

# Xerox®

## Security Guide



### Office Class Multi-Function Products & Single-Function Printers

| <b>AltaLink® Multi-Function Products</b> | <b>VersaLink® Multi-Function Products</b> | <b>VersaLink® Printers</b>            |
|--|---|---------------------------------------|
| B8045, B8055, B8065, B8075, B8090        | B405, B605, B615, B7025, B7030, B7035     | B400, B600, B610                      |
| C8030, C8035, C8045, C8055, C8070        | C405, C505, C605, C7020, C7025, C7030     | C400, C500, C600, C7000, C8000, C9000 |

February 2018 update

Xerox® Security Guide for Office Class Products: AltaLink® • VersaLink®

© 2018 Xerox Corporation. All rights reserved. Xerox and Xerox and Design® are trademarks of Xerox Corporation in the United States and/or other countries. BR25497

Other company trademarks are also acknowledged.

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.

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

# Table of Contents

---

|          |  |          |
|----------|--|----------|
| <b>1</b> | <b>Introduction .....</b>                            | <b>5</b> |
|          | Purpose .....  | 5        |
|          | Target Audience .....                                | 5        |
|          | Disclaimer.....                                      | 5        |
| <b>2</b> | <b>Product Description.....</b>                      | <b>6</b> |
|          | Physical Components .....                            | 6        |
|          | Architecture .....                                   | 6        |
|          | User Interface.....                                  | 7        |
|          | Scanner .....  | 7        |
|          | Marking Engine .....                                 | 7        |
|          | Controller.....                                      | 7        |
|          | Controller External Interfaces.....                  | 7        |
|          | Front Panel USB (Type A) port(s) .....               | 7        |
|          | 10/100/1000 MB Ethernet RJ-45 Network Connector..... | 8        |
|          | Rear USB (Type B) Target port.....                   | 8        |
|          | Optional Equipment.....                              | 8        |
|          | RJ-11 Analog Fax and Telephone .....                 | 8        |
|          | Wireless Network Connector.....                      | 8        |
|          | Near Field Communications (NFC) Reader .....         | 8        |
|          | SMART CARD – CAC/PIV .....                           | 8        |
|          | Foreign Product Interface.....                       | 8        |
| <b>3</b> | <b>User Data Protection.....</b>                     | <b>9</b> |
|          | User Data protection while within product.....       | 9        |
|          | Encryption .....                                     | 9        |
|          | TPM Chip .....                                       | 9        |
|          | Media Sanitization (Image Overwrite) .....           | 9        |
|          | Immediate Image Overwrite .....                      | 9        |
|          | On-Demand Image Overwrite .....                      | 9        |
|          | User Data in transit .....                           | 10       |
|          | Inbound User Data .....                              | 10       |
|          | Print Job Submission.....                            | 10       |
|          | Encrypted Transport.....                             | 10       |
|          | Description .....                                    | 10       |

|   |           |
|---|-----------|
| Outbound User Data .....  | 10        |
| Scanning to Network Repository, Email, Fax Server .....                                       | 10        |
| Protocol .....  | 10        |
| Encryption .....  | 10        |
| Description .....   | 10        |
| Scanning to User Local USB Storage Product .....  | 11        |
| Add on Apps- Cloud, Google, DropBox, and others .....   | 11        |
| <b>4 Network Security.....</b>  | <b>12</b> |
| TCP/IP Ports & Services .....   | 12        |
| Listening services (inbound ports) .....  | 12        |
| Network Encryption .....  | 13        |
| IPSec    13   |           |
| Wireless 802.11 Wi-Fi Protected Access (WPA) .....  | 14        |
| TLS      14   |           |
| Public Key Encryption (PKI) .....   | 15        |
| Device Certificates .....   | 15        |
| Trusted Certificates .....  | 16        |
| Certificate Validation .....  | 17        |
| Email Signing and Encryption using S/MIME.....  | 17        |
| SNMPv3   17   |           |
| Network Access Control.....   | 18        |
| 802.1x    18  |           |
| Cisco Identity Services Engine (ISE) .....  | 18        |
| Cisco ISE allows you to deploy the following controls and monitoring of Xerox products:.....  | 18        |
| Contextual Endpoint Connection Management .....   | 19        |
| FIPS140-2 Compliance Validation .....   | 19        |
| Additional Network Security Controls.....   | 19        |
| Endpoint Firewall Options .....   | 19        |
| IP Whitelisting (IP Address Filtering).....   | 20        |
| Stateful Firewall (Advanced IP Filtering) .....   | 20        |
| <b>5 Device Security: BIOS, Firmware, OS, Runtime, and Operational security controls.....</b> | <b>21</b> |
| Fail Secure Vs Fail Safe.....   | 22        |
| Pre-Boot Security .....   | 22        |
| BIOS      22  |           |
| Embedded Encryption .....   | 22        |
| Boot Process Security .....   | 22        |
| Firmware Integrity.....   | 22        |

|   |           |
|---|-----------|
| Runtime Security .....  | 23        |
| Event Monitoring & Logging .....  | 23        |
| Audit Log   | 23        |
| Operational Security .....  | 23        |
| Firmware Restrictions .....   | 23        |
| Service Technician (CSE) Access Restriction .....                                 | 24        |
| Additional Service Details .....  | 24        |
| Backup & Restore (Cloning).....   | 24        |
| EIP Applications .....  | 24        |
| XCP (eXtensible Customizable Platform) .....                                      | 24        |
| <b>6 Configuration &amp; Security Policy Management Solutions .....</b>           | <b>25</b> |
| <b>7 Identification, Authentication, and Authorization .....</b>                  | <b>26</b> |
| Authentication .....  | 26        |
| AltaLink® and VersaLink® devices support the following authentication mode: ..... | 26        |
| Local Authentication .....  | 26        |
| Password Policy .....   | 26        |
| Network Authentication .....  | 27        |
| Smart Card Authentication .....   | 27        |
| Convenience Authentication .....  | 27        |
| Simple Authentication (non-secure).....   | 28        |
| Authorization (Role Based Access Controls) .....                                  | 28        |
| Remote Access .....   | 28        |
| Local Access .....  | 28        |
| <b>8 Additional Information &amp; Resources.....</b>                              | <b>29</b> |
| Security @ Xerox®.....  | 29        |
| Responses to Known Vulnerabilities.....   | 29        |
| Additional Resources .....  | 29        |
| <b>Appendix A: Product Security Profiles .....</b>                                | <b>30</b> |
| AltaLink® B8045/B8055/B8065/B8075/B8090 .....                                     | 31        |
| AltaLink® C8030 / C8035 / C8045 / C8055 / C8070 .....                             | 33        |
| VersaLink® B7025, B7030 B7035 .....   | 35        |
| VersaLink® C7000, C7020, C7025, C7030 .....                                       | 37        |
| VersaLink® C400, C405 .....   | 39        |
| VersaLink® B400, B405.....  | 39        |
| VersaLink® C500, C600, C505, C605 .....   | 43        |
| VersaLink® B600, B605, B610, B615.....  | 45        |
| VersaLink® C8000, C9000 .....   | 47        |

|  |           |
|--|-----------|
| <b>Appendix B: Security Events .....</b> | <b>49</b> |
| Xerox AltaLink® Security Events .....    | 49        |
| VersaLink® Security Events .....         | 65        |

# 1 Introduction

## **Purpose**

---

The purpose of this document is to disclose information for the Xerox ® Office Class printers and multi-function products (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**

---

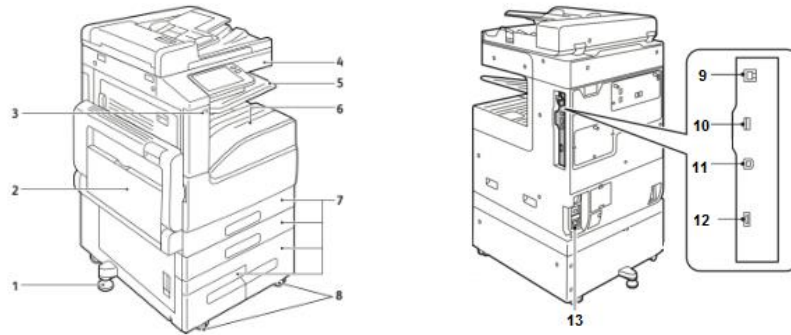
The information in this document is accurate to the best knowledge of the authors and is provided without warranty of any kind. In no event shall Xerox be liable for any damages whatsoever resulting from user's use or disregard of the information provided in this document including direct, indirect,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

---

## 2 Product Description

### Physical Components

AltaLink® and 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 handlers, etc. may vary configuration, however, they are not relevant to security and are not discussed.

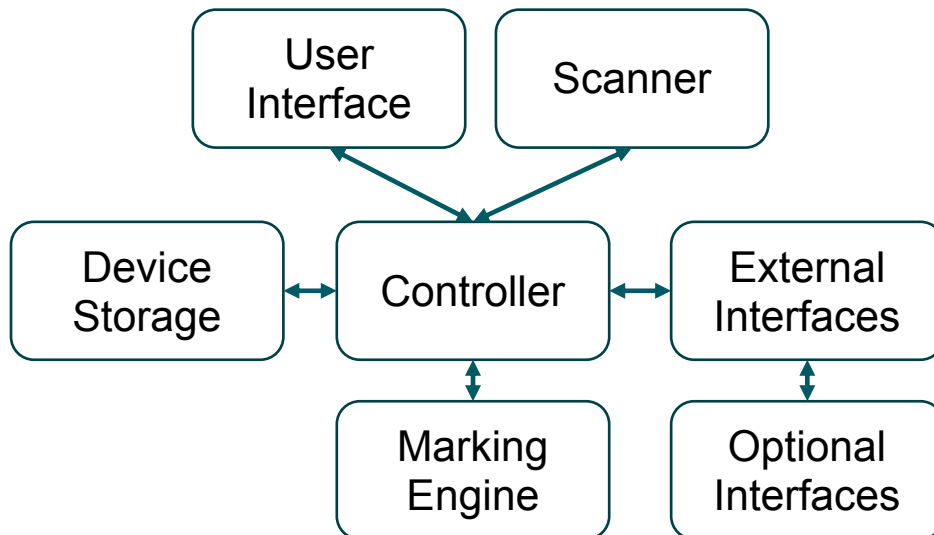


- |  |   |
|--|---|
| <ul style="list-style-type: none"> <li>1. Stabilizer.</li> <li>2. Bypass paper feed tray.</li> <li>3. Front USB Port(s)*</li> <li>4. Touch screen user interface.</li> <li>5. Upper paper tray.</li> <li>6. Lower paper tray.</li> <li>7. Paper feed trays.</li> </ul> | <ul style="list-style-type: none"> <li>8. Caster wheels.</li> <li>9. Rear USB Port(s)*</li> <li>10. Optional Wi-Fi dongle port*</li> <li>11. RJ45 Ethernet connection*</li> <li>12. Service port<br/>(May require disassembly to access).</li> <li>13. AC Power.</li> </ul> |
|--|---|

\*Denotes a security related component

### Architecture

AltaLink® and 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. AltaLink® and 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 that 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 conforms 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 can be disabled completely by a system administrator.

## **Optional Equipment**

---

### **RJ-11 Analog Fax and Telephone**

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

### **Wireless Network Connector**

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

AltaLink® products accept an optional wireless kit that can be installed in the rear USB 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. AltaLink® products come standard with an RFID reader built into the front panel. 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. Note that encryption may be disabled to enhance performance on AltaLink® products (though this is not recommended in secure environments). Xerox VersLink products do not have such an option.

