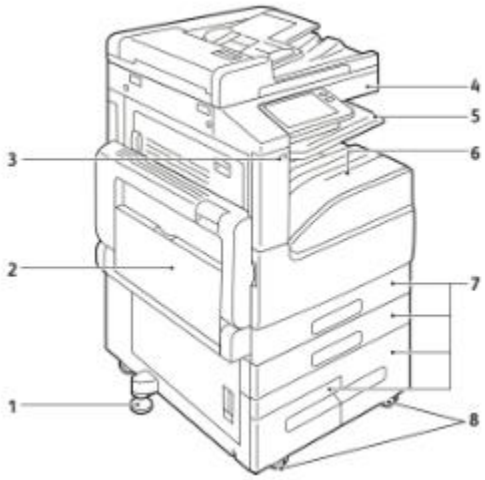
Security Resource	URL
Frequently Asked Security Questions	https://www.xerox.com/en-us/information-security/frequently-asked-questions
Common Criteria Certified Products	https://security.business.xerox.com/en-us/documents/common-criteria/
Current Software Release Quick Lookup Table	https://www.xerox.com/security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

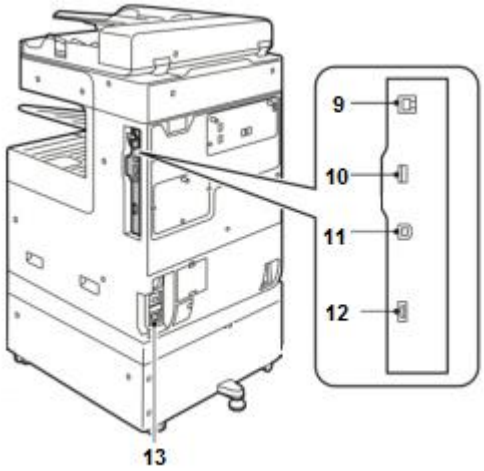
9. Appendix A: Product Security Profiles

This appendix describes specific details of each VersaLink® product.

VersaLink B7125/B7130/B7135

PHYSICAL OVERVIEW





1. Stabilizer
2. Bypass paper feed tray
3. USB2.0 (Host Type A)*
4. Touch screen user interface.
5. Upper paper tray
6. Lower paper tray
7. Paper feed trays
8. **Caster wheels**
9. **USB3.0 (Target Type B)***
10. **Optional Wi-Fi dongle port***
11. **RJ45 Ethernet connection***
12. **Debug serial port (DIN)* (Located under steel plate)**
13. **AC Power**

SECURITY RELATED INTERFACES

Security Related Interfaces	
Ethernet	10/100/1000 MB Ethernet interface.
Optional Wi-Fi Dongle	Supports optional 802.11 Dongle.
Rear USB 3.0 (Type B)	USB target connector used for printing. Note: This port can 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 NFC or CAC readers. Note: This port can be disabled completely by a system administrator.

ENCRYPTION AND OVERWRITE

Encryption and Overwrite	
Encryption	AES-256
TPM Chip	TPM chip is standard and cannot be disabled.
Media Sanitization	Immediate and On-Demand Image Overwrite.

CONTROLLER NON-VOLATILE STORAGE

	IC	HDD	SSD	SD Card
	N/A	**Optional**	**N/A**	**Internal**
Contains User Data (e.g., Print, Scan, Fax)	N/A	Yes	N/A	Yes
Encryption Support	N/A	Always-On	N/A	Always-On
NIST 800-171 Overwrite Support	N/A	Yes	N/A	N/A
Contains Configuration Settings	N/A	Yes	N/A	Yes
Configuration Settings Erasable	N/A	Factory Reset	N/A	Factory Reset

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

CONTROLLER VOLATILE MEMORY

Size	Type	Use	User Data	How to Clear	Volatile
4GB	DDR3 DRAM	Executable code, Printer control data, temporary storage of job data	Yes	Power off system	Yes

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.

