

Security Guide

Xerox® VersaLink® B620 Printer

Xerox® VersaLink® C620 Color Printer



2024 Xerox Corporation. All rights reserved. Xerox®, CentreWare®, VersaLink®, Xerox Extensible Interface Platform® are trademarks of Xerox Corporation in the United States and/or other countries. BR39993

Other company trademarks are also acknowledged.

Document Version: 1 (February 2024).

Copyright protection claimed includes all forms and matters of copyrightable material and information now allowed by statutory or judicial law or hereinafter granted including without limitation, material generated from the software programs which are displayed on the screen, such as icons, screen displays, looks, etc.

| | | |
|-----------|---|------------|
| 1. | Introduction | 1-4 |
| | Purpose | 1-4 |
| | Target Audience | 1-4 |
| | Disclaimer | 1-4 |
| 2. | Product Description | 2-5 |
| | Physical Components | 2-5 |
| | Architecture | 2-6 |
| | User Interface..... | 2-7 |
| | Scanner | 2-7 |
| | Marking Engine | 2-7 |
| | Controller..... | 2-7 |
| | Controller External Interfaces | 2-7 |
| | Front/Rear Panel USB (Type A) port(s)..... | 2-7 |
| | 10/100/1000 MB Ethernet TIA-568 Network Connector | 2-8 |
| | Rear USB (Type B) Target Port | 2-8 |
| | Optional Equipment..... | 2-8 |
| | Wireless Network Connector | 2-8 |
| | Near Field Communications (NFC) Reader..... | 2-8 |
| | SMART CARD – CAC/PIV | 2-8 |
| 3. | User Data Protection..... | 3-1 |
| | User Data Protection While Within Product | 3-1 |
| | Encryption | 3-1 |
| | Private Key Management..... | 3-1 |
| | Job Data Removal available on standard emmc configuration | 3-1 |
| | Media Sanitization (Image Overwrite) Available With Optional HDD Configuration..... | 3-1 |
| | Immediate Image Overwrite Available With Optional HDD COnfiguration | 3-1 |
| | User Data in Transit | 3-2 |
| | Inbound User Data (Print Job Submission) | 3-2 |
| | EMail Signing and Encryption using S/MIME | 3-2 |
| | Native Apps– ‘PRINT FROM’ Google Drive, DropBox, and Microsoft OneDrive | 3-4 |
| 4. | Network Security | 4-5 |
| | Listening Services (inbound ports)..... | 4-6 |
| | Network Encryption..... | 4-7 |
| | IPsec | 4-7 |
| | Wireless 802.11 Wi-Fi Protected Access (WPA) | 4-7 |

| | | |
|-----------|--|------------|
| | TLS..... | 4-9 |
| | SNMPv3 | 4-9 |
| | Public Key Infrastructure (PKI)..... | 4-10 |
| | Device Certificates | 4-10 |
| | Trusted Certificates | 4-12 |
| | Minimum Key Length | 4-12 |
| | Network Access Control..... | 4-13 |
| | 802.1x | 4-13 |
| | Cisco Identity Services Engine (ISE) | 4-13 |
| | Contextual Endpoint Connection Management | 4-14 |
| | FIPS140-3 COMPLIANCE | 4-14 |
| | Additional Network Security Controls..... | 4-14 |
| | IP Filtering | 4-14 |
| | Personal Identifiable Information (PII)..... | 4-15 |
| 5. | Device Security: BIOS, Firmware, OS, Runtime, and Operational Security Controls | 5-1 |
| | Pre-Boot Security | 5-1 |
| | BIOS..... | 5-1 |
| | Embedded Encryption..... | 5-1 |
| | Boot Process Security..... | 5-1 |
| | Trusted Boot..... | 5-1 |
| | Firmware Integrity | 5-2 |
| | Runtime Security..... | 5-2 |
| | Operational Security..... | 5-2 |
| | Firmware Restrictions | 5-2 |
| | Event Monitoring and Logging | 5-3 |
| | Configuration Watchdog | 5-3 |
| | Audit Log | 5-3 |
| | Security Information Event Management (SIEM) Support..... | 5-4 |
| | Operational Security..... | 5-4 |
| | Service Technician (CSE) Access Restriction | 5-4 |
| | Additional Service Details | 5-4 |
| | Cloning | 5-4 |
| | Backup and Restore | 5-4 |
| | FLEET ORCHESTRATOR | 5-5 |
| | EIP Applications | 5-5 |
| | XEROX EASY ASSIST | 5-5 |

| | | |
|------------|--|-------------|
| 6. | Configuration and Security Policy Management Solutions..... | 6-1 |
| 7. | Identification, Authentication, and Authorization..... | 7-1 |
| | Authentication | 7-1 |
| | Local Authentication..... | 7-1 |
| | Password Policy..... | 7-2 |
| | Network Authentication | 7-2 |
| | Smart Card Authentication..... | 7-2 |
| | Convenience Authentication | 7-3 |
| | Authorization (Role-Based Access Controls)..... | 7-3 |
| | Remote Access | 7-3 |
| | Local Access..... | 7-3 |
| 8. | Additional Information and Resources..... | 8-1 |
| | Security @ Xerox® | 8-1 |
| | Responses to Known Vulnerabilities..... | 8-1 |
| | Additional Resources | 8-1 |
| 9. | Appendix A: Product Security Profiles..... | 9-2 |
| | VersaLink® B620 | 9-2 |
| | Physical Overview..... | 9-2 |
| | Controller Non-Volatile Storage | 9-3 |
| | Marking Engine Non-Volatile Storage..... | 9-3 |
| | Marking Engine Volatile Memory | 9-4 |
| | Physical Overview..... | 9-5 |
| | Security Related Interfaces..... | 9-5 |
| | Controller Non-Volatile Storage | 9-6 |
| | Marking Engine Non-Volatile Storage..... | 9-6 |
| | Marking Engine Volatile Memory | 9-6 |
| 10. | Appendix B: Security Events..... | 10-1 |
| | Xerox VersaLink Security Events..... | 10-1 |

1. Introduction

Purpose

The purpose of this document is to disclose information for the VersaLink® devices (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

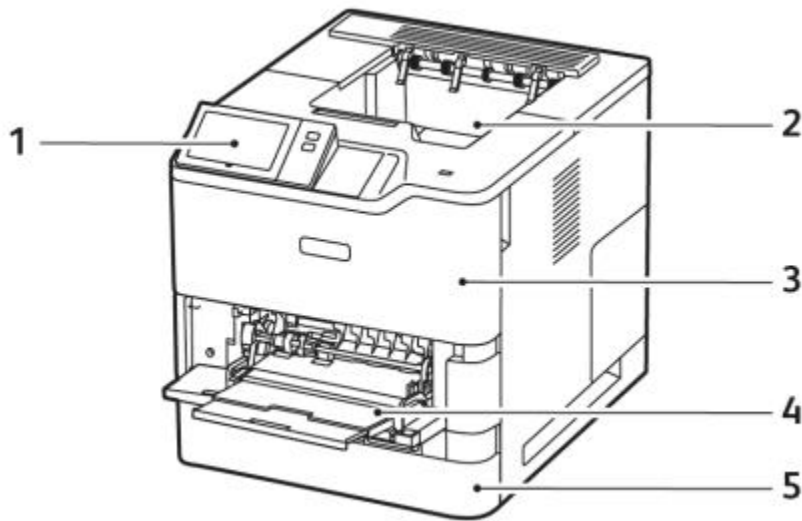
The content of this document is provided for information purposes only. The performance of the products referenced herein is exclusively subject to the applicable Xerox Corporation terms and conditions of sale and/or lease. Nothing stated in this document constitutes the establishment of any additional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

2. Product Description

PHYSICAL COMPONENTS

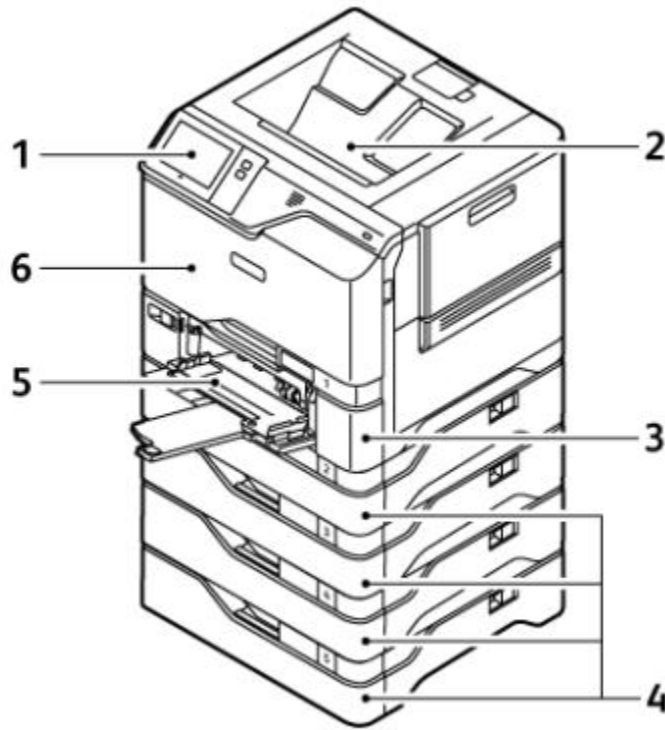
Xerox® VersaLink® B620 (Mono Printer) and C620 (Color Printer) are very similar and consist of a, marking engine, controller, and user interface. A typical configuration is depicted below. Please note that options including finishers, paper trays, document handlers, etc. may vary configuration, however, they are not relevant to security and are not discussed.

B620 Mono PRINTER



- | | |
|------------------------------------|------------------------------------|
| 1. Control Panel or User Interface | 4. Bypass Tray 100-sheets |
| 2. Standard Output Tray | 5. Tray 1, Standard 550-sheet tray |
| 3. Door A, Front Door | |

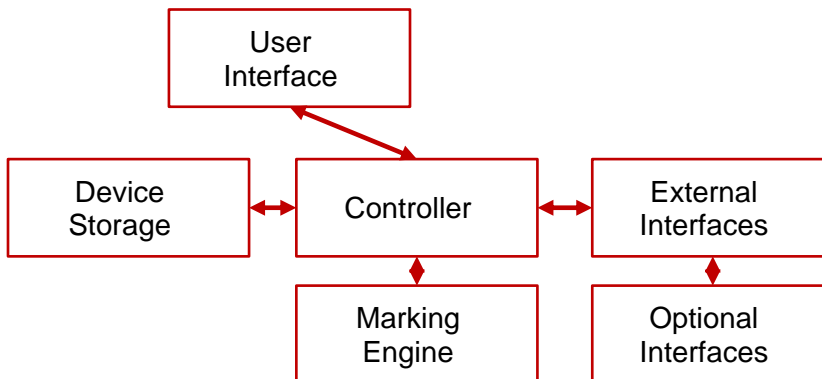
C620 Color Printer



- | | |
|---|--|
| 1. Control Panel or User Interface | 4. Trays 2-5, Optional 550-sheet Trays |
| 2. Standard Output Tray | 5. Bypass Tray, 100-sheets |
| 3. Tray 1, Standard 550-sheet Tray with an integrated 100-sheet Bypass Tray | 6. Door A, Front Door |

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 User Interface (LUI) in order to distinguish it from the remote web server interface, also known as Embedded Web Server (EWS) or 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 printer only models do not support an integrated scanner.

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, 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. Standard models are equipped with an embedded Multi-Media Card (eMMC). For model specific details please see Appendix A: Product Security Profiles.

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

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/REAR PANEL USB (TYPE A) PORT(S)

This device has USB Type A ports in the front and the rear of the device. One or more USB ports may be located on the front of the product, near the user interface. USB ports may be enabled or disabled by a system administrator. The USB (Type A) ports supports the following:

- Walk-up users may insert a USB thumb drive to store or retrieve documents 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 USB ports can be disabled independently.

- Connection of optional equipment such as Bluetooth or CAC readers.
- Firmware updates may be submitted through USB ports. Note that the product must be configured to allow local firmware updates, or the update will not be processed. The user must be an administrator to perform firmware updates.
- Installation of other files such as clone files or weblet files. Note that the product must be configured to allow the installation of clone files and weblet files. The user must be an administrator to perform clone or weblet file installations.

10/100/1000 MB ETHERNET TIA-568 NETWORK CONNECTOR

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

REAR USB (TYPE B) TARGET PORT

A USB type B port is 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.

Optional Equipment

WIRELESS NETWORK CONNECTOR

VersaLink® products accept an optional wireless and Bluetooth combination kit. Bluetooth is used for iBeacon for AirPrint Discovery. When enabled and configured, iBeacon enables the Xerox device to advertise basic printer discovery information, including a routable IP address, via the Bluetooth Low Energy Beacon. iBeacon functionality can be disabled using the embedded web server of the product.

NEAR FIELD COMMUNICATIONS (NFC) READER

VersaLink® products come standard with an NFC Chip built into the front panel. This is read only from an NFC client. 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.

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

VersaLink® products support a variety of smart cards that can be used to log in to the machine. Please contact Xerox Support for a list of supported cards and card readers.

3. User Data Protection

Xerox® printers and Printer products receive, process, and may optionally store user data from several sources including local print jobs or mobile and cloud applications, etc. Xerox® products protect user data being processed by employing strong encryption. The standard configuration is sold with eMMC.

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. Encryption cannot be disabled on this family of products.

PRIVATE KEY MANAGEMENT

Any private key on the system is managed in compliance with NIST Special Publication 800-57 *Recommendation for Key Management*. This includes keying material in transition and at rest. An onboard TPM module (v2.0) compliant with ISO/IEC 11889 is used in support of private key management.

JOB DATA REMOVAL AVAILABLE ON STANDARD EMMC CONFIGURATION

The Job Data Removal feature is provided to allow security conscious customers the facility to remove all residual image data from the Network Controller. Job Data Removal is being introduced to provide customers with eMMC devices the ability to clean up the disk by purging job data (no overwrite).

MEDIA SANITIZATION (IMAGE OVERWRITE) AVAILABLE WITH OPTIONAL HDD CONFIGURATION

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 the algorithm as described in the following link:

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

IMMEDIATE IMAGE OVERWRITE AVAILABLE WITH OPTIONAL HDD CONFIGURATION

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 overwrite of sensitive data with minimal impact to performance, robust error reporting, and logging via the Audit Log. When enabled, Immediate Image Overwrite (IIO) will overwrite and remove any remnants of temporary files of all print jobs from the image disk as soon as the job finishes processing.

Note: eMMC, SD-Card, and Flash media cannot be completely sanitized by multi-pass overwriting methods due to the memory wear mapping that occurs. Please refer to NIST-800-88 “Table A-8: Flash Memory-Based Storage Product Sanitization” for technical details.

User Data in Transit

This section focuses on the protection of user data (print /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. |
| Xerox Print Stream Encryption | The Xerox® Global Print Driver® supports document encryption for any print jobs to enabled products. Simply configure Document Encryption to On in the Advanced tab of the print driver at print time. |
| EIP Print from URL (HTTPS) | Securely submit a print job directly to product via EIP using HTTPS. |
| EIP Print Encryption | EIP print supports encryption of print jobs to any supported products. Simply configure the encryption key type, key and invocation vector per the EIP API definition. |
| Microsoft Universal Print | Supported products are securely registered with Microsoft Universal Print using key exchanges. All data in Universal Print is encrypted in transit and in storage to securely submit a print job to the product. |

EMAIL SIGNING AND ENCRYPTION USING S/MIME

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

NOTE: SHA1, AES128, and AES192 are deprecated and considered insecure. Xerox recommends using SHA256 and AES256 and above.

| VersaLink® Printer | | | |
|---------------------|------------|------------------------------|------------------------------|
| | | B620 | C620 |
| Email S/MIME | | | |
| | Versions | v3 | v3 |
| | Digest | SHA1, SHA256, SHA384, SHA512 | SHA1, SHA256, SHA384, SHA512 |
| | Encryption | AES128, AES192, AES256, 3DES | AES128, AES192, AES256, 3DES |

NATIVE APPS- 'PRINT FROM' GOOGLE DRIVE, DROPBOX, AND MICROSOFT ONEDRIVE

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.

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).



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. Some ports can be configured to different value for some features/protocols.

| Port | Type | Service Name |
|------------|---------|--|
| 80 or 443 | TCP | HTTP including: Web User Interface Web Services for Products (WSD) WebDAV |
| 68 | UDP | DHC ACK Response to DHCP |
| 88 | UDP | Kerberos |
| 110 | TCP | POP3 |
| 139 | TCP | NETBIOS |
| 161 | TCP | SNMP |
| 162 | TCP | SNMP Trap |
| 137 | UDP | NETBIOS (Name Service) |
| 138 | UDP | NETBIOS (Datagram Service) |
| 161 | UDP | SNMP |
| 427 | TCP/UDP | SLP |
| 443 | TCP | HTTPS – HTTP over TLS, IPPS |
| 445 | TCP | SMB |
| 500 & 4500 | TCP/UDP | IPsec |
| 515 | TCP | LPR |
| 631 | TCP | IPP |
| 3702 | TCP/UDP | WSD (Discovery) |
| 4000 | TCP | ThinPrint |
| 5353 | TCP/UDP | mDNS |
| 5354 | TCP | mDNS Responder IPC |
| 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 |
| 51333 | TCP | Fleet Orchestrator downloads |
| 53202 | TCP | WSD Transfer |
| 53303 | TCP | WSD Print |

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.

NOTE: SHA1, AES128, and AES192 are deprecated and considered insecure. Xerox recommends using SHA256 and AES256 and above.

| | | | | VersaLink® Printer | |
|--------------|------------------------------------|---|---|--------------------|------|
| | | | | B620 | C620 |
| IPsec | | | | | |
| | Supported IP Versions | IPv4, IPv6 | IPv4, IPv6 | | |
| | Key exchange authentication method | Preshared Key & digital signature authentication (device authentication certificate, server validation certificate) | Preshared Key & digital signature authentication (device authentication certificate, server validation certificate) | | |
| | Transport Mode | Transport & Tunnel mode | Transport & Tunnel mode | | |
| | Security Protocol | ESP & AH | ESP & AH | | |
| | ESP Encryption Method | AES, Null | AES, Null | | |
| | ESP Authentication Methods | SHA1, SHA256, None | SHA1, SHA256, None | | |

WIRELESS 802.11 WI-FI PROTECTED ACCESS (WPA)

Products equipped with Wi-Fi support WPA3 Personal, WPA3 Personal Transitional, WPA3 Enterprise, WPA3 Enterprise 192-bit mode (dependent on dongle used), WPA2 Personal, WPA2 Enterprise, and Mixed Mode.

The wireless network adapters used in Xerox® products are certified by the Wi-Fi Alliance.

| | | | | VersaLink® Printer | |
|-----------------------|---------------------|------------------------------------|------------------------------------|--------------------|------|
| | | | | B620 | C620 |
| Wi-Fi (802.11) | | | | | |
| | No Encryption | Supported | Supported | | |
| | WEP | RC4 | RC4 | | |
| | WPA2 Personal (PSK) | CCMP (AES), TKIP, TKIP+CCMP (AES), | CCMP (AES), TKIP, TKIP+CCMP (AES), | | |

| | | | |
|--|---|--|--|
| | | PMF (Protected Management Frame) optional support Password-based authentication via Pre-Shared Key (PSK) | PMF (Protected Management Frame) optional support Password-based authentication via Pre-Shared Key (PSK) |
| | WPA2 Enterprise | CCMP (AES), TKIP, TKIP+CCMP (AES) PEAPv0 MS-CHAPv2 EAP-TLS EAP-TTLS/PAP EAP-TTLS/MS-CHAPv2 EAP-TTLS/EAP-TLS PMF (Protected Management Frame) optional support | CCMP (AES), TKIP, TKIP+CCMP (AES) PEAPv0 MS-CHAPv2 EAP-TLS EAP-TTLS/PAP EAP-TTLS/MS-CHAPv2 EAP-TTLS/EAP-TLS PMF (Protected Management Frame) optional support |
| | WPA3 Personal (SAE) CCMP (AES) | PMF (Protected Management Frame) support required Password-based authentication via Simultaneous Authentication of Equals (SAE) | PMF (Protected Management Frame) support required Password-based authentication via Simultaneous Authentication of Equals (SAE) |
| | WPA3 Personal Transitional | WPA3 / WPA2 Personal CCMP (AES) PMF (Protected Management Frame) support optional Password-based authentication: WPA3-SAE/ WPA2-PSK | WPA3 / WPA2 Personal CCMP (AES) PMF (Protected Management Frame) support optional Password-based authentication: WPA3-SAE/ WPA2-PSK |
| | WPA3 Enterprise | CCMP (AES) PEAPv0 MS-CHAPv2 EAP-TLS EAP-TTLS/PAP EAP-TTLS/MS-CHAPv2 EAP-TTLS/EAP-TLS Server certificate validation required PMF (Protected Management Frame) support required | CCMP (AES) PEAPv0 MS-CHAPv2 EAP-TLS EAP-TTLS/PAP EAP-TTLS/MS-CHAPv2 EAP-TTLS/EAP-TLS Server certificate validation required PMF (Protected Management Frame) support required |
| | WPA3 Enterprise- 192 bit (dependent on dongle used) | AES-GCMP-256 EAP-TLS EAP-TTLS/EAP-TLS Server certificate validation required | AES-GCMP-256 EAP-TLS EAP-TTLS/EAP-TLS Server certificate validation required |

| | | | |
|--|---------------------------|---|---|
| | | PMF (Protected Management Frame) support required | PMF (Protected Management Frame) support required |
| | BSSID Roaming Restriction | Supported | Supported |

TLS

VersaLink® products support configurable TLS Versions and TLS Hash Algorithms for device features that use TLS.

NOTE: TLS 1.0 and 1.1 are deprecated and considered insecure. Xerox recommends using TLS 1.2 or higher.

| VersaLink® Printer | | | |
|--------------------|---------------------|--|---|
| | | B620 | C620 |
| TLS | | | |
| | TLS Versions | TLS TLS 1.3 TLS 1.2 (recommended) TLS 1.1 and TLS 1.2 (default), or TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3 Include or not include TLS 1.3 setting Note: Do not include TLS 1.3 if some features require servers that do not support TLS 1.3 | TLS TLS 1.3 TLS 1.2 (recommended) TLS 1.1 and TLS 1.2 (default), or TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3 Include or not include TLS 1.3 setting Note: Do not include TLS 1.3 if some features require servers that do not support TLS 1.3 |
| | TLS Hash Algorithms | SHA-256 and above (recommended) SHA-1, SHA-256 and above (default) Note: The setting does not apply Print from Cloud features other than for authentication. | SHA-256 and above (recommended) SHA-1, SHA-256 and above (default) Note: The setting does not apply Print from Cloud features other than for authentication. |

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

NOTE: SHA1, AES128, and AES192 are deprecated and considered insecure. Xerox recommends using SHA256 and AES256 and above.

| VersaLink® Printer | | | |
|--------------------|------------|-------------|-------------|
| | | B620 | C620 |
| SNMPv3 | | | |
| | Digest | SHA1, MD5 | SHA1, MD5 |
| | Encryption | AES128, DES | AES128, DES |

Public Key Infrastructure (PKI)

Digital certificates are a key component of public key infrastructure. A digital certificate contains information about the identity of an entity, the certificate authority that issued the certificate, and its associated public and private key pair. The certificate's private key is used to generate digital signatures, and the public key is used to validate those digital signatures. For entities to validate a digital signature, the certificate and its public key are shared freely. Trust is established by validating the certificate path, which contains the certificate authorities that issued the certificate.

DEVICE CERTIFICATES

VersaLink® products support both CA signed and self-signed device certificates. The device certificates support a bit length of up to 4096 bits.

VersaLink® products require a device certificate. The PRINTER will use the device certificate as its identity. The PRINTER EWS certificate is an example of a device certificate. The device certificate must be issued by a certificate authority (CA) trusted by the device.

The Xerox device certificate, which is the default device certificate installed on the PRINTER, is issued by the Xerox Root CA embedded in the PRINTER firmware. The Xerox device certificate details are configurable and can be recreated as needed by the device administrator.

The PRINTER can be configured to use any installed CA signed certificate as its device certificate. To install a CA signed certificate, the device administrator can generate and download a Certificate Signing Request (CSR) from the PRINTER, have the CSR be signed by an Enterprise CAs or 3rd Party CAs, and then imported the CA signed certificate into the PRINTER. Alternatively, this process can be completed off-box and a CA signed certificate in PKCS #12 format can be imported into the PRINTER.

| VersaLink® Printer | | | |
|----------------------------|--------------------|-----------------------------------|-----------------------------------|
| | | B620 | C620 |
| Device Certificates | | | |
| | Certificate Length | Up to 4096 (for RSA certificates) | Up to 4096 (for RSA certificates) |

| | | | |
|--|----------------------------|-------------|-------------|
| | Default Device Certificate | ECDSA P-384 | ECDSA P-384 |
| | Supported Hashes | SHA256 | SHA256 |
| | Product Web Server | Supported | Supported |
| | IPPS Printing | Supported | Supported |
| | 802.1X Client | Supported | Supported |
| | IPsec | Supported | Supported |
| | SFTP | Supported | Supported |

TRUSTED CERTIFICATES

Public Root and Intermediate Root Certificate Authority (CA) certificates may be imported to the product's certificate store to establish trust with external products and services. The following categories are supported:

- A 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.
- Peer Device certificates are certificates that are installed on the printer for solution-specific uses.

NOTE: SHA1, AES128, and AES192 are deprecated and considered insecure. Xerox recommends using SHA256 and AES256 and above.

| VersaLink® Printer | | | |
|--|--|----------------------|----------------------|
| | | B620 | C620 |
| Trusted Certificates (CA & Peer device) | | | |
| | Minimum Length RSA Restriction Options | None, 1024, 2048 | None, 1024, 2048 |
| | Maximum Length | 4096 | 4096 |
| | Supported Hashes | SHA1/224/256/384/512 | SHA1/224/256/384/512 |
| | IPsec | Supported | Supported |
| | LDAP | Supported | Supported |
| | 802.1X Client | Supported | Supported |
| | Email Signing | Supported | Supported |
| | Email Encryption | Supported | Supported |
| | Email (STARTLS) | Supported | Supported |
| | OCSP Signing | Supported | Supported |

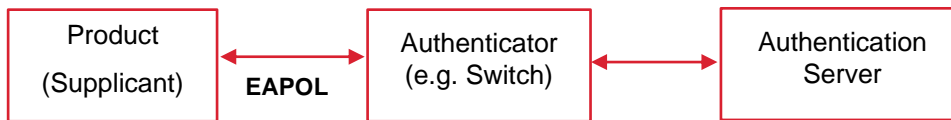
MINIMUM KEY LENGTH

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.

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® Printer | |
|-------------------------------|------------------------|--|--|--|------|
| | | | | B620 | C620 |
| Network Access Control | | | | | |
| | 802.1x | Supported | | Supported | |
| | Authentication Methods | PEAPv0/EAP MSCHAPv2, EAP-MSCHAPv2, EAP-TLS | | PEAPv0/EAP MSCHAPv2, EAP-MSCHAPv2, 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 PRINTERS.

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 levels 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 PRINTERS 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/PRINTER
- 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 PRINTERS by:

- Providing real time policy violation alerts and logging
- Enforcing network segmentation policy
- Isolating the printing products to prevent general access to printers and PRINTERS in restricted areas

Automated access to policy enforcement

- Provide extensive reporting of printing product network activity

| VersaLink® Printer | | | |
|-------------------------------|-----------|-------------|-------------|
| | | B620 | C620 |
| 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.

FIPS140-3 COMPLIANCE

When enabled, cryptographic functions are FIPS 140-3 compliant and performed from within a FIPS compliant module, except those acknowledged as exceptions during FIPS 140-3 enablement.

Additional Network Security Controls

IP FILTERING

The devices contain a static host-based firewall that provides the ability to prevent unauthorized network access based on IP address and/or port number. Filtering rules can be set by the SA using

the Embedded Web Server. An authorized SA can create rules to (Accept/Reject/Drop) for ALL or a range of IP addresses. In addition to specifying IP addresses to filter, an authorized SA can enable/disable all traffic over a specified transport layer port.

PERSONAL IDENTIFIABLE INFORMATION (PII)

Personal Identifiable Information (PII) can be entered or stored into the device through several means: address book, device description, display device information, audit logs, and engineering logs. The PII is encrypted on the device, and it is 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 they 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 Security

BIOS

The embedded BIOS used in VersaLink® products cannot be accessed by users. 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 is 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 can be securely 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-256 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

TRUSTED BOOT

Xerox® VersaLink® products utilize a Trusted Boot process to enable a secure boot utilizing Intel's Boot Guard and the Unified EFI Forum/Microsoft specified (UEFI) BIOS approach to ensure a verified Chain of Trust is utilized to perform the PRINTER boot process. This process establishes a root of trust extending from the Intel processor to the UEFI and continuing to the Boot Manager and the Xerox Firmware. The startup process verifies that the installation software/firmware has not been altered, giving the customer assurance that the code has not been altered or replaced.

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 encrypted and 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.

Runtime Security

Each VersaLink® device comes with Trellix Embedded Control built-in and enabled by default and cannot be disabled. Trellix embedded Control is used to protect a variety of endpoints that range from wearable devices to critical systems controlling electrical generation.

Executable control prevents unauthorized code from executing. Xerox has defined a whitelist of executable programs; software that is not on the secure whitelist is not allowed to execute. Trellix cannot be disabled on VersaLink® products; it is always enabled.

When an anomaly is detected, it is logged to the device audit log and optional alerts are immediately sent via email. Events are also reportable through CentreWare® Web or Xerox Device Manager, and Trellix® ePolicy Orchestrator (ePO).

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.

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
- Document Feeder
- Finisher (Option for processing printed paper. No description on Finisher is provided in this document because the user's image data will not be stored in it.)

- High-capacity feeder (No description of the high-capacity feeder is provided in this document because user's image data will not be stored in it.)
- High-capacity stacker (No description of the 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.)
- The downloading function can be disabled by a system administrator from the local UI or the Embedded Web Server.
- For additional information on Firmware updates and various upgrade methods supported, please see the System Administrator Guide.

Event Monitoring and Logging

CONFIGURATION WATCHDOG

Configuration Watchdog allows Administrators to configure the periodic monitoring of up to 26 security-related features. If, during a check, a monitored security setting is discovered to have been changed, the system will automatically reset it. In the case that remediation is unsuccessful, an email alert is generated, and the event is captured in the Audit Log (see below for information on the Audit Log). For a list of the security settings covered, please see the System Administrator Guide.

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 over a hundred unique events. A maximum of 15,000 events can be stored on the device. When the Audit Log reaches 13,500 entries (90% "full"), an email alert will be sent if configured. When it reaches 28,500 events, the device will send another message stating there have been 15,000 events since the last alert. The device will keep alerting at 15,000 event intervals. 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 can 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 and Audit Log can't be disabled on this version of VersaLink® products.

SECURITY INFORMATION EVENT MANAGEMENT (SIEM) SUPPORT

Xerox® VersaLink® B620 / C620 supports the ability to directly connect to industry leading security and event management (SIEM) systems. Once configured, Xerox® VersaLink® B620 / C620 PRINTERS send security information, along with the event severity, to the SIEM system for processing and reporting. Events are generated as they occur and are transmitted in Common Event Format (CEF), which a SIEM system can interpret. The firmware supports connection to Trellix Enterprise Security Manager, LogRhythm, and Splunk Enterprise Security. Additional SIEM systems which comply with the CEF and syslog standards are expected to be compatible as well.

Operational Security

SERVICE TECHNICIAN (CSE) ACCESS RESTRICTION

The CSE (Customer Service Engineer) account allows a Xerox Technician to access the PRINTER's diagnostics and maintenance routines. The CSE role has only 'guest privileges' to the other user interfaces including the Local and Embedded Web Server. However, CSE access to these other interfaces can be restricted if needed.

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.

CLONING

Certain system settings can be captured (copied) in a clone file that may be installed on other VersaLink systems. Clone files are encrypted and this VersaLink PRINTER does not support installing older clone files created on other Atlantis 1.0 and 1.5 devices. Access to both creating and installing a clone file can be restricted using role-based access controls. Clone files can only be created through the Embedded Web Server or via USB at the Local UI. Clone files can be installed through the following methods: Embedded Web Server, USB at the Local UI, Web service, submission as a print job, or Fleet Orchestrator. Clone file installation can be disabled totally or partially, by disabling the print submission of clone files.

BACKUP AND RESTORE

Like cloning, backup & restore, can capture (copy) certain system and device specific settings in a backup file. This file may be reapplied to the same device at any time. This backup can be stored at the device or exported, and the exported file is encrypted. The restore of backup files can be disabled.

FLEET ORCHESTRATOR

The Fleet Orchestrator feature allows you to share configuration files automatically between Xerox devices. This tool can be used to enhance and customize the security profile of Xerox printers/PRINTERS in several ways:

- The SA can create a set of security-related (and convenience) configuration items and have the entire fleet implement them. This is accomplished by creating a Full or partial Clone file with the desired settings and letting Fleet Orchestrator system ensure all the devices have that file.
- The SA can use the Auto-Assembly feature to add and maintain a list of printers/PRINTERS in their organization. The devices connect to a single Publisher PRINTER automatically. They also sense when that connection has been broken and reconnect automatically. Once connected the device share configuration files within the Trust Community.
- Fleet Orchestrator can also reapply a clone file to a printer/PRINTER every day to ensure the device settings stay as specified.

The device discovery process is based on industry standard DNS and DHCP protocols.

SECURITY DASHBOARD

The Security Dashboard displays a list of security features on the device organized into four NIST standard categories: Authentication, Confidentiality, Integrity, and Availability. The admin can view the current status of security features and navigate directly to configuration pages to view or modify security settings as necessary.

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 within the **Xerox App Gallery**. Products can be configured to prevent installation of unauthorized EIP applications. Discussion of individual EIP application security is beyond the scope of this document. EIP applications utilize the security framework provided by the Third-party vendor and the EIP configuration of the product. Please consult documentation for individual EIP application as provided by the Third-party vendor for security details.

XEROX EASY ASSIST

The Xerox® Easy Assist app provides help for users and SAs to get the most out of their Xerox printer.

This app does not perform any new security-related functions but uses the standard protocols and features within the printer to help the user.

The Xerox® Easy Assist app is useful for the non-admin user and can also be used by the admin to monitor a set of printers and look for help on issues. The settings pages within the app use the admin password just as the Web Page does. The admin password (if supplied by the user) is maintained in a secured memory space.

6. Configuration and Security Policy Management Solutions

Xerox Device Manager and Xerox® CentreWare® Web (available as a free download) centrally manage Xerox Devices. Additionally, these VersaLink® products come with Trellix built in and can be managed with Trellix provides an enhanced security posture supporting proactive monitoring, threat detection, and remediation capabilities. 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 the 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 enables granular control to assign 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

Xerox® VersaLink® devices support the following authentication mode:

- Local Authentication
- Network Authentication
- Smart Card Authentication (CAC, PIV, etc.)
- 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 recommended security features to secure the system.

Note: Usernames and passwords stored in the user database are not transmitted over the network and passwords are encrypted.

PASSWORD POLICY

The following password attributes can be configured:

| Password Policy | |
|--|---|
| Minimum Length | 1 |
| Maximum Length | 63 |
| Default Minimum | 4 |
| Password cannot contain Username | Supported |
| Password complexity options (in addition to alphabetic characters) | Can be set to require a number, an upper-case character, lower case character and a special character |

Admin password can be set using any character within the printable Unicode and the VersaLink default administrator password meets the 2020 California Password Law (SB-327). This law states that each 'internet-connectable' device must have a unique password by default.

All newly sold Xerox devices will have the default administrator password be the serial number of the device. It is recommended the customer change this new default administrator password, as soon as possible, to a strong password that the customer can use and recall.

NETWORK AUTHENTICATION

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

| Network Authentication Providers | B620 | C620 |
|---------------------------------------|-------------------------------|-------------------------------|
| Kerberos (Microsoft Active Directory) | Supported | Supported |
| Kerberos (MIT) | Supported | Supported |
| SMB NTLM Versions Supported | NTLMv2 | NTLMv2 |
| LDAP Versions Supported | Version 3 (including TLS 1.2) | Version 3 (including TLS 1.2) |

SMART CARD AUTHENTICATION

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. It provides two-factor security: 1) a PIN is required to unlock the smart card and 2) the user's smart card credential is authenticated over the network using Kerberos PKINIT authentication.

Smart Card Authentication requires card reader hardware. Please contact Xerox Support for a list of supported cards and card readers.

| Smart Cards | B620 | C620 |
|--------------------------|-----------|-----------|
| Common Access Card (CAC) | Supported | Supported |
| PIV/ PIV II | Supported | Supported |
| Gemalto MD | Supported | Supported |

| | | |
|-------------|-----------|-----------|
| SIPR | Supported | Supported |
|-------------|-----------|-----------|

Support for the SIPR network is provided using a Smart Card authentication solution created by 90meter under contract for Xerox. Details regarding 90meter can be found online here: <https://www.90meter.com/>

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 manner. The level of security provided is dependent upon the chosen implementation.

Some examples of third party convenience authentication providers include:

Xerox Workplace Cloud <https://www.xerox.com/>

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)

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, print, plex, 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 users.

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.

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.

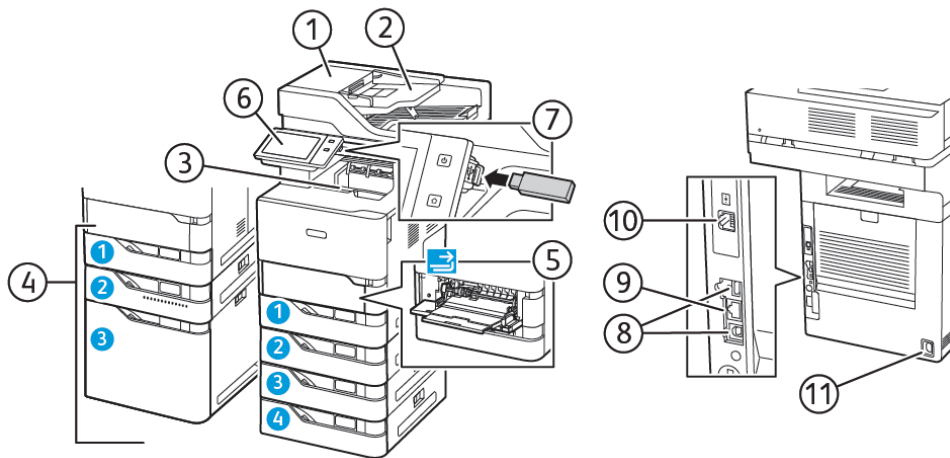
| Security Resource | URL |
|---|---|
| Frequently Asked Security Questions | https://www.xerox.com/en-us/information-security/frequently-asked-questions |
| Common Criteria Certified Products | https://security.business.xerox.com/en-us/documents/common-criteria/ |
| Current Software Release Quick Lookup 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® B620

PHYSICAL OVERVIEW



- 4. Single-Pass Duplex Automatic Document Feeder (DADF)
- 5. Document Feeder Tray
- 6. Output Tray
- 7. Paper Input Trays
- 8. Bypass Tray
- 9. Control Panel
- 10. Front USB Port
- 8. Rear USB A and B Ports
- 9. Ethernet Port
- 10. Fax Port
- 11. 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 NOT be disabled. |

| | |
|---|---|
| Front & Rear USB2.0 (Type A) port(s) | <p>Users may insert a USB thumb drive to print from or store files to. (Physical security of this information is the responsibility of the user or operator.) Note that features that leverage USB ports) can be disabled independently based on services.</p> <p>Firmware upgrades may be applied using this port. Connection of optional equipment such as NFC or CAC readers.</p> <p>Note: These ports can be disabled completely by a system administrator.</p> |
|---|---|

CONTROLLER NON-VOLATILE STORAGE

| Model | Size | Type | Use | User Data | How to Clear |
|-------------|-----------------|-------|---|-----------|---------------|
| B620 | 32 GB or higher | eMMC* | Contains User Data (e.g., Print,) and Configuration Settings. This data is encrypted and Encryption is always-on | Yes | Factory Reset |

*eMMC: embedded Multi-Media Card, is a Standard Configuration

Controller Volatile Memory

| Model | Size | Type | Use | User Data | How to Clear |
|-------------|------|-----------|--|-----------|------------------|
| B620 | 4 GB | DDR3 DRAM | Executable code, Printer control data, temporary storage of job data | Yes | Power off system |
| C620 | 4 GB | DDR3 DRAM | Executable code, Printer control data, temporary storage of job data | Yes | Power off system |

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

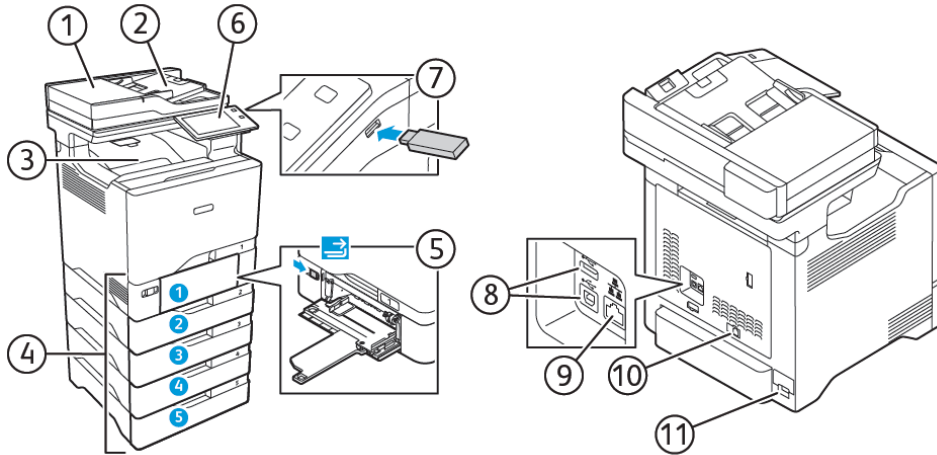
The marking engine does not contain any non-volatile storage.

MARKING ENGINE VOLATILE MEMORY

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

VersaLink® C620

PHYSICAL OVERVIEW



- | | |
|--|---|
| <ul style="list-style-type: none"> 1. Single-Pass Duplex Automatic Document Feeder (DADF) 2. Document Feeder Tray 3. Output Tray 4. Paper Input Trays 5. Bypass Tray 6. Control Panel 7. Front USB Port | <ul style="list-style-type: none"> 8. Rear USB A and B Ports 9. Ethernet Port 10. Fax Port 11. 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 NOT be disabled. |
| Front & Rear USB2.0 (Type A) port(s) | Users may insert a USB thumb drive to print from or store files to. (Physical security of this information is the responsibility of the user or operator.) Note that features that leverage USB |

| | |
|--|--|
| | <p>ports can be disabled independently based on services.</p> <p>Firmware upgrades may be applied using this port. Connection of optional equipment such as NFC or CAC readers.</p> <p>Note: These ports can be disabled completely by a system administrator.</p> |
|--|--|

CONTROLLER NON-VOLATILE STORAGE

| Model | Size | Type | Use | User Data | How to Clear |
|-------|-----------------|-------|---|-----------|---------------|
| C620 | 32 GB or higher | eMMC* | Contains User Data (e.g., Print) and Configuration Settings. This data is encrypted and Encryption is always-on | Yes | Factory Reset |

*eMMC: embedded Multi-Media Card, is a Standard Configuration

Controller Volatile Memory

| Model | Size | Type | Use | User Data | How to Clear |
|-------|------|-----------|--|-----------|------------------|
| C620 | 4 GB | DDR3 DRAM | Executable code, Printer control data, temporary storage of job data | Yes | Power off system |
| C620 | 8 GB | DDR3 DRAM | Executable code, Printer control data, temporary storage of job data | Yes | Power off system |

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

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

MARKING ENGINE VOLATILE MEMORY

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

10. Appendix B: Security Events

Xerox VersaLink Security Events

| ID | Event | Description |
|----|------------------------|---|
| 1 | System Startup | Device Name Device Serial Number |
| 2 | System Shutdown | Device Name Device Serial Number |
| 3 | Standard ODIO Started | Device Name Device Serial Number |
| 4 | Standard ODIO Complete | Device Name Device Serial Number Completion Status (Success Failed) |
| 5 | Print Job | Job Name User Name Source Service Name Completion Status IIO Status Accounting User ID Accounting Account ID |
| 9 | Email Job | Job Name User Name Completion Status IIO Status Accounting User ID Accounting Account ID Encryption On or Off Total Number of SMTP Recipients SMTP Recipients |
| 10 | Audit Log Disabled | Device Name Device Serial Number |
| 11 | Audit Log Enabled | Device Name Device Serial Number |
| 12 | Copy Job | Job Name User Name Completion Status IIO Status Accounting User ID Accounting Account ID |
| 14 | LAN Fax Job | Job Name User Name Completion Status IIO Status Accounting User ID |

| | | |
|----|------------------------------|--|
| | | Accounting Account ID Total Fax Recipient Phone Numbers Fax Recipient Phone Numbers |
| 16 | Full Disk Overwrite Started | Device Name Device Serial Number |
| 17 | Full Full Overwrite Complete | Device Name Device Serial Number Overwrite Status |
| 21 | Delete File/Directory | Service (print) Job Name or Directory Name User Name Completion Status IIO Status |
| 26 | PagePack Login | Device Name Device Serial Number Completion Status: Success (if Passcode is okay) Failed (if Passcode is not okay) Locked Out (if max attempts exceed 5) Time Remaining: Hrs (Remaining for next attempt) Min (Remaining for next attempt) |
| 27 | Postscript Passwords | Device Name Device Serial Number Startup Mode or System Params Password or Start Job Password Completion Status (Enabled Disabled Changed) |
| 29 | Network User Login | User Name Device Name Device Serial Number Completion Status (Success/Failed) |
| 30 | SA Login | User Name Device Name Device Serial Number Completion Status (Success/Failed) |
| 31 | User Login | User Name Device Name Device Serial Number Completion Status (Success/Failed) |
| 32 | Service Login | Service Name Device Name Device Serial Number Completion Status (Success/Failed) |
| 33 | Audit Log Download | User Name Device Name Device Serial Number Destination (WebUI, USB drive) Completion Status (Success/Failed) |
| 34 | IIO Feature Status | User Name Device Name |

| | | |
|----|--|--|
| | | Device Serial Number IIO Status (Enabled/Disabled) |
| 35 | SA Pin Changed | User Name Device Name Device Serial Number Completion Status Interface (Web Local SNMP Web Service) Session IP Address (If Available) |
| 36 | Audit Log Saved | User Name Device Name Device Serial Number Completion Status |
| 37 | Force Traffic over Secure Connection (HTTPS) | User Name Device Name Device Serial Number Completion Status (Enabled Disabled Terminated) |
| 38 | Security Certificate | User Name Device Name Device Serial Number Completion Status (Created/Uploaded_Success/Downloaded) |
| 39 | IP Sec | User Name Device Name Device Serial Number Completion Status (Configured/Enabled/Disabled/Terminated) |
| 40 | SNMPv3 | User Name Device Name Device Serial Number Completion Status (Configured/Enabled/Disabled/Terminated) |
| 41 | IP Filtering Rules | User Name Device Name Device Serial Number Completion Status (Rule Added/Rule Edited/Rule Deleted) |
| 42 | Network Authentication | User Name Device Name Device Serial Number Completion Status (Configured/Enabled/Disabled) |
| 43 | Device Clock | User Name Device Name Device Serial Number Completion Status (Time Zone Changed/Date/Time Changed/Time Format Changed/Date Format Changed) |
| 44 | Software Upgrade | User Name Device Name Device Serial Number Completion Status (Success/Failed) |
| 45 | Clone File Operations | User Name Device Name Device Serial Number Completion Status (Clone file installed: (Success / Failed) / |

| | | |
|----|---------------------------------|--|
| | | Clone file downloaded: (Success / Failed)/ (Submit clone file) |
| 47 | Xerox Secure Access | Device Name Device Serial Number Completion status (Configured/Enabled/Disabled) |
| 48 | Service Login Copy Mode | Service Name Device Name Device Serial Number Completion Status (Success/Failed) |
| 49 | Smartcard Login | User Name (if valid Card and Password are entered) Device Name Device Serial Number Completion Status (Success/Failed) |
| 50 | Process Terminated | Device Name Device Serial Number Process Name Termination Reason |
| 51 | ODIO Scheduled | User Name Device Name Device Serial Number Completion Status (Enabled/Disabled) ODIO Schedule Mode Configured ODIO Schedule Frequency Configured ODIO Schedule Day of Week Configured ODIO Schedule Day of Month Configured |
| 53 | CPSR Backup | File Name User Name Completion Status (Normal/Error) IIO Status |
| 54 | CPSR Restore | File Name User Name Completion Status (Normal/Error) IIO Status |
| 55 | SA Tools Access Admin | Device Serial Number Completion Status (Locked/Unlocked) |
| 57 | Session Timer Logout | Device Name Device Serial Number Interface (WebUI, LUI, CAC) User Name (who was logged out) Session IP (if available) |
| 58 | Session Timeout Interval Change | Device Name Device Serial Number Interface (WebUI, LUI, CAC) (Timer affected by change) User Name (who made this change) Session IP (if available) Completion Status (Success/Failed) |
| 59 | User Permissions | User Name Device Name Device Serial Number Completion Status (Enabled/Disabled/Configured) |

| | | |
|----|--------------------------------------|--|
| | | Interface (WebUI, LUI, CAC, SNMP) Session IP Address (if available) |
| 60 | Device Clock NTP | Device Name Device Serial Number Enable/Disable/Config NTP NTP Server IP Address/Hostname Server Port Completion Status (Success/Failed) |
| 61 | Device Administrator Role Permission | User Name (of user making the change) Device Name Device Serial Number User Name (of target user) Completion Status (Grant/Revoke) |
| 62 | Smartcard Configuration | User Name Device Name Device Serial Number Card type (SIPR Token, CAC/PIV) Completion Status (Enabled/Disabled/Configured) |
| 63 | IPv6 Configuration | User Name Device Name Device Serial Number Completion Status (Enabled Wireless / Disabled Wireless Configured Wireless) / (Enabled Wired / Disabled Wired / Configured Wired) |
| 64 | 802.1x | User Name Device Name Device Serial Number Completion Status (Success/Failed) |
| 65 | Abnormal System Termination | Device Name Device Serial Number |
| 66 | Local Authentication | User Name Device Name Device Serial Number Completion Status (Enabled/Disabled) |
| 67 | Web User Interface Authentication | User Name Device Name Device Serial Number Authentication Method Enabled (Network/Local) |
| 68 | FIPS Mode | User Name Device Name Device Serial Number Completion Status (Enable/Disable/Configure) |
| 69 | Xerox Secure Access Login | User Name Device Name Device Serial Number Completion Status (Success/Failed) |
| 70 | Print from USB | User Name Device Name Device Serial Number |

| | | |
|----|-------------------------------------|--|
| | | Completion Status (Enabled/Disabled) |
| 71 | USB Port Enable/Disable | User Name Device Name Device Serial Number USB Port ID Completion Status (Enabled/Disabled) |
| 73 | System Log Download | Username Device Name File Names Downloaded Destination (IP address or USB device) Completion Status (Success/Failed) |
| 75 | Remote Control Panel Configuration | User Name Device Name Device Serial Number Completion Status (Enabled/Disabled/Configured) |
| 76 | Remote Control Panel Session | User Name Device Name Device Serial Number Completion Status (Initiated/Terminated) Remote Client IP Address |
| 80 | SMTP Connection Encryption | User Name Device name Device Serial Number Completion Status (Enabled for STARTLS/ Enabled for STARTLS if available/ Enabled for TLS/Disabled/Configured) |
| 81 | Email Domain Filtering Rule | User Name Device Name Device Serial Number Completion Status (Feature Enabled/Feature Disabled/Rule Added/Rule Deleted) |
| 82 | Software Verification Test Started | Device Name Device Serial Number |
| 83 | Software Verification Test Complete | Device Name Device Serial Number Completion Status (Success/Failed/Cancelled) |
| 84 | TrllixSecurity State | User Name Device Name Device Serial Number Security Mode (Enhanced Security/Integrity Control) Completion Status (Enabled/Disabled/Pending) |
| 85 | TrellixTrellix Security Event | Device Name Device Serial Number Type (Read/Modify/Execute/Deluge) Trellix Message Text |
| 87 | Trellix Agent | User Name Device Name Device Serial Number |

| | | |
|-----|-------------------------------------|---|
| | | Completion Status (Enabled/Disabled) |
| 88 | Digital Certificate Import Failure | Device Name Device Serial Number Email Address of Requestor (if available) Failure Reason (Invalid Address/Invalid Certificate/Invalid Signature) |
| 89 | Device User Account Management | User Name (Managing User Names) Device Name Device Serial Number User Name Added or Deleted Completion Status (Created/Deleted) |
| 90 | Device User Account Password Change | User Name (Managing Passwords) Device Name Device Serial Number User Name Affected Completion Status (Password Modified) |
| 94 | FTP/SFTP Filing Passive Mode | User Name Device Name Device Serial Number Completion Status (Enabled/Disabled) |
| 96 | EIP Weblets Allow Install | User Name Device Name Device Serial Number Completion Status (Enable Installation/Block Installation) |
| 97 | EIP Weblets Install | User Name Device Name Device Serial Number Weblet Name Action (Install/Delete) Completion (Success/Fail) |
| 98 | EIP Weblets Enable | User Name Device Name Device Serial Number Weblet Name Completion Status (Enable/Disable) |
| 99 | Network Connectivity | User Name Device Name Device Serial Number Completion Status (Enable Wireless/Disable Wireless/ Configure Wireless/Enable Wired/Disable Wired/ Configure Wired/Enable WiFi Direct/Disable WiFi Direct/Configure WiFi Direct) |
| 100 | Address Book Permissions | User Name Machine Name Machine serial number Completion Status (SA Only/Open Access Enabled WebUI)/ (SA Only/Open Access Enabled LocalUI) |
| 101 | Address Book Export | User Name Machine Name Machine Serial Number |

| | | |
|-----|--|--|
| 102 | Software Upgrade Policy | User Name Device Name Device Serial Number Completion Status (Enable Installation/Disable Installation) |
| 103 | Supplies Plan Activation | Device Name Device Serial Number Completion Status Success (if Passcode is okay) Failed (if Passcode is not okay) Locked out (if Max Attempts Exceed 5) Time Remaining Hrs (remaining for next attempt) Min (remaining for next attempt) |
| 104 | Plan Conversion | Device Name Device Serial Number Completion Status Success (if Passcode is okay) Failed (if Passcode is not okay) Locked out (if Max Attempts Exceed 5) Time Remaining Hrs (remaining for next attempt) Min (remaining for next attempt) |
| 105 | IPv4 Configuration | User Name Device Name Device Serial Number Completion Status (Enabled Wireless/Disabled Wireless/ Configured Wireless/Enabled Wired/Disabled Wired/ Configured Wired) |
| 106 | SA PIN Reset | Device Serial Number Completion Status (Success/Failed) |
| 107 | Convenience Authentication Login | User Name Device Name Device Serial Number Completion Status (Success/Failed) |
| 108 | Convenience Authentication Configuration | User Name Device Name Device Serial Number Completion Status (Enabled/Disabled/Configured) |
| 110 | Custom Authentication Login | User Name Device Name Device Serial Number Completion Status (Success/Failed) |
| 111 | Custom Authentication Configuration | User Name Device Name Device Serial Number Completion Status (Enabled/Disabled/Configured) |
| 112 | Billing Impression Mode | User Name Device Name Device Serial Number |

| | | |
|-----|--|--|
| | | Mode Set to (A4 Mode/A3 Mode) Completion Status (Success/Failed) |
| 114 | Device Cloning Installation Policy | User Name Device Name Device Serial Number Completion Status (Enable for Encrypted Files Only/Disable) |
| 115 | Save for Reprint Job | Job Name User Name Print from USB/Print from URL Completion Status |
| 116 | Web User Interface Access Permission | Device Name Device Serial Number Completion Status (Standard Access/Open Access/Restricted) |
| 117 | System Log Push to Xerox | Username if Authenticated Server Destination URL Log Identifier String (Filename) Completion Status (Success/Failed) |
| 123 | Near Field Communication | User Name Device Name Device Serial Number Completion Status (Enabled/Disabled) |
| 124 | Invalid Login Attempt Lockout | Device Name Device Serial Number Interface (WebUI, Local UI, , SNMP, Remote, Fax, Secure Fax) Session IP Address (if available) |
| 125 | Secure Protocol Log Enable/Disable | User Name Device Name Device Serial Number Completion Status (Enable/Disable) |
| 126 | Display Device Information Configure | User Name Device Name Device Serial Number Completion Status (Configured) |
| 127 | Successful Login After Lockout Expired | Device Name Device Serial Number Interface (WebUI, Local UI) Session IP Address (if available) Count of Invalid Attempts: xx attempts, where xx = the number of attempts |
| 128 | Erase Customer Data | Device Serial Number Erase Customer Data Device Serial Number Completion Status (Success/Failed) |
| 129 | Audit Log SFTP Scheduled Configure | User Name Device Name Device Serial Number Completion Status (Enable/Disable/Configured) |

| | | |
|-----|------------------------------------|--|
| 130 | Audit Log SFTP Transfer | User Name Device Name Device Serial Number Destination Server Completion Status (File Transmitted) |
| 131 | Remote Software Download Policy | User Name Device Name Device Serial Number Completion Status (Enable/Disable) |
| 136 | Remote Services NVM Write | Device Name Device Serial Completion Status (Success/Fail) |
| 137 | Remote Services FIK Install | Device Name Device Serial Completion Status (Success/Fail) User-readable names for the features being installed |
| 138 | Remote Services Data Push | Device Name Device Serial Completion Status (Success/Fail) |
| 139 | Remote Services | User Name Device Name Device Serial Status (Enabled/Disabled) |
| 140 | Restore Backup Installation Policy | User Name Device Name Device Serial Number Completion Status (Enable/Disable) |
| 141 | Backup-Restore File Downloaded | File Name User Name Interface (WebUI) IP Address of the Destination (if applicable) Completion Status (Success/Failed) |
| 142 | Backup-Restore Restore Installed | File Name User Name Device Name Device IP address Interface (WebUI) Completion Status (Success/Failed) |
| 144 | User or Group Role Assignment | User Name Device Name Device Serial Number User or Group Name (Assigned) Role Name Action (Added/Removed) |
| 145 | User Permission Role | User Name Device Name Device Serial Number Role Name Completion Status (Created/Deleted/Configured) |

| | | |
|-----|--|---|
| 146 | Admin Password Reset Policy Configure | User Name Device Name Device Serial Number |
| 147 | Local User Account Password Policy | User Name Device Name Device Serial Number |
| 148 | Restricted Admin Login | User Name Device Name Device Serial Number Completion Status (Success/Failed) |
| 149 | Restricted Administrator Role Permission | User Name (of user making the change) Device Name Device Serial Number User Name (of target user) Action (Grant/Revoke) |
| 150 | Manual Session Logout | Device Name Device Serial Number Interface (WebUI, LUI, CAC) User Name (who was logged out) Session IP (if available) |
| 151 | IPP | User Name Device Name Device Serial Number Completion Status (Enabled/Disabled/Configured) |
| 152 | HTTP Proxy Server | User Name Device Name Device Serial Number Completion Status (Enabled/Disabled/Configured) |
| 153 | Remote Services Software Download | Device Name Device Serial Number File Name |
| 154 | Restricted Admin Permission Role | User Name Device Name Device Serial Number Restricted Admin Role Name Completion Status (Created/Deleted/Configured) |
| 155 | EIP Weblet Installation Security Policy | User Name Device Name Device Serial Number Policy (Allow Installation of Encrypted Weblets/Allow Installation of Both Encrypted and Unencrypted Weblets) |
| 156 | Lockdown and Remediate Security | User Name Device Name Device Serial Number Completion Status (Enabled/Disabled) |
| 157 | Lockdown Security Check Complete | User Name Device Name Device Serial Number Completion Status (Success/Failed) |

| | | |
|-----|--|--|
| 158 | Lockdown Remediation Complete | User Name Device Name Device Serial Number Completion Status (Success/Failed) |
| 159 | Send Engineering Logs on Data Push | User Name (if available) Device Name Device Serial Number Current Setting (Enabled/Disabled) |
| 160 | Allow the Print Submission of Clone Files | User Name (if available) Device Name Device Serial Number Completion Status (Enabled/Disabled, Permanently Removed) |
| 161 | Network Troubleshooting Start/StopData Capture | User Name Device Name Device Serial Number Completion Status (Started/Stopped) |
| 162 | Network Troubleshooting Data Download | User Name File Name (of downloaded file) Device Name Device Serial Number Destination (IP Address) Completion Status (Success/Failed) |
| 163 | DNS-SD Data Download | User Name File Name (of downloaded file) Device Name Device Serial Number Destination (IP address) Completion Status (Success/Failed) |
| 165 | SMB Browse | User Name Device Name Device Serial Number Completion Status (Enabled/Disabled/Configured) |
| 166 | Job Data Removal Standard Started | Device Name Device Serial Number |
| 167 | Job Data Removal Standard Complete | Device Name Device Serial Number Completion Status (Success/Failed) |
| 168 | Job Data Removal Full Started | Device Name Device Serial Number |
| 169 | Job Data Removal Full Complete | Device Name Device Serial Number Completion Status (Success/Failed) |
| 170 | Scheduled Job Data Removal Configure | User Name Device Name Device Serial Number Completion Status (Enable/Disable/Configured) |

| | | |
|-----|---|---|
| 171 | Cross-Origin Resource Sharing (CORS) | User Name Device Name Device Serial Number Completion Status (Enable/Disable) |
| 173 | Fleet Orchestrator Trust Operations | User Name Device Name Device Serial Number Member Name Member Serial Number TC Lead Device Name TC Lead Serial Number Trust Operation (Grant/Revoke) Completion Status (Success/Failed) |
| 174 | Fleet Orchestrator Feature | User Name Device Name Device Serial Number Trust Operation (Enable/Disable/Configure) Completion Status (Success/Failed) |
| 175 | Fleet Orchestrator – Store File for Distribution | User Name Device Name Device Serial Number File type (SWUP/Clone/Add-On) File Name |
| 176 | Xerox Configuration Watchdog | User Name Device Name Device Serial Number Completion Status (Enabled/Disabled) |
| 177 | Xerox Configuration Watchdog Check Complete | User Name (if available, SYSTEM, if executed as a scheduled event) Device Name Device Serial Number Completion Status (Success/Failed) |
| 178 | Xerox Configuration Watchdog Remediation Complete | User Name (if available, SYSTEM, if executed as a scheduled event) Device Name Device Serial Number Completion Status (Success/Failed) |
| 179 | ThinPrint Feature | User Name Device Name Device Serial Number Completion Status (Enabled/Disabled/Configured) |
| 180 | Beaconing for iBeacon for AirPrint Discovery | User Name Device Name Device Serial Number Completion Status (Enabled/Disabled) |
| 181 | Network Troubleshooting | User Name Device Name Device Serial Number Completion Status (Installed/Uninstalled) |
| 182 | POP3 Connection Encryption (TLS) | User Name Device Name |

| | | |
|-----|---------------------------------|--|
| | | Device Serial Number Completion Status (Enabled/Disabled/Configured) |
| 183 | FTP Browse | User Name Device Name Device Serial Number Completion Status (Configured/Enabled/Disabled) |
| 184 | SFTP Browse | User Name Device Name Device Serial Number Completion Status (Configured/Enabled/Disabled) |
| 190 | Cloud Service | User Name Device Name Device Serial Number Completion Status (Enabled/Disabled) |
| 193 | Xerox Workplace Cloud | User Name Device Name Device Serial Number Completion Status (Enabled/Disabled) |
| 195 | Card Reader | Device Name Device Serial Number Completion Status (Connected/Disconnected) |
| 196 | EIP App Management | User Name Device Name Device Serial Number App Name Action (Install/Delete) Completion Status (Success/Failed) |
| 197 | EIP Apps Enablement | User Name Device Name Device Serial Number App Name Action (Install/Delete) Completion Status (Enabled/Disabled) |
| 199 | Car Reader Upgrade Policy | User Name Device Name Device Serial Number Completion Status (Enabled/Disabled) |
| 200 | Car Reader Upgrade Attempted | User Name Device Name Device Serial Number Completion Status (Success/Failed) Car Reader upgrade file name Car reader Serial Number |
| 204 | Syslog Server | User Name |

| | | |
|-----|---|--|
| | | Device Name Device Serial Number Server IPv4 Address (if available) Server IPv6 Address (if available) Completion Status (Configured/Enabled/Disabled) |
| 205 | TLS (Version and/or Hash) | User Name Device Name Device Serial Number Completion Status (Configured) |
| 206 | Security Dashboard Configuration | User Name Device Name Device Serial Number Completion Status (Configured) |
| 208 | Canceled Job | Job Name User Name IIO status Accounting User ID Accounting Account ID |
| 209 | Embedded Accounts | User Name Device Name Device Serial Number Completion Status (Enabled Disabled) |
| 210 | SNMP v1/v2c | User Name Device Name Device Serial Number Completion Status (Configured Enabled Disabled) |
| 211 | Xerox Workplace Cloud Remote Management | User Name Device Name Device Serial Number Completion Status (Enabled Disabled) |
| 218 | Universal Print Enablement | User Name Device Name Device Serial Number Universal Print Completion Status ("Enabled" "Disabled") Session IP Address (If Available) |

| | | |
|-----|----------------------------------|---|
| 219 | Universal Print Registration | User Name Device Name Device Serial Number Universal Print Registration Status ("Registered" "Unregistered" "Certificate expired" "Registration claim code expired") Session IP Address (If Available) |
| 220 | IDP Authentication Login Attempt | User Name Device Name Device Serial Number Completion Status (Success) |
| 221 | IDP Authentication Enablement | User Name Device Name Device Serial Number Completion Status (Enabled Disabled) |
| | | |