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.

#### **TPM Chip**

Some models include a Trusted Platform Module (TPM). The TPM is compliant with ISO/IEC 11889, the international standard for a secure cryptoprocessor, 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)**

AltaLink® and 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.

---

#### **Immediate Image Overwrite**

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

#### **On-Demand Image Overwrite**

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

## User Data in transit

---

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

### Inbound User Data

#### **Print Job Submission**

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

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

### Outbound User Data

#### **Scanning to Network Repository, Email, Fax Server**

AltaLink® and 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 and WPA 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  |
| SMBv3        | Optional   | Encryption may be enabled on a Windows share. AltaLink® products currently support SMB encryption. 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**

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**

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 3<sup>rd</sup> party vendor. (For example, Microsoft O365 or Google apps would utilize Microsoft & Google's security mechanisms respectively). Please consult documentation for individual Apps and 3<sup>rd</sup> party security for details.

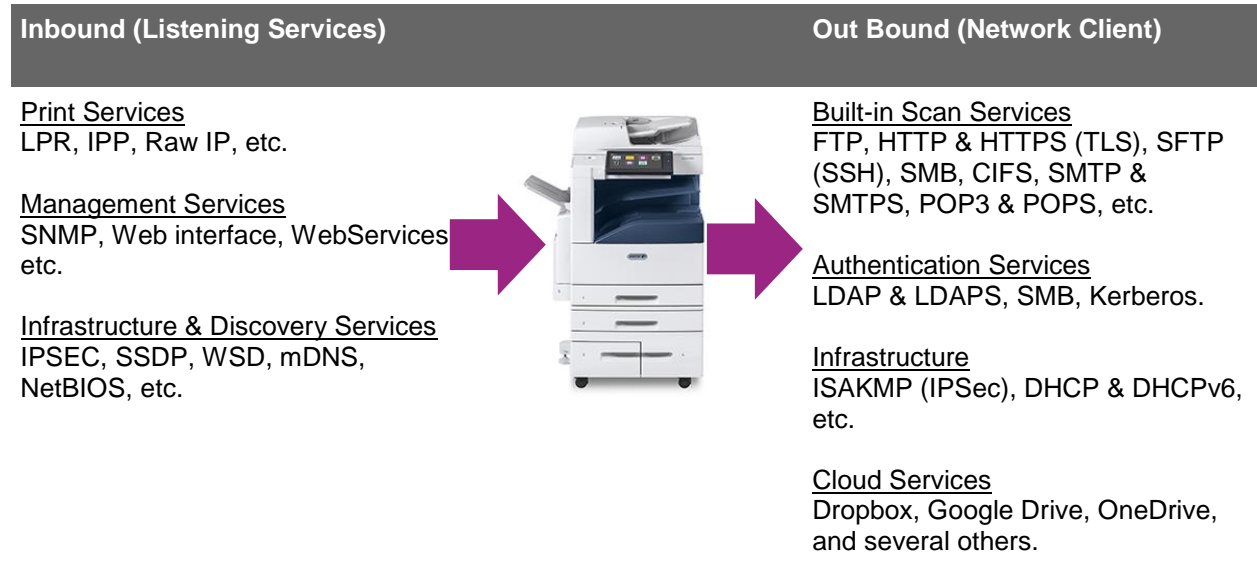
|  | <b>AltaLink® Multifunction</b>                                       | <b>VersaLink® Multifunction</b>   | <b>VersaLink® Printers</b>  |
|--|--|---|---|
|  | B8045, B8055, B8065, B8075, B8090, C8030, C8035, C8045, C8055, C8070 | B405, B605, B615, B7025, B7030, B7035, C405, C505, C605, C7020, C7025, C7030        | B400, B600, B610, C400, C500, C600, C7000, C8000, C9000                             |
| <b>Local Data Encryption (HDD, SDD, IC, SD Card)</b>     | AES-256  | AES-256   | AES-256   |
| <b>Federal Information Protection Standard 140-2</b>     | Yes  | Yes   | Yes   |
| <b>Media Sanitization NIST 800-171 (Image Overwrite)</b> | All models use magnetic HDD  | Models with magnetic HDD. See <a href="#">Appendix A: Product Security Profiles</a> | Models with magnetic HDD. See <a href="#">Appendix A: Product Security Profiles</a> |
| <b>Print Submission</b>                                  |  |   |   |
|  | IPPS (TLS)   | Supported   | Supported   |
|  | HTTPS (TLS)  | Supported   | Supported   |
|  | Xerox Print Stream Encryption  | Supported   | (Not currently supported)   |
| <b>Scan to Repository Server</b>                         |  |   |   |
|  | HTTPS (TLS)  | 1.2   | (Not currently supported)   |
|  | SFTP (SSH)   | SSH-2   | (Not currently supported)   |
|  | SMB (unencrypted)  | v1, v2, v3  | v3  |
|  | SMB (with share encryption enabled)                                  | V3  | (Not currently supported)   |
|  | HTTP (unencrypted)   | Supported   | (Not currently supported)   |
|  | FTP (unencrypted)  | Supported   | (Not currently supported)   |
| <b>Scan to Fax Server</b>                                |  |   |   |
|  | HTTPS (TLS)  | 1.2   | (Not currently supported)   |
|  | SFTP (SSH)   | SSH-2   | (Not currently supported)   |
|  | SMB (unencrypted)  | v1, v2, v3  | v3  |
|  | SMB (with share encryption enabled)                                  | V3  | (Not currently supported)   |
|  | S/MIME   | Supported   | Supported   |
|  | HTTP (unencrypted)   | Supported   | (Not currently supported)   |
|  | FTP (unencrypted)  | Supported   | (Not currently supported)   |
|  | SMTP (unencrypted)   | Supported   | Supported   |
| <b>Scan to Email</b>                                     |  |   |   |
|  | S/MIME   | Supported   | Supported   |
|  | SMTP (unencrypted)   | Supported   | Supported   |

## 4 Network Security

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

### TCP/IP Ports & 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.

| Port       | Type    | Service Name   |
|------------|---------|--|
| 80 or 443  | TCP     | HTTP including:<br>Web User Interface<br>UPnP Discovery<br>Web Services for Products (WSD)<br>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. AltaLink® and VersaLink® products support IPsec for both IPv4 and IPv6 protocols.

|       | AltaLink® Multifunction  | VersaLink® Multifunction  | VersaLink® Printers                                     |
|-------|--|---|---|
|       | B8045, B8055, B8065, B8075, B8090, C8030, C8035, C8045, C8055, C8070 | B405, B605, B615, B7025, B7030, B7035, C405, C505, C605, C7020, C7025, C7030                        | B400, B600, B610, C400, C500, C600, C7000, C8000, C9000 |
| IPSec |  |   |   |
|       | Supported IP Versions  | IPv4, IPv6  | IPv4, IPv6  |
|       | Key exchange authentication method                                   | Preshared Key & digital signature, device authentication certificate, server validation certificate | Preshared Key & digital signature                       |
|       | Transport Mode   | Transport & Tunnel mode   | Transport mode only                                     |
|       | Security Protocol  | ESP & AH  | ESP only  |
|       | ESP Encryption Method  | AES, 3DES, Null   | AES, 3DES, DES  |
|       | ESP Authentication Methods   | SHA1, SHA256, None  | SHA1, SHA256, None                                      |

**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.

|                       |                           | <b>AltaLink® Multifunction</b>   | <b>VersaLink® Multifunction</b>   | <b>VersaLink® Printers</b>  |
|-----------------------|---------------------------|--|---|---|
|                       |                           | <b>B8045, B8055, B8065, B8075, B8090, C8030, C8035, C8045, C8055, C8070</b>  | <b>B405, B605, B615, B7025, B7030, B7035, C405, C505, C605, C7020, C7025, C7030</b>                           | <b>B400, B600, B610, C400, C500, C600, C7000, C8000, C9000</b>  |
| <b>Wi-Fi (802.11)</b> |                           |  |   |   |
|                       | No Encryption             | Supported  | Supported   | Supported   |
|                       | WEP                       | RC4  | RC4   | RC4   |
|                       | WPA2 Personal (PSK)       | CCMP (AES), TKIP, TKIP+CCMP (AES)  | CCMP (AES)  | CCMP (AES)  |
|                       | WPA2 Enterprise           | CCMP (AES), TKIP, TKIP+CCMP (AES)<br>--<br>PEAPv0 MS-CHAPv2<br>EAP-TLS<br>EAP-TTLS/PAP<br><br>EAP-TTLS/MS-CHAPv2<br>EAP-TTLS/EAP-TLS | CCMP (AES) + TKIP<br>--<br>PEAPv0 MS-CHAPv2<br>EAP-TLS<br>EAP-TTLS/PAP<br>EAP-TTLS/CHAP<br>EAP-TTLS/MS-CHAPv2 | CCMP (AES) + TKIP<br>--<br>PEAPv0 MS-CHAPv2<br>EAP-TLS<br>EAP-TTLS/PAP<br>EAP-TTLS/CHAP<br>EAP-TTLS/MS-CHAPv2 |
|                       | BSSID Roaming Restriction | Supported  | (Not Currently Supported)   | (Not Currently Supported)   |

**TLS**

AltaLink® and VersaLink® products support the latest version, TLS 1.2.

|                               |                       | <b>AltaLink® Multifunction</b>  | <b>VersaLink® Multifunction</b>   | <b>VersaLink® Printers</b>                                     |
|-------------------------------|-----------------------|---|---|--|
|                               |                       | <b>B8045, B8055, B8065, B8075, B8090, C8030, C8035, C8045, C8055, C8070</b> | <b>B405, B605, B615, B7025, B7030, B7035, C405, C505, C605, C7020, C7025, C7030</b> | <b>B400, B600, B610, C400, C500, C600, C7000, C8000, C9000</b> |
| <b>TLS Versions Supported</b> |                       |   |   |  |
|                               | Product Web Interface | 1.2, 1.1, 1.0   | 1.2, 1.1, 1.0   | 1.2, 1.1, 1.0  |
|                               | Product Web Services  | 1.2, 1.1, 1.0   | 1.2, 1.1, 1.0   | 1.2, 1.1, 1.0  |
|                               | Product IPPS printing | 1.2, 1.1, 1.0   | 1.2, 1.1, 1.0   | 1.2, 1.1, 1.0  |
|                               | Remote control        | 1.2   | 1.2   | 1.2  |



## **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**

AltaLink® and 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.

|                            | <b>AltaLink® Multifunction</b>                                       | <b>VersaLink® Multifunction</b>  | <b>VersaLink® Printers</b>                              |
|----------------------------|--|--|---|
|                            | B8045, B8055, B8065, B8075, B8090, C8030, C8035, C8045, C8055, C8070 | B405, B605, B615, B7025, B7030, B7035, C405, C505, C605, C7020, C7025, C7030 | B400, B600, B610, C400, C500, C600, C7000, C8000, C9000 |
| <b>Device Certificates</b> |  |  |   |
| Certificate Length         | 1024, 2048   | 1024, 2048   | 1024, 2048  |
| Supported Hashes           | SHA1, SHA256   | SHA256, SHA384, SHA512   | SHA256, SHA384, SHA512                                  |
| Product Web Server         | Supported  | Supported  | Supported   |
| IPPS (TLS) Printing        | Supported  | Supported  | Supported   |
| 802.1X Client              | Supported  | Supported  | Supported   |
| Email Signing              | Supported  | Supported  | (Not Applicable)  |
| Email Encryption           | Supported  | Supported  | (Not Applicable)  |
| OCSP Signing               | Supported  | Supported  | Supported   |
| IPSec                      | Supported  | (Not currently supported)  | (Not currently supported)                               |

|  |      |           |                           |                  |
|--|------|-----------|---------------------------|------------------|
|  | SFTP | Supported | (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.

| AltaLink® Multifunction  | VersaLink® Multifunction   | VersaLink® Printers                                     |
|--|--|---|
| B8045, B8055, B8065, B8075, B8090, C8030, C8035, C8045, C8055, C8070 | B405, B605, B615, B7025, B7030, B7035, C405, C505, C605, C7020, C7025, C7030 | B400, B600, B610, C400, C500, C600, C7000, C8000, C9000 |

| Trusted Certificates |                                    |   |  |  |
|----------------------|------------------------------------|---|--|--|
|                      | Minimum Length Restriction Options | None, 1024, 2048  | 1024, 2048                               | 1024, 2048                               |
|                      | Maximum Length                     | 4096  | 4096                                     | 4096                                     |
|                      | Supported Hashes                   | SHA1/224/256/384/512  | SHA1/224/256/384/512                     | SHA1/224/256/384/512                     |
|                      | Supported Formats                  | .cer, .crt, .der, .pem, PKCS#7 (.p7b), PKCS#12 (.pfx, .p12) | .cer, .der, PKCS#7, PKCS#12 (.pfx, .p12) | .cer, .der, PKCS#7, PKCS#12 (.pfx, .p12) |
|                      | IPSec                              | Supported   | Supported                                | Supported                                |
|                      | LDAP                               | Supported   | Supported                                | Supported                                |
|                      | Scanning (HTTPS/TLS)               | Supported   | (Not currently supported)                | (Not Applicable)                         |
|                      | Scanning (SFTP/SSH)                | Used for audit log transfer                                 | (Not currently supported)                | (Not Applicable)                         |
|                      | 802.1X Client                      | Supported   | Supported                                | Supported                                |
|                      | Email Signing                      | Supported   | Supported                                | (Not Applicable)                         |
|                      | Email Encryption                   | Supported   | Supported                                | (Not Applicable)                         |
|                      | OCSP Signing                       | Supported   | Supported                                | Supported                                |

### Certificate Validation

AltaLink® and 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.

|              |            | AltaLink® Multifunction  | VersaLink® Multifunction   | VersaLink® Printers                                     |
|--------------|------------|--|--|---|
|              |            | B8045, B8055, B8065, B8075, B8090, C8030, C8035, C8045, C8055, C8070 | B405, B605, B615, B7025, B7030, B7035, C405, C505, C605, C7020, C7025, C7030 | B400, B600, B610, C400, C500, C600, C7000, C8000, C9000 |
| Email S/MIME |            |  |  |   |
|              | Versions   | v3   | v2, v3, v3.2   | (Not Applicable)  |
|              | Digest     | SHA1, SHA256, SHA384, SHA512   | MD5, SHA1, SHA256  | (Not Applicable)  |
|              | Encryption | 3DES, AES128, AES192, AES256   | 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:

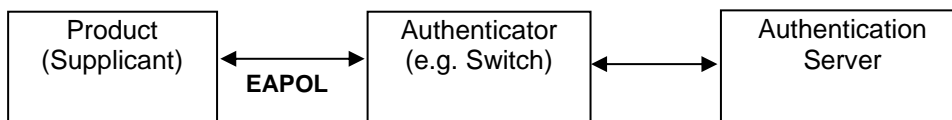
- Message integrity to ensure that a packet has not been tampered with in transit
- Authentication to verify that the message is from a valid source
- Encryption of packets to prevent unauthorized access

|        |            | AltaLink® Multifunction  | VersaLink® Multifunction   | VersaLink® Printers                                     |
|--------|------------|--|--|---|
|        |            | B8045, B8055, B8065, B8075, B8090, C8030, C8035, C8045, C8055, C8070 | B405, B605, B615, B7025, B7030, B7035, C405, C505, C605, C7020, C7025, C7030 | B400, B600, B610, C400, C500, C600, C7000, C8000, C9000 |
| SNMPv3 |            |  |  |   |
|        | Digest     | SHA1, MD5  | SHA1, MD5  | SHA1, MD5   |
|        | Encryption | DES, AES128  | 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.



|                        |                        |   |   |   | AltaLink® Multifunction  | VersaLink® Multifunction   | VersaLink® Printers                                     |
|------------------------|------------------------|---|---|---|--|--|---|
|                        |                        |   |   |   | B8045, B8055, B8065, B8075, B8090, C8030, C8035, C8045, C8055, C8070 | B405, B605, B615, B7025, B7030, B7035, C405, C505, C605, C7020, C7025, C7030 | B400, B600, B610, C400, C500, C600, C7000, C8000, C9000 |
| Network Access Control |                        |   |   |   |  |  |   |
|                        | 802.1x                 | Supported   | Supported                               | Supported                               |  |  |   |
|                        | Authentication Methods | PSK, AES (CCMP)/TKIP, PEAPv0/MS-CHAPv2, EAP-TLS, EAP-TTLS/PAP, EAP-TTLS/MS-CHAPv2, EAP-TTLS/EAP-TLS | 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 AltaLink® and VersaLink®, 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

|                        |           | AltaLink® Multifunction  | VersaLink® Multifunction   | VersaLink® Printers                                     |
|------------------------|-----------|--|--|---|
|                        |           | B8045, B8055, B8065, B8075, B8090, C8030, C8035, C8045, C8055, C8070 | B405, B605, B615, B7025, B7030, B7035, C405, C505, C605, C7020, C7025, C7030 | B400, B600, B610, C400, C500, C600, C7000, C8000, C9000 |
| Network Access Control |           |  |  |   |
|                        | Cisco ISE | Supported  | 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 AltaLink® and 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.

AltaLink® products include FIPS compliant algorithms of SNMPv3 and Kerberos, however an exception can be approved to run these in non-FIPS compliant mode when configured for non-FIPS algorithms.

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

Additional network security controls are discussed in the following sections.

### Endpoint Firewall Options

|          |  | AltaLink® Multifunction  | VersaLink® Multifunction   | VersaLink® Printers                                     |
|----------|--|--|--|---|
|          |  | B8045, B8055, B8065, B8075, B8090, C8030, C8035, C8045, C8055, C8070 | B405, B605, B615, B7025, B7030, B7035, C405, C505, C605, C7020, C7025, C7030 | B400, B600, B610, C400, C500, C600, C7000, C8000, C9000 |
| Firewall |  | Stateful Packet Filter   | IP Whitelisting  | IP Whitelisting   |

|  |                   |           |                           |                           |
|--|-------------------|-----------|---------------------------|---------------------------|
|  | Stateful Firewall | Supported | (Not currently supported) | (Not currently supported) |
|  | IP Whitelist      | Supported | Supported                 | Supported                 |

**IP Whitelisting (IP Address Filtering)**

VersaLink® products support IP Whitelisting only.

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

**Stateful Firewall (Advanced IP Filtering)**

AltaLink® products support stateful packet inspection that it tracks connections and packet flows. Rules may be configured that examine incoming and outgoing packets. Packets are matched against each rule in order until a match occurs and allows the packet to be accepted, rejected, or dropped.

## 5 Device Security: BIOS, Firmware, OS, Runtime, and Operational security controls

AltaLink® and 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.

---

### Boot Process Integrity

---

#### Firmware Integrity & Verification

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

---

### Runtime Intrusion Prevention & Detection

---

#### Runtime Executable Control

- McAfee Embedded Control prevents unauthorized software from executing. This prevents worms, viruses, spyware, and other malware that install themselves from executing illegitimately.

#### Runtime Intrusion Detection – Memory Control

- McAfee Embedded Control ensures that running processes are protected from malicious attempts to hijack them. Unauthorized code injected into a running process is detected and prevented.

#### Event Monitoring & Logging

- The Audit Log feature records security-related events.

---

### Continuous Operational Security

---

#### Firmware and Diagnostic Security Controls

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

## Fail Secure Vs Fail Safe

---

AltaLink® and 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 AltaLink® and 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 AltaLink® and 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, AltaLink® and 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 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.**

AltaLink® and 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 AltaLink® device comes with McAfee Embedded Control built-in and enabled by default. McAfee 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.

Memory control monitors memory and running processes. If unauthorized code is injected into a running process, it is detected and prevented.

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 McAfee® ePolicy Orchestrator® (ePO).

## Event Monitoring & 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:<br>Identity: User Name, Job Name, Computer Name, Printer Name, Folder Name, or Accounting Account ID display when Network Accounting is enabled.<br>Completion Status<br>Image Overwrite Status: The status of overwrites completed on each job. Immediate Image must be enabled. |

AltaLink® products currently support 159 unique security events. 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.

### **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 PSW. 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 & 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 & Security Policy Management Solutions

Xerox Device Manager and Xerox CentreWare® Web (available as a free download) centrally manage Xerox Devices. Additionally, AltaLink® products come with McAfee built in and can be managed with McAfee ePO™ providing an enhanced security posture supporting proactive monitoring, threat detection, and remediation capabilities.

For details please visit [Xerox.com](http://Xerox.com) or speak with a Xerox representative.

## 7 Identification, Authentication, and Authorization

AltaLink® and 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

AltaLink® and 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.

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

#### Password Policy

The following password attributes can be configured:

|  | AltaLink®<br>Multifunction   | VersaLink®<br>Multifunction  | VersaLink® Printers                                     |
|--|--|--|---|
|  | B8045, B8055, B8065, B8075, B8090, C8030, C8035, C8045, C8055, C8070 | B405, B605, B615, B7025, B7030, B7035, C405, C505, C605, C7020, C7025, C7030 | B400, B600, B610, C400, C500, C600, C7000, C8000, C9000 |
| <b>Password Policy</b>   |  |  |   |
| Minimum Length   | 1  | 1  | 1   |
| Maximum Length   | 63   | 63   | 63  |
| Password cannot contain User Name                                  | Supported  | Supported  | Supported   |
| Password complexity options (in addition to alphabetic characters) | Require a number   | Require a number<br>Require non-alphabetic                                   | Require a number<br>Require non-alphabetic              |

### **Network Authentication**

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

|   | <b>AltaLink® Multifunction</b>                                       | <b>VersaLink® Multifunction</b>  | <b>VersaLink® Printers</b>                              |
|---|--|--|---|
|   | B8045, B8055, B8065, B8075, B8090, C8030, C8035, C8045, C8055, C8070 | B405, B605, B615, B7025, B7030, B7035, C405, C505, C605, C7020, C7025, C7030 | B400, B600, B610, C400, C500, C600, C7000, C8000, C9000 |
| <b>Network Authentication Providers</b> |  |  |   |
|   | 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**

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: <http://www.90meter.com/>

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

|                    | <b>AltaLink® Multifunction</b>                                       | <b>VersaLink® Multifunction</b>  | <b>VersaLink® Printers</b>                              |
|--------------------|--|--|---|
|                    | B8045, B8055, B8065, B8075, B8090, C8030, C8035, C8045, C8055, C8070 | B405, B605, B615, B7025, B7030, B7035, C405, C505, C605, C7020, C7025, C7030 | B400, B600, B610, C400, C500, C600, C7000, C8000, C9000 |
| <b>Smart Cards</b> |  |  |   |
|                    | Common Access Card (CAC)   | Supported  | Supported   |
|                    | PIV / PIV II   | Supported  | Supported   |
|                    | Net (Gemalto .Net v1, Gemalto .Net v2)                               | Supported  | Supported   |
|                    | Gemalto MD   | Supported  | (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)**

---

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

## 8 Additional Information & Resources

### Security @ Xerox®

---

Xerox maintains an evergreen public web page that contains the latest security information pertaining to its products. Please see <http://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: <http://www.xerox.com/information-security/information-security-articles-whitepapers/enus.html>

### Additional Resources

---

Below are additional resources.

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

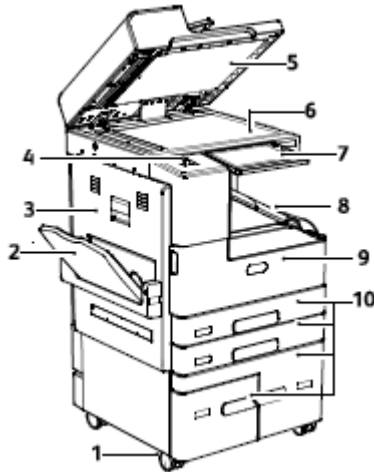
## Appendix A: Product Security Profiles

This appendix describes specific details of each AltaLink® and VersaLink® product.

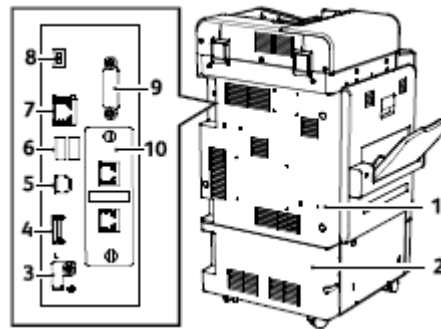


## AltaLink® B8045/B8055/B8065/B8075/B8090

### Physical Overview



1. Locking Caster
2. Tray 5
3. Left Side Door
4. USB Port
5. Document Cover
6. Document Glass
7. Control Panel
8. Center Output Tray
9. Front Door
10. Trays 1-4



1. Upper Rear Cover
2. Lower Rear Cover
3. USB Memory Port, for service only
4. USB Memory Card Connections
5. USB Port, Type B
6. USB Ports, Type A
7. Ethernet Connection
8. Status Indicator
9. Foreign Device Interface (optional)
10. Fax Connections (optional)

### 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.<br>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.<br>Firmware upgrades may be applied using this port.<br>Connection of optional equipment such as NFC or CAC readers.<br>Note: This port can be disabled completely by a system administrator. |

### Encryption and Overwrite

|                    |  |
|--------------------|--|
| Encryption         | AES-256                                  |
| TPM Chip           | (Not Currently Supported)                |
| Media Sanitization | Immediate and On-Demand Image Overwrite. |

**Controller Non-Volatile Storage**

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

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

IC- Integrated Circuit, soldered to circuit board  
 HDD- Magnetic Hard Disk Drive

SSD- Solid State Disk  
 SD Card- Secure Digital Card

**Controller Volatile Memory**

| Size   | Type       | Use  | User Data | How to Clear     | Volatile |
|--|------------|--|-----------|------------------|----------|
| 4GB  | DDR3 SDRAM | 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**

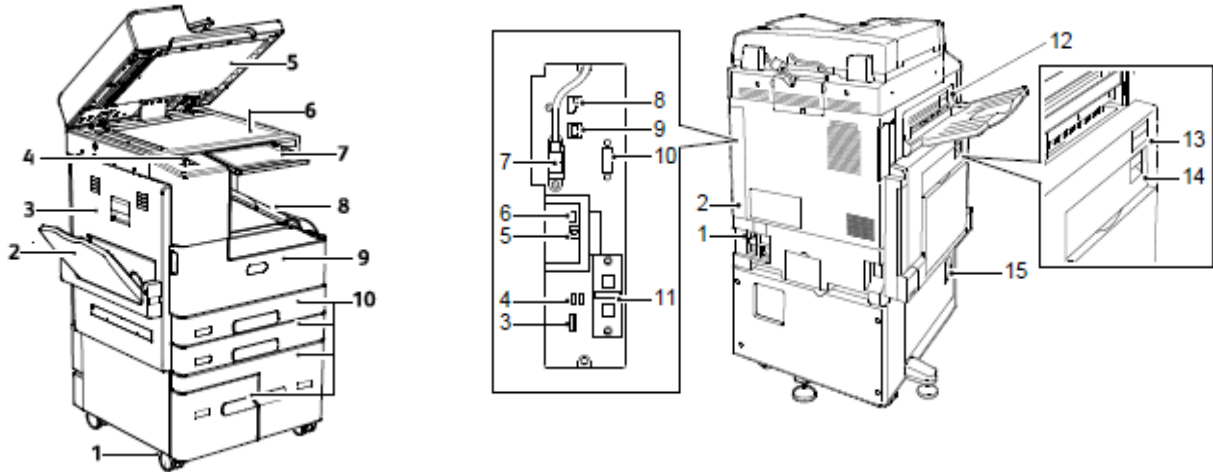
N/A. The marking engine does not contain any non-volatile storage.

**Marking Engine Volatile Memory**

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

## AltaLink® C8030 / C8035 / C8045 / C8055 / C8070

### Physical Overview



- |   |  |
|---|--|
| <ol style="list-style-type: none"> <li>1. Leveler Foot</li> <li>2. Tray 5</li> <li>3. Left Tray</li> <li>4. USB Port</li> <li>5. Document Cover</li> <li>6. Document Glass</li> <li>7. Power/Wake Button</li> <li>8. Control Panel</li> <li>9. Center Output Tray</li> <li>10. Center Bottom Tray</li> <li>11. Main Power Switch behind Front Door</li> </ol> | <ol style="list-style-type: none"> <li>1. Circuit Breaker</li> <li>2. Rear Right Cover</li> <li>3. USB Memory Card Connections and SIM Slot</li> <li>4. USB Port, Type A</li> <li>5. USB Port, Type B</li> <li>6. Status Indicator</li> <li>7. Side 2 Scan Cable</li> <li>8. Data Port, for service only</li> <li>9. Ethernet Connection</li> <li>10. Foreign Device Interface (optional)</li> <li>11. Fax Connections (optional)</li> <li>12. Door D Release Lever</li> <li>13. Door A Release Lever</li> <li>14. Door B Release Lever</li> <li>15. Door C Release Lever</li> </ol> |
|---|--|

### 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.<br>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.<br>Firmware upgrades may be applied using this port.<br>Connection of optional equipment such as NFC or CAC readers.<br>Note: This port can be disabled completely by a system administrator. |

### Encryption and Overwrite

|                    |  |
|--------------------|--|
| Encryption         | AES-256                                  |
| TPM Chip           | (Not Currently Supported)                |
| Media Sanitization | Immediate and On-Demand Image Overwrite. |

**Controller Non-Volatile Storage**

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

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

IC- Integrated Circuit, soldered to circuit board

SSD- Solid State Disk

HDD- Magnetic Hard Disk Drive

SD Card- Secure Digital Card

**Controller Volatile Memory**

| Size   | Type       | Use  | User Data | How to Clear     | Volatile |
|--|------------|--|-----------|------------------|----------|
| 4GB  | DDR3 SDRAM | 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**

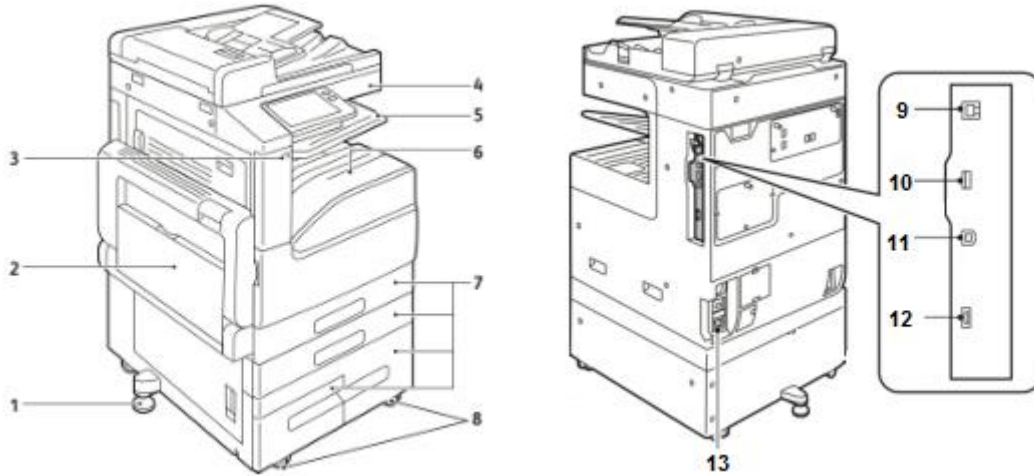
N/A. The marking engine does not contain any non-volatile storage.

**Marking Engine Volatile Memory**

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

## VersaLink® B7025, B7030 B7035

### Physical Overview



- 11. Stabilizer
- 12. Bypass paper feed tray
- 13. USB2.0 (Host Type A)\*
- 14. Touch screen user interface.
- 15. Upper paper tray
- 16. Lower paper tray
- 17. Paper feed trays

- 18. Caster wheels
- 19. USB3.0 (Target Type B)\*
- 20. Optional Wi-Fi dongle port\*
- 21. RJ45 Ethernet connection\*
- 22. Debug serial port (DIN)\*  
(Located under steel plate)
- 23. AC Power

### 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.<br>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.<br>Firmware upgrades may be applied using this port.<br>Connection of optional equipment such as NFC or CAC readers.<br>Note: This port can be disabled completely by a system administrator. |

### 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 | Required      |
| Contains User Data (E.g. Print, Scan, Fax) |     | Yes           |     | Yes           |
| Encryption Support                         |     | Always-On     |     | Always-On     |
| NIST 800-171 Overwrite Support             |     | Yes           |     |               |
| Contains Configuration Settings            |     | Yes           |     | Yes           |
| Encryption Support                         |     | Always-On     |     | Always-On     |
| Customer Erasable                          |     | Factory Reset |     | Factory Reset |

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

IC- Integrated Circuit, soldered to circuit board  
 HDD- Magnetic Hard Disk Drive

SSD- Solid State Disk  
 SD Card- Secure Digital Card

**Controller Volatile Memory**

| Size   | Type      | Use  | User Data | How to Clear     | Volatile |
|--|-----------|--|-----------|------------------|----------|
| 2GB  | 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**

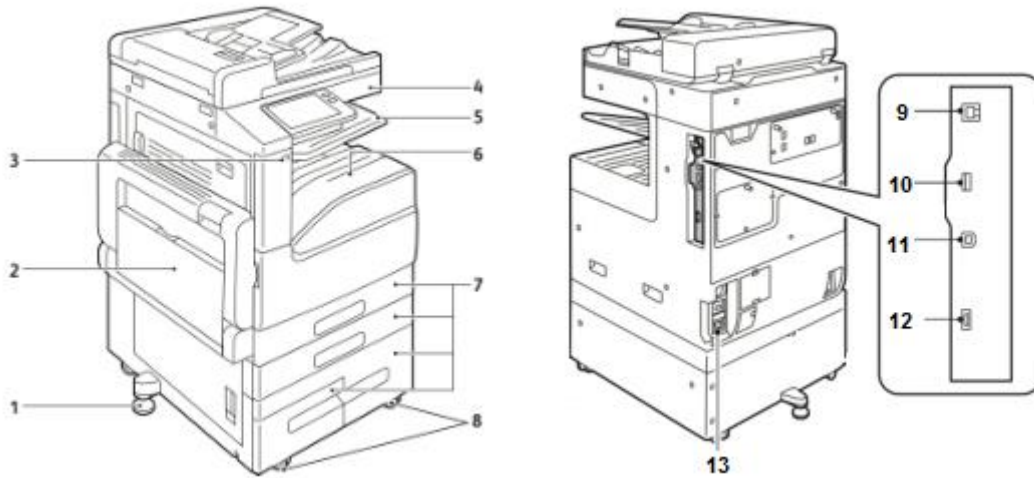
N/A. The marking engine does not contain any non-volatile storage.

**Marking Engine Volatile Memory**

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

## VersaLink® C7000, C7020, C7025, C7030

### 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

|  |   |
|--|---|
| 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.<br>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.<br>Firmware upgrades may be applied using this port.<br>Connection of optional equipment such as NFC or CAC readers.<br>Note: This port can be disabled completely by a system administrator. |

### 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 | Required      |
| Contains User Data (E.g. Print, Scan, Fax) |     | Yes           |     | Yes           |
| Encryption Support                         |     | Always-On     |     | Always-On     |
| NIST 800-171 Overwrite Support             |     | Yes           |     |               |
| Contains Configuration Settings            |     | Yes           |     | Yes           |
| Encryption Support                         |     | Always-On     |     | Always-On     |
| Customer Erasable                          |     | Factory Reset |     | Factory Reset |

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

IC- Integrated Circuit, soldered to circuit board  
 HDD- Magnetic Hard Disk Drive

SSD- Solid State Disk  
 SD Card- Secure Digital Card

**Controller Volatile Memory**

| Size   | Type      | Use  | User Data | How to Clear     | Volatile |
|--|-----------|--|-----------|------------------|----------|
| 2/4GB  | 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.

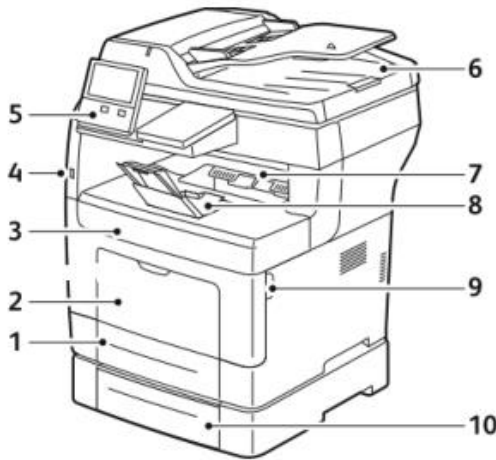
**Marking Engine Volatile Memory**

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

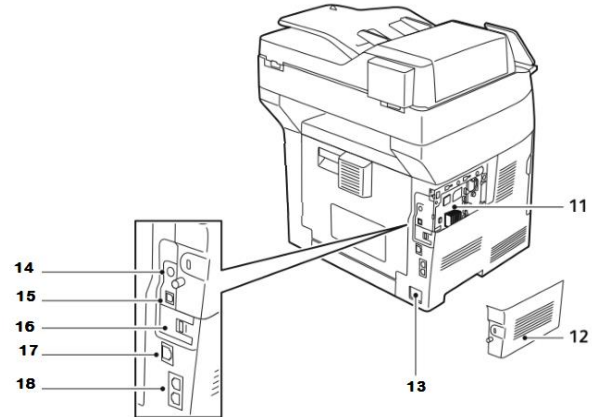


## VersaLink® B400, B405

### Physical Overview



1. Upper Paper Tray
2. Special Paper Feed
3. Front Bezel
4. USB 2.0 (A)
5. Touch Screen User Interface , Power Button and Optional NFC
6. Document Feeder
7. Catch Tray
8. Catch Tray Extension
9. Jam Clearance Open



10. Lower Paper Tray
11. Optional SSD Install Location
12. SSD Install Location Cover
13. AC Power
14. Foreign Device Interface
15. USB 3.0 (B)
16. Optional Wireless Adapter Connector
17. RJ-45 Ethernet Connector
18. RJ-11 Fax and Telephone Connector

### 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.<br>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.<br>Firmware upgrades may be applied using this port.<br>Connection of optional equipment such as NFC or CAC readers.<br>Note: This port can be disabled completely by a system administrator. |

### 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 |
|--|---------------|-----|---------------|---------|
|  | Required      | N/A | Optional      | N/A     |
| Contains User Data (E.g. Print, Scan, Fax) |               |     | Yes           |         |
| Encryption Support                         |               |     | Always-On     |         |
| NIST 800-171 Overwrite Support             |               |     | Yes           |         |
| Contains Configuration Settings            | Yes           |     | Yes           |         |
| Encryption Support                         | Always-On     |     | Always-On     |         |
| Customer Erasable                          | Factory Reset |     | Factory Reset |         |

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

IC- Integrated Circuit, soldered to circuit board  
 HDD- Magnetic Hard Disk Drive

SSD- Solid State Disk  
 SD Card- Secure Digital Card

**Controller Volatile Memory**

| Size   | Type      | Use  | User Data | How to Clear     | Volatile |
|--|-----------|--|-----------|------------------|----------|
| 2GB  | 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**

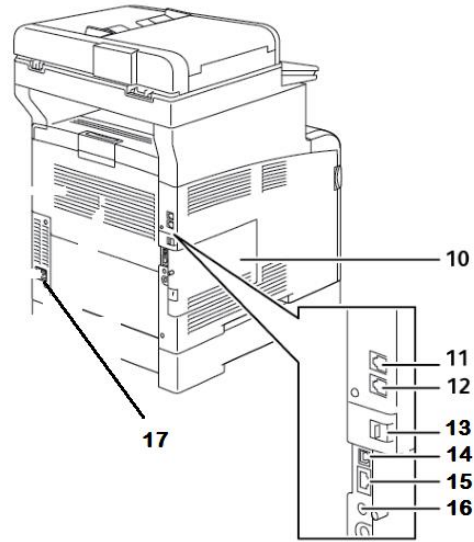
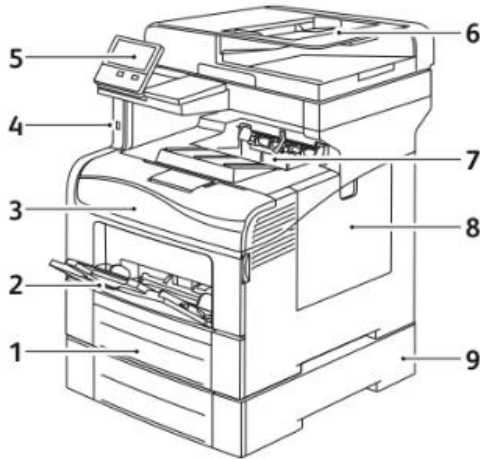
N/A. The marking engine does not contain any non-volatile storage.

**Marking Engine Volatile Memory**

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

## VersaLink® C400, C405

### Physical Overview



1. Upper Paper Tray
2. Special Paper Feed
3. Front Bezel
4. USB 2.0 (A)
5. Touch Screen User Interface, Power Button and Optional NFC
6. Document Feeder
7. Catch Tray
8. Side Panel

9. Lower Paper Tray
10. Service Panel
11. RJ-11 Fax and Telephone Connector
12. RJ-11 Fax and Telephone Connector
13. Optional Wireless Adapter Connector
14. USB 3.0 (B)
15. RJ-45 Ethernet Connector
16. Foreign Device Interface
17. AC Power

### 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.<br>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.<br>Firmware upgrades may be applied using this port.<br>Connection of optional equipment such as NFC or CAC readers.<br>Note: This port can be disabled completely by a system administrator. |

### 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 |
|--|---------------|---------------|-----|---------|
|  | Required      | Optional      | N/A | N/A     |
| Contains User Data (E.g. Print, Scan, Fax) |               | Yes           |     |         |
| Encryption Support                         |               | Always-On     |     |         |
| NIST 800-171 Overwrite Support             |               | Yes           |     |         |
|  |               |               |     |         |
| Contains Configuration Settings            | Yes           | Yes           |     |         |
| Encryption Support                         | Always-On     | Always-On     |     |         |
| Customer Erasable                          | Factory Reset | Factory Reset |     |         |

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

IC- Integrated Circuit, soldered to circuit board  
 HDD- Magnetic Hard Disk Drive

SSD- Solid State Disk  
 SD Card- Secure Digital Card

**Controller Volatile Memory**

| Size   | Type      | Use  | User Data | How to Clear     | Volatile |
|--|-----------|--|-----------|------------------|----------|
| 2GB  | 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**

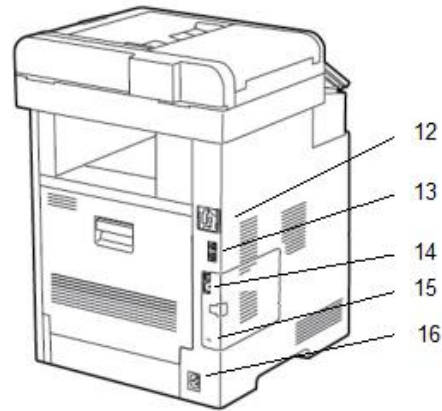
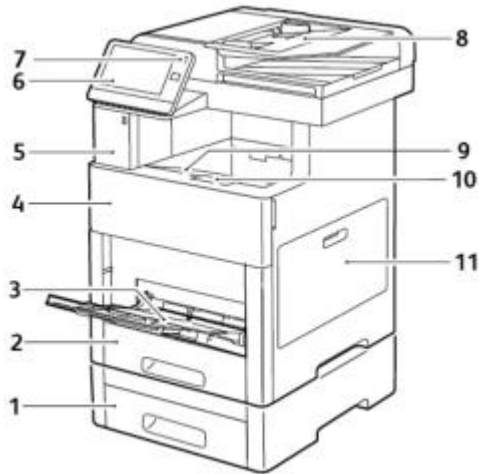
**N/A. The marking engine does not contain any non-volatile storage.**

**Marking Engine Volatile Memory**

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

## VersaLink® C500, C600, C505, C605

### Physical Overview



1. Paper feed tray.
2. Paper feed tray.
3. Bypass paper feed tray.
4. Front bezel.
5. USB2.0(A).
6. Touch screen user interface.
7. System power button.
8. Document feeder.

9. Document output tray.
10. Document output tray extension.
11. Jam clearance panel.
12. Optional Wi-Fi dongle connection.
13. RJ11 Fax
14. USB3.0 (B) & RJ45 Ethernet connection.
15. Foreign device interface.
16. AC Power.

### 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.<br>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.<br>Firmware upgrades may be applied using this port.<br>Connection of optional equipment such as NFC or CAC readers.<br>Note: This port can be disabled completely by a system administrator. |

### 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 |
|--|---------------|---------------|-----|---------|
|  | Required      | Optional      | N/A | N/A     |
| Contains User Data (E.g. Print, Scan, Fax) |               | Yes           |     |         |
| Encryption Support                         |               | Always-On     |     |         |
| NIST 800-171 Overwrite Support             |               | Yes           |     |         |
| Contains Configuration Settings            | Yes           | Yes           |     |         |
| Encryption Support                         | Always-On     | Always-On     |     |         |
| Customer Erasable                          | Factory Reset | Factory Reset |     |         |

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

IC- Integrated Circuit, soldered to circuit board  
 HDD- Magnetic Hard Disk Drive

SSD- Solid State Disk  
 SD Card- Secure Digital Card

**Controller Volatile Memory**

| Size   | Type      | Use  | User Data | How to Clear     | Volatile |
|--|-----------|--|-----------|------------------|----------|
| 2/4GB  | 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**

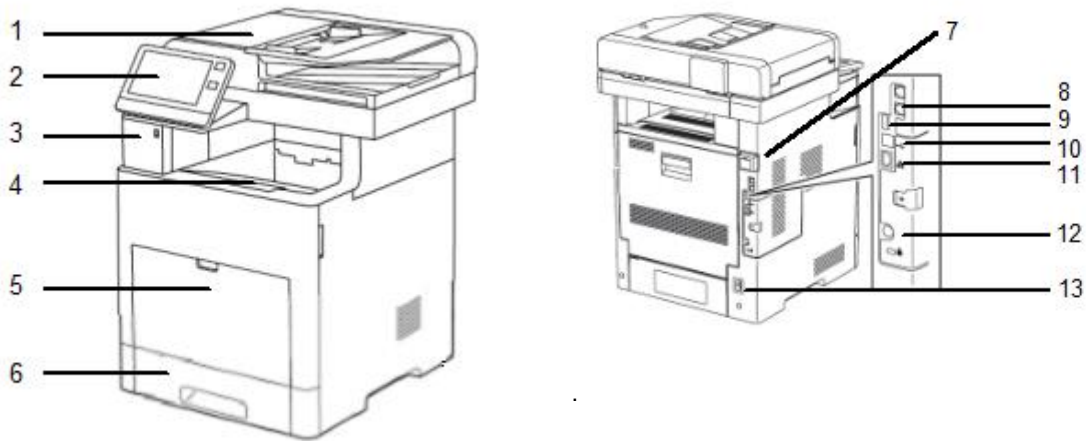
**N/A. The marking engine does not contain any non-volatile storage.**

**Marking Engine Volatile Memory**

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

## VersaLink® B600, B605, B610, B615

### Physical Overview



1. Document feeder.
2. Touch screen user interface.
3. USB2.0(A).
4. Document output tray.
5. Bypass paper feed.
6. Paper tray

7. Optional Wi-Fi dongle connection.
8. Optional RJ11 Fax
9. USB2.0(A)
10. USB3.0(B)
11. RJ45 Ethernet
12. Foreign device interface.
13. AC Power.

### 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.<br>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.<br>Firmware upgrades may be applied using this port.<br>Connection of optional equipment such as NFC or CAC readers.<br>Note: This port can be disabled completely by a system administrator. |

### 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 |
|--|---------------|---------------|-----|---------|
|  | Required      | Optional      | N/A | N/A     |
| Contains User Data (E.g. Print, Scan, Fax) |               | Yes           |     |         |
| Encryption Support                         |               | Always-On     |     |         |
| NIST 800-171 Overwrite Support             |               | Yes           |     |         |
| Contains Configuration Settings            | Yes           | Yes           |     |         |
| Encryption Support                         | Always-On     | Always-On     |     |         |
| Customer Erasable                          | Factory Reset | Factory Reset |     |         |

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

IC- Integrated Circuit, soldered to circuit board  
 HDD- Magnetic Hard Disk Drive

SSD- Solid State Disk  
 SD Card- Secure Digital Card

**Controller Volatile Memory**

| Size   | Type      | Use  | User Data | How to Clear     | Volatile |
|--|-----------|--|-----------|------------------|----------|
| 2GB  | 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.

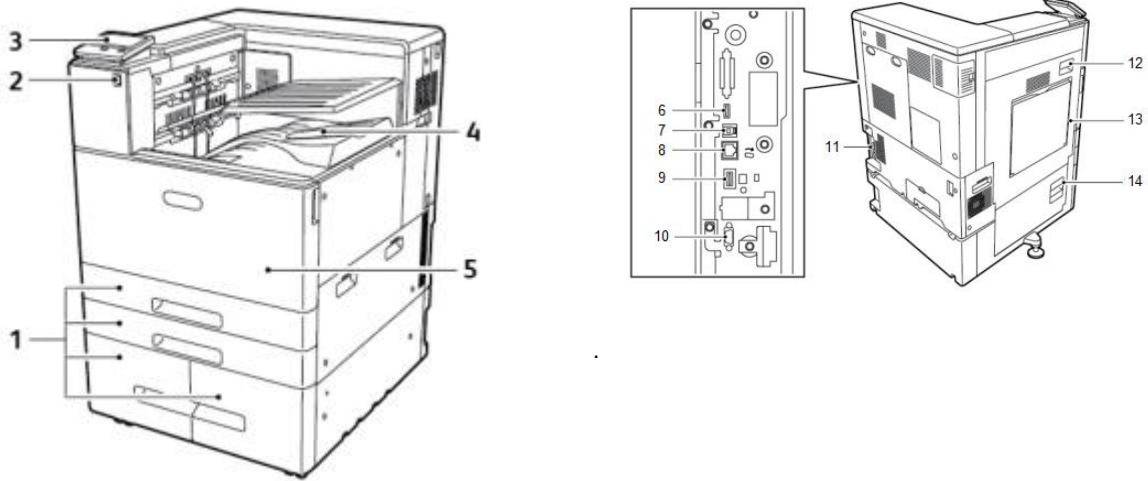
**Marking Engine Volatile Memory**

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



## VersaLink® C8000, C9000

### Physical Overview



- |  |   |
|--|---|
| <ul style="list-style-type: none"> <li>1. Paper feed tray.</li> <li>2. USB2.0(A).</li> <li>3. Touch screen user interface.</li> <li>4. Document output tray.</li> <li>5. Jam clearance panel.</li> </ul> | <ul style="list-style-type: none"> <li>6. USB2.0(A).</li> <li>7. USB3.0(B).</li> <li>8. RJ45 Ethernet connection.</li> <li>9. Optional Wi-Fi dongle connection.</li> <li>10. Foreign device interface.</li> <li>11. AC Power.</li> <li>12. Jam clearance panel.</li> <li>13. Special paper tray.</li> <li>14. Jam clearance panel.</li> </ul> |
|--|---|

### 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.<br>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.<br>Firmware upgrades may be applied using this port.<br>Connection of optional equipment such as NFC or CAC readers.<br>Note: This port can be disabled completely by a system administrator. |
| Product Service Port                         | Used only by Xerox service technicians. Port is covered by a metal plate.   |

### 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 | Required      |
| Contains User Data (E.g. Print, Scan, Fax) |     | Yes           |     | Yes           |
| Encryption Support                         |     | Always-On     |     | Always-On     |
| NIST 800-171 Overwrite Support             |     | Yes           |     |               |
| Contains Configuration Settings            |     | Yes           |     | Yes           |
| Encryption Support                         |     | Always-On     |     | Always-On     |
| Customer Erasable                          |     | Factory Reset |     | Factory Reset |

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

IC- Integrated Circuit, soldered to circuit board  
 HDD- Magnetic Hard Disk Drive

SSD- Solid State Disk  
 SD Card- Secure Digital Card

**Controller 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.

## Appendix B: Security Events

### Xerox AltaLink® Security Events

---

| <b>ID</b> | <b>Event</b>                  | <b>Description</b>  |
|-----------|-------------------------------|---|
| 1         | System startup                | Device name<br>Device serial number   |
| 2         | System shutdown               | Device name<br>Device serial number   |
| 3         | Manual ODIO Standard started  | Device name<br>Device serial number   |
| 4         | Manual ODIO Standard complete | Device name<br>Device serial number<br>Overwrite Status   |
| 5         | Print job                     | Job name<br>User Name<br>Completion Status<br>IIO status<br>Accounting User ID<br>Accounting Account ID   |
| 6         | Network scan job              | Job name<br>User Name<br>Completion Status<br>IIO status<br>Accounting User ID<br>Accounting Account ID<br>total-number-net-destination<br>net-destination.                                     |
| 7         | Server fax job                | Job name<br>User Name<br>Completion Status<br>IIO status<br>Accounting User ID<br>Accounting Account ID<br>Total-fax-recipient-phone-numbers<br>fax-recipient-phone-numbers<br>net-destination. |
| 8         | IFAX                          | Job name<br>User Name<br>Completion Status<br>IIO status<br>Accounting User ID<br>Accounting Account ID<br>total-number-of-smtp-recipients<br>smtp-recipients                                   |

|    |                           |   |
|----|---------------------------|---|
| 9  | Email job                 | Job name<br>User Name<br>Completion Status<br>IIO status<br>Accounting User ID<br>Accounting Account ID<br>total-number-of-smtp-recipients<br>smtp-recipients               |
| 10 | Audit Log Disabled        | Device name<br>Device serial number   |
| 11 | Audit Log Enabled         | Device name<br>Device serial number   |
| 12 | Copy                      | Job name<br>User Name<br>Completion Status<br>IIO status<br>Accounting User ID<br>Accounting Account ID<br>Total-fax-recipient-phone-numbers<br>fax-recipient-phone-numbers |
| 13 | Efax                      | Job name<br>User Name<br>Completion Status<br>IIO status<br>Accounting User ID<br>Accounting Account ID<br>Total-fax-recipient-phone-numbers<br>fax-recipient-phone-numbers |
| 14 | Lan Fax Job               | Job name<br>User Name<br>Completion Status<br>IIO status<br>Accounting User ID<br>Accounting Account ID<br>Total-fax-recipient-phone-numbers<br>fax-recipient-phone-numbers |
| 15 | Data Encryption enabled   | Device name<br>Device serial number   |
| 16 | Manual ODIO Full started  | Device name<br>Device serial number   |
| 17 | Manual ODIO Full complete | Device name<br>Device serial number<br>Overwrite Status   |
| 18 | Data Encryption disabled  | Device name<br>Device serial number   |
| 20 | Scan to Mailbox job       | Job name or Dir name<br>User Name<br>Completion Status<br>IIO status  |
| 21 | Delete File/Dir           | Job name or Dir name<br>User Name<br>Completion Status<br>IIO status  |

|    |                      |  |
|----|----------------------|--|
| 23 | Scan to Home         | UserName<br>Device name<br>Device serial number<br>Completion Status (Enabled/Disabled)  |
| 24 | Scan to Home job     | Job name or Dir name<br>User Name<br>Completion Status (Normal/Error)<br>IIO status<br>Accounting User ID-Name<br>Accounting Account ID-Name<br>total-number-net-destination<br>net-destination  |
| 25 | Copy store job       | Job name or Dir name<br>User Name<br>Completion Status (Normal/Error)<br>IIO status  |
| 26 | PagePack login       | Device name<br>Device serial number<br>Completion Status:<br>Success: (if Passcode is ok)<br>Failed: (if Passcode is not ok)<br>Locked out (if Max Attempts Exceed 5)<br>Time Remaining:<br>Hrs (Remaining for next attempt)<br>Min (Remaining for next attempt) |
| 27 | Postscript Passwords | Device name<br>Device serial number<br>StartupMode (enabled/disabled)<br>System Params Password changed<br>Start Job Password changed  |
| 29 | Network User Login   | UserName<br>Device name<br>Device serial number<br>Completion Status (Success, Failed)   |
| 30 | SA login             | UserName<br>Device name<br>Device serial number<br>Completion Status (Success or Failed)   |
| 31 | User Login           | UserName<br>Device name<br>Device serial number<br>Completion Status (Success or Failed)   |
| 32 | Service Login        | Service name<br>Device name<br>Device serial number<br>Completion status (Success or Failed).  |
| 33 | Audit log download   | UserName<br>Device name<br>Device Serial Number<br>Completion status (Success or Failed).  |
| 34 | IIO feature status   | UserName<br>Device name<br>Device serial number<br>IIO Status (enabled or disabled)  |

|    |  |  |
|----|--|--|
| 35 | SA pin changed                                     | UserName<br>Device name<br>Device serial number<br>Completion status   |
| 36 | Audit log Saved                                    | UserName<br>Device name<br>Device serial number<br>Completion status   |
| 37 | SSL  | UserName<br>Device name<br>Device serial number<br>Completion Status (Enabled/Disabled/Terminated)               |
| 38 | X509 certificate                                   | UserName<br>Device name<br>Device serial number<br>Completion Status (Created/uploaded/Downloaded).              |
| 39 | IP sec Enable/Disable/Configure                    | UserName<br>Device name<br>Device serial number<br>Completion Status<br>(Configured/enabled/disabled/Terminated) |
| 40 | SNMPv3   | UserName<br>Device name<br>Device serial number<br>Completion Status (Configured/enabled/disabled).              |
| 41 | IP Filtering Rules                                 | UserName<br>Device name<br>Device serial number<br>Completion Status (Configured/enabled/disabled).              |
| 42 | Network Authentication<br>Enable/Disable/Configure | UserName<br>Device name<br>Device serial number<br>Completion Status (Enabled/Disabled)                          |
| 43 | Device clock                                       | UserName<br>Device name<br>Device serial number<br>Completion Status (time changed/date changed)                 |
| 44 | SW upgrade   | Device name<br>Device serial number<br>Completion Status (Success, Failed)                                       |
| 45 | Cloning  | Device name<br>Device serial number<br>Completion Status (Success, Failed)                                       |
| 46 | Scan Metadata Validation                           | Device name<br>Device serial number<br>Completion Status (Metadata Validation Success or Failed)                 |
| 47 | Xerox Secure Access<br>Enable/Disable/Configure    | Device name<br>Device serial number<br>Completion status (Configured/enabled/disabled)                           |
| 48 | Service login copy mode                            | Service name<br>Device name<br>Device serial number<br>Completion Status (Success, Failed)                       |

|    |  |  |
|----|--|--|
| 49 | Smartcard (CAC/PIV) access                         | UserName (if valid Card and Password are entered)<br>Device name<br>Device serial number<br>Process Name   |
| 50 | Process terminated                                 | Device name<br>Device serial number<br>Process name  |
| 51 | ODIO scheduled                                     | Device name<br>Device serial number<br>ODIO type (Full or Standard)<br>Scheduled time<br>ODIO status (Started/Completed/canceled)<br>Completion Status (Success/Failed/Canceled) |
| 53 | CPSR Backup  | File Name<br>User Name<br>Completion Status (Normal / Error)<br>IIO Status   |
| 54 | CPSR Restore                                       | File Name<br>User Name<br>Completion Status (Normal / Error)<br>IIO Status   |
| 55 | SA Tools Access Admin                              | Device serial number<br>Completion Status (Locked/Unlocked)  |
| 57 | Session Timer Logout                               | Device Name<br>Device Serial Number<br>Interface (Web, LUI)<br>User Name (who was logged out)<br>Session IP (if available)   |
| 58 | Session Timer Interval Change                      | Device Name<br>Device Serial Number<br>Interface (Web, LUI)(Timer affected by change)<br>User Name (who made this change)<br>Session IP (if available)<br>Completion Status      |
| 59 | Feature Access Control<br>Enable/Disable/Configure | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Enabled/Disabled/Configured)<br>Interface (Web, Local, CAC, SNMP)<br>Session IP address (if available)    |
| 60 | Device Clock NTP Enable/Disable                    | Device Name<br>Device serial number<br>Enable/Disable NTP<br>NTP Server IP Address<br>Completion Status (Success/Failed)   |
| 61 | Grant / Revoke Admin                               | Device Name<br>Device Serial Number<br>User Name (of target user)<br>Grant or Revoke (the admin right)<br>Completion Status (Success/Failed)                                     |
| 62 | Smartcard (CAC/PIV)<br>Enable/Disable/Configure    | UserName<br>Device Name<br>Device Serial Number<br>Completion Status (Success/Failed)  |

|    |  |   |
|----|--|---|
| 63 | IPv6<br>Enable/Disable/Configure                               | UserName<br>Device Name<br>Device Serial Number<br>Completion Status (Success/Failed)   |
| 64 | 802.1x<br>Enable/Disable/Configure                             | UserName<br>Device Name<br>Device Serial Number<br>Completion Status (Success/Failed)   |
| 65 | Abnormal System Termination                                    | Device Name<br>Device Serial Number   |
| 66 | Local Authentication   | UserName<br>Device Name<br>Device Serial Number<br>Completion Status (Enabled/Disabled)   |
| 67 | Web User Interface Authentication<br>(Enable Network or Local) | UserName<br>Device Name<br>Device Serial Number<br>Authentication Method Enabled (Network/Local)  |
| 68 | FIPS Mode<br>Enable/Disable/Configure                          | UserName<br>Device name<br>Device Serial Number<br>Enable/Disable/Configure   |
| 69 | Xerox Secure Access Login                                      | UserName<br>Device Name<br>Device Serial Number<br>Completion Status (Success/Failed)   |
| 70 | Print from USB<br>Enable/Disable                               | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Enabled/Disabled)  |
| 71 | USB Port<br>Enable/Disable                                     | User Name<br>Device Name<br>Device Serial Number<br>USB Port (Front/Rear)<br>Completion Status (Enabled/Disabled)   |
| 72 | Scan to USB<br>Enable/Disable                                  | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Enabled/Disabled)  |
| 73 | System Log Download  | Username<br>IP of requesting device (if available)<br>File names downloaded<br>Destination (IP address or USB device)<br>Completion status (Success/failed) |
| 74 | Scan to USB Job  | Job Name<br>User Name<br>Completion Status<br>IIO Status<br>Accounting User ID-Name<br>Accounting Account ID-Name   |



|    |   |  |
|----|---|--|
| 75 | Remote UI feature   | User Name<br>Device Name<br>Device Serial Number<br>Completion Status<br>(Enabled/Disabled/Configured)   |
| 76 | Remote UI session   | User Name<br>Device Name<br>Device Serial Number<br>Completion Status<br>(Initiated/Terminated)<br>Remote Client IP Address  |
| 77 | Remote Scan Feature<br>Enable/Disable<br>(TWAIN driver)                 | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Enable/Disable)   |
| 78 | Remote Scan Job Submitted<br>(TWAIN driver)                             | UserName (at client if available)<br>IP address of submitting client<br>Device name<br>Device serial number<br>Job name (if accepted)<br>Completion status (accept/reject request) |
| 79 | Scan to Web Service Job<br>(Remote Scan Job Competed)<br>(TWAIN driver) | Job name<br>UserName<br>Accounting User ID-Name<br>Accounting Account ID-Name<br>Completion status<br>Destination  |
| 80 | SMTP Connection Encryption  | UserName<br>Device name<br>Device serial number<br>Completion Status<br>(Enabled for STARTTLS / Enabled for STARTTLS if Avail<br>/ Enabled for SSL/TLS / Disabled)                 |
| 81 | Email Domain Filtering Rule   | User name<br>Device Name<br>Device Serial Number<br>Completion Status (Feature Enabled/Feature Disabled,<br>Rule Added / Rule Deleted)   |
| 82 | Software Self Test Started  | Device Name<br>Device Serial Number  |
| 83 | Software Self Test Complete   | Device Name<br>Device Serial Number<br>Completion Status(Success/Failed/Cancelled)   |
| 84 | McAfee Security State<br>NOTE: ColorQube 8900 ONLY                      | UserName<br>Device name<br>Device serial number<br>Security Mode<br>(Enhanced Security / Integrity Control)<br>Completion Status<br>(Enabled / Disabled / Pending)                 |

|    |  |  |
|----|--|--|
| 85 | McAfee Security Event<br>NOTE: ColorQube 8900 ONLY | Device name<br>Device serial number<br>Type<br>(Read / Modify / Execute / Deluge)<br>McAfee message text   |
| 87 | McAfee Agent<br>NOTE: ColorQube 8900 ONLY          | User name<br>Device name<br>Device serial number<br>Completion Status<br>(Enabled / Disabled)  |
| 88 | Digital Certificate Import Failure                 | Device name  |
| 89 | User Name<br>Add/Delete                            | Device serial number   |
| 90 | User Name Password Change                          | Security Mode  |
| 91 | EFax Job Secure Print Passcode                     | UserName (managing passcodes)<br>Device name<br>Device serial number<br>Completion Status (Passcode Created/Changed)                                   |
| 92 | Scan2Mailbox Folder Password<br>Change             | UserName (managing passwords)<br>Device name<br>Device serial number<br>Folder Name<br>Completion Status (Password was Changed)                        |
| 93 | EFax Mailbox Passcode                              | UserName (managing passcodes)<br>Device name<br>Device serial number<br>Completion Status (Passcode<br>Created/Changed)                                |
| 94 | FTP/SFTP Filing Passive Mode                       | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Enabled / Disabled)   |
| 95 | EFax Forwarding Rule                               | User Name<br>Device Name<br>Device Serial Number<br>Fax Line 1 or 2 (if applicable)<br>Completion Status (Rule Edit / Rule Enabled / Rule<br>Disabled) |
| 96 | EIP Weblets Allow<br>Install                       | UserName<br>Device name<br>Device serial number<br>Completion Status (Enable Installation / Block<br>Installation)                                     |
| 97 | EIP Weblets Install                                | UserName<br>Device name<br>Device serial number<br>Weblet Name<br>Action (Install / Delete)<br>Completion (Success / Fail)                             |
| 98 | EIP Weblets Enable / Disable                       | UserName<br>Device name<br>Device serial number<br>Weblet Name<br>Completion Status (Enable / Disable)   |

|     |                                       |   |
|-----|---------------------------------------|---|
| 99  | Network Connectivity Enable / Disable | UserName<br>Device name<br>Device serial number<br>Completion Status<br>(Enable Wireless / Disable Wireless)<br>(Enable Wired /Disable Wired)   |
| 100 | Address Book Permissions              | UserName<br>Machine Name<br>Machine serial number<br>Completion Status<br>(SA Only/Open Access Enabled WebUI) /<br>(SA Only/Open Access Enabled LocalUI)  |
| 101 | Address Book Export                   | UserName<br>Machine Name<br>Machine serial number   |
| 102 | SW upgrade enable / disable           | UserName<br>Device name<br>Device serial number<br>Completion Status (Enable Installation / Disable Installation)   |
| 103 | Supplies Plan Activation              | Device name<br>Device serial number<br>Completion Status:<br>Success: (if Passcode is ok)<br>Failed: (if Passcode is not ok)<br>Locked out (if Max Attempts Exceed 5)<br>Time Remaining :<br>Hrs (Remaining for next attempt)<br>Min (Remaining for next attempt) |
| 104 | Plan Conversion                       | Device name<br>Device serial number<br>Completion Status:<br>Success: (if Passcode is ok)<br>Failed: (if Passcode is not ok)<br>Locked out (if Max Attempts Exceed 5)<br>Time Remaining :<br>Hrs (Remaining for next attempt)<br>Min (Remaining for next attempt) |
| 105 | IPv4<br>Enable/Disable/Configure      | UserName<br>Device name<br>Device serial number<br>Completion Status<br>(Enabled Wireless/Disabled Wireless/<br>Configured Wireless)<br>(Enabled Wired/Disabled Wired/<br>Configured Wired)   |
| 106 | SA PIN Reset                          | Device serial number<br>Completion Status (Success/Failed)  |
| 107 | Convenience Authentication Login      | UserName<br>Device name<br>Device serial number<br>Completion Status (Success or Failed)  |

|     |   |   |
|-----|---|---|
| 108 | Convenience Authentication Enable/Disable/Configure | UserName<br>Device name<br>Device serial number<br>Completion Status<br>(Enabled/Disabled/Configured)                                     |
| 109 | Efax Passcode Length                                | UserName (managing passcodes)<br>Device name<br>Device serial number<br>Completion Status (Passcode Length Changed)                       |
| 110 | Custom Authentication Login                         | UserName<br>Device name<br>Device serial number<br>Completion Status (Success or Failed)  |
| 111 | Custom Authentication Enable/Disable/Configure      | UserName<br>Device name<br>Device serial number<br>Completion Status<br>(Enabled/Disabled/Configured)                                     |
| 112 | Billing Impression Mode                             | UserName<br>Device name<br>Device serial number<br>Mode Set to (A4 Mode, A3 Mode<br>Completion Status (Success, Failed<br>Impression data |
| 113 | Airprint Enable/Disable/Configure                   | UserName<br>Device name<br>Device serial number<br>Completion Status<br>(Enabled/Disabled/Configured)                                     |
| 114 | Device cloning enable / disable                     | UserName<br>Device name<br>Device serial number<br>Completion Status<br>Enable / Disable  |
| 115 | Save for reprint job                                | UserName<br>Device name<br>Device serial number<br>Completion Status<br>(Standard Access, Open Access, Restricted)                        |
| 116 | Web UI Access/Configure                             | UserName<br>Device name<br>Device serial number<br>Completion Status<br>(Standard Access, Open Access, Restricted)                        |
| 117 | System log push to Xerox                            | Username if authenticated<br>Server destination URL<br>Log identifier string (filename)<br>Completion Status<br>(Success / Failed)        |

|     |   |  |
|-----|---|--|
| 119 | Scan to WebDAV<br>Job                   | Job name<br>User Name<br>Completion Status<br>IIO status<br>Accounting User ID-Name<br>Accounting Account ID-Name<br>WebDAV destination.                                       |
| 120 | Mopria Print<br>enable / disable        | UserName<br>Device name<br>Device serial number<br>Completion Status<br>Enable / Disable   |
| 121 | PoS credit card API enable /<br>disable | UserName<br>Device name<br>Device serial number<br>Completion Status<br>Enable / Disable   |
| 122 | PoS CC data transfer<br>data transfer   | Job name or number<br>Machine Name<br>Machine serial number<br>Destination server<br>Completion status (Success / Fail)  |
| 124 | Invalid Login Attempt<br>Lockout        | Device name<br>Device serial number<br>Interface (Web UI, Local UI)<br>Session IP Address if available   |
| 125 | Protocol audit Log enable/Disable       | UserName<br>Device Name<br>Device serial number<br>Completion Status<br>Enable / Disable   |
| 126 | Display Device information<br>configure | UserName<br>Device Name<br>Device serial number<br>Completion Status<br>(Configured)   |
| 127 | Invalid Login Lockout<br>Expires        | Device name<br>Device serial number<br>Interface (Web UI)<br>Session IP Address if available<br>Count of invalid attempts: "attempts xx" where xx =<br>the number of attempts. |
| 128 | Erase Customer Data                     | Erase Customer Data<br>Device serial number<br>Success / Failed  |
| 129 | Audit log SFTP scheduled<br>Configure   | UserName<br>Device Name<br>Device serial number<br>Completion status (Enable/Disable/Configured)   |

|     |  |   |
|-----|--|---|
| 130 | Audit Log SFTP Transfer                                | UserName<br>Device Name<br>Device serial number<br>Destination server<br>Completion Status<br>(File Transmitted)  |
| 131 | Remote Software<br>Download<br>Enable Disable          | UserName<br>Device name<br>Device serial number<br>Completion Status (Enable/Disable)   |
| 132 | Airprint & Mopria Scanning<br>Enable/Disable/Configure | UserName<br>Device Name<br>Device serial number<br>Completion Status<br>(Enable/Disable/Configured)   |
| 133 | Airprint & Mopria Scan Job<br>Submitted                | Job name (if accepted)<br>UserName (if available)<br>IP address of submitting client<br>Device name<br>Device serial number<br>Completion status<br>(accept/reject request) |
| 134 | Airprint & Mopria Scan Job<br>Completed                | Job name<br>UserName (if available)<br>Completion status  |
| 136 | Remote Services NVM Write                              | Device Name<br>Device Serial<br>Completion Status (Success-Fail)  |
| 137 | Remote Services FIK Install                            | Device Name<br>Device Serial<br>Completion Status (Success-Fail)<br>User-readable names for the features being installed  |
| 138 | Remote Services Data Push                              | Device Name<br>Device Serial<br>Completion Status (Success-Fail)  |
| 139 | Remote Services  | User Name,<br>Device Name,<br>Device Serial<br>Status: ("Enabled" / "Disabled")   |
| 140 | Restore enable/disable                                 | User Name<br>Device name<br>Device serial number<br>Completion status<br>Enable / Disable   |
| 141 | Backup-Restore<br>file downloaded                      | File Name<br>User Name<br>Interface (WebUI)<br>IP Address of the destination (if applicable)<br>Completion Status (Success or Failed)                                       |

|     |   |   |
|-----|---|---|
| 142 | Backup-Restore<br>restore installed           | File Name<br>User name<br>Device name<br>Device IP address<br>Interface (WebUI)<br>Completion Status (Success or Failed)                  |
| 143 | Google Cloud Services                         | User name<br>Device name<br>Device serial number<br>Completion Status-(Enabled / Disabled / Configured)                                   |
| 144 | User or Group Role<br>Assignment              | User name<br>Device name<br>Device serial number<br>User or group name (assigned)<br>Role name<br>Action (added/removed)                  |
| 145 | User Permission Role                          | User name<br>Device name<br>Device serial number<br>Role name<br>Completion status (Created / Deleted / Configured)                       |
| 146 | Admin Password Policy Configure               | User name<br>Device name<br>Device serial number  |
| 147 | Local user account password<br>policy         | User name<br>Device name<br>Device serial number  |
| 148 | Restricted admin login                        | User name<br>Device name<br>Device serial number<br>Completion status: "Success" or "Failed"  |
| 149 | Grant / revoke restricted admin<br>rights     | User name (of user making the change)<br>Device name<br>Device serial number<br>User name (of target user)<br>Action: "Grant" or "Revoke" |
| 150 | Manual session logout                         | Device Name<br>Device Serial Number<br>Interface (Web, LUI, CAC)<br>User Name (who was logged out)<br>Session IP (if available)           |
| 151 | IPP Enable/Disable/Configure                  | User name<br>Device name<br>Device serial number<br>Completion status: ("Enabled" / "Disabled" /<br>"Configured")                         |
| 152 | HTTP Proxy Server<br>Enable/Disable/Configure | User name<br>Device name<br>Device serial number<br>Completion status: ("Enabled" / "Disabled" /<br>"Configured")                         |

|     |   |  |
|-----|---|--|
| 153 | Remote Services Software Download         | Device Name<br>Device Serial number<br>File Name   |
| 154 | Restricted Admin Permission Role          | User name<br>Device name<br>Device serial number<br>Restricted admin role name<br>Completion status (Created / Deleted / Configured)                                     |
| 155 | EIP Weblet Installation Security Policy   | User name<br>Device name<br>Device serial number<br>Policy: ("allow installation of encrypted Weblets" / "allow installation of both encrypted and unencrypted Weblets") |
| 159 | Send Engineering Logs on Data Push        | User name (if available)<br>Device name<br>Device serial number<br>Current setting ("Enabled" / "Disabled")  |
| 160 | Allow the Print Submission of Clone Files | UserName (if available)<br>Device name<br>Device serial number<br>Completion status: ("Enabled" / "Disabled")  |
| 161 | Network Troubleshooting Start, Stop       | User name<br>Device Name<br>Device Serial Number<br>Completion Status ("Started", "Stopped")   |
| 162 | Network Troubleshooting Data Download     | User name<br>File name (of downloaded file)<br>Device Name<br>Device Serial Number<br>Destination (IP address)<br>Completion Status ("Success" / "Failed")               |
| 163 | dns-sd text file download                 | User name<br>File name (of downloaded file)<br>Device Name<br>Device Serial Number<br>Destination (IP address)<br>Completion Status ("Success" / "Failed")               |
| 164 | One-Touch App Management                  | User Name<br>Device name<br>Device serial number<br>Onetouch application Display Name<br>Action ("Install" / "Un-install")<br>Completion: ("Success" / "Failed")         |
| 165 | SMB Browse                                | User name<br>Device name<br>Device serial number<br>Completion status: ("Enabled" / "Disabled" / "Configured")   |
| 166 | Job Data Removal Standard started         | Device name<br>Device serial number  |



|     |  |   |
|-----|--|---|
| 167 | Job Data Removal Standard complete                     | Device name<br>Device serial number<br>Completion Status (“Success” / “Failed”)   |
| 168 | Job Data Removal Full started                          | Device name<br>Device serial number   |
| 169 | Job Data Removal Full complete                         | Device name<br>Device serial number<br>Completion Status (“Success” / “Failed”)   |
| 170 | Scheduled Job Data Removal Configure                   | User Name<br>Device name<br>Device serial number<br>Status (“Enable”/”Disable”/”Configured”)  |
| 171 | Cross-Origin-Resource-Sharing (CORS)                   | User Name<br>Device name<br>Device serial number<br>Status (“Enable”/”Disable”)   |
| 172 | One-Touch App Export                                   | User name<br>Device name<br>Device serial number<br>Completion Status: (“Success”   “Failed”)   |
| 173 | Device File Distribution Trust Operations              | User name<br>Device name<br>Device serial number<br>Member name<br>Member serial number<br>TC Lead Device Name<br>TC Lead Serial Number<br>Trust operation: (“Grant”   “Revoke”)<br>Completion status: (“Success”   “Failed”) |
| 174 | Device File Distribution Feature                       | User name<br>Device name<br>Device serial number<br>Trust operation: (“Enable”   ”Disable”   “Configure”)<br>Completion status: (“Success”   “Failed”)  |
| 175 | Device File Distribution - Store File for Distribution | User name<br>Device name<br>Device serial number<br>File type: (“SWUP”   “Clone”   “Add-On”)<br>File name   |
| 176 | Xerox Configuration Watchdog                           | User name<br>Device Name<br>Device Serial number<br>Completion status: (“Enabled”   “Disabled”)   |
| 177 | Xerox Configuration Watchdog Check Complete            | User name (if available. “SYSTEM”, if executed as a scheduled event)<br>Device name<br>Device serial number<br>Completion status (“Success”   “Failed”)   |

|     |   |   |
|-----|---|---|
| 178 | Xerox Configuration Watchdog Remediation Complete | User name (if available. "SYSTEM", if executed as a scheduled event)<br>Device name<br>Device serial number<br>Completion status ("Success"   "Failed") |
| 179 | ThinPrint Feature                                 | User Name<br>Device name<br>Device serial number<br>Completion Status: ("Enabled"   "Disabled"   "Configured")  |
| 180 | Beaconing for "iBeacon for AirPrint Discovery"    | User Name<br>Device name<br>Device serial number<br>Completion Status: ("Enabled"   "Disabled")   |
| 181 | Network Troubleshooting Install, Uninstall        | User Name<br>Device name<br>Device serial number<br>Completion Status: ("Installed"   "Uninstalled")  |
| 182 | POP3 Connection Encryption (TLS)                  | User Name<br>Device name<br>Device serial number<br>Completion Status: ("Enabled"   "Disabled"