MARKING ENGINE NON-VOLATILE STORAGE

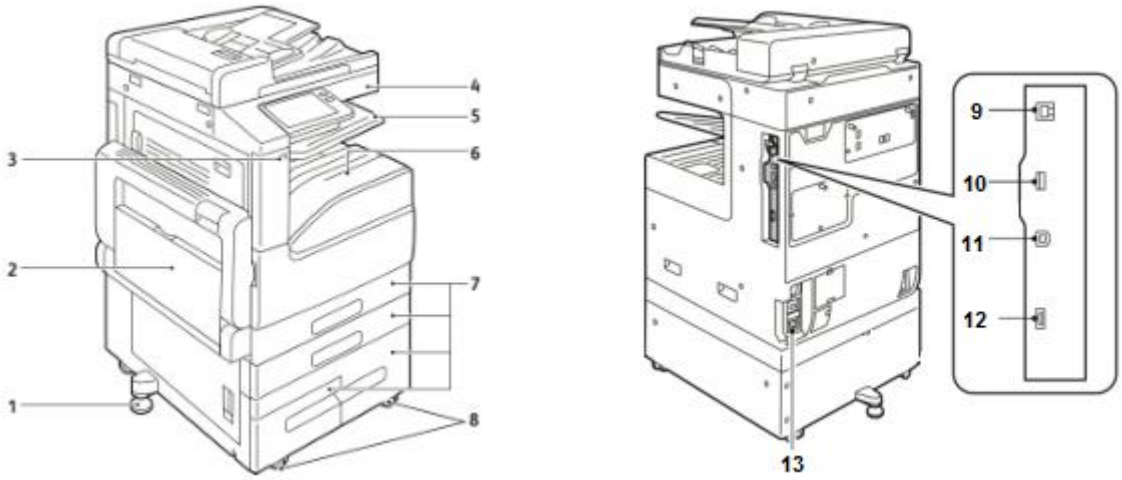
N/A. The marking engine does not contain any non-volatile storage.

MARKING ENGINE VOLATILE MEMORY

N/A. The marking engine volatile memory does not store or process user data.

VersaLink C7120/C7125/C7130

PHYSICAL OVERVIEW



1. Stabilizer
2. Bypass paper feed tray
3. USB2.0 (Host Type A)*
4. Touch screen user interface.
5. Upper paper tray
6. Lower paper tray
7. Paper feed trays
8. Caster wheels
9. USB3.0 (Target Type B)*
10. Optional Wi-Fi dongle port*
11. RJ45 Ethernet connection*
12. Debug serial port (DIN)* (Located under steel plate)
13. AC Power

SECURITY RELATED INTERFACES

Security Related Interfaces	
Ethernet	10/100/1000 MB Ethernet interface.
Optional Wi-Fi Dongle	Supports optional 802.11 Dongle.
Rear USB 3.0 (Type B)	USB target connector used for printing. Note: This port can 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 NFC or CAC readers. Note: This port can be disabled completely by a system administrator.

ENCRYPTION AND OVERWRITE

Encryption and Overwrite	
Encryption	AES-256
TPM Chip	TPM chip is standard and cannot be disabled.
Media Sanitization	Immediate and On-Demand Image Overwrite.

CONTROLLER NON-VOLATILE STORAGE

	IC	HDD	SSD	SD Card
	N/A	**Optional**	**N/A**	**Internal**
Contains User Data (e.g., Print, Scan, Fax)	N/A	Yes	N/A	Yes
Encryption Support	N/A	Always-On	N/A	Always-On
NIST 800-171 Overwrite Support	N/A	Yes	N/A	N/A
Contains Configuration Settings	N/A	Yes	N/A	Yes
Configuration Settings Erasable	N/A	Factory Reset	N/A	Factory Reset

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

CONTROLLER VOLATILE MEMORY

Size	Type	Use	User Data	How to Clear	Volatile
4GB	DDR3 DRAM	Executable code, Printer control data, temporary storage of job data	Yes	Power off system	Yes

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.

MARKING ENGINE NON-VOLATILE STORAGE

N/A. The marking engine does not contain any non-volatile storage.

MARKING ENGINE VOLATILE MEMORY

N/A. The marking engine volatile memory does not store or process user data.

10. Appendix B: Security Events

Xerox VersaLink Security Events

ID	Event	Description
101	Started normally (cold boot)	
101	Started normally (warm boot)	
101	Started (NVM initialized)	
101	Started (Hard Disk initialized)	
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	
501	Adjust 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”)
601	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
601	Export Address Book	

ID	Event	Description
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	Software	Completion: (“Updated”) ROM Type: (“IOT” / “UI”/ “Controller”/ “FAX”) New Version Previous Version
701	Trusted Communication	Completion: (“Failed”) Protocol Name: (“SSL/TLS” / “IPSEC”/ “S/MIME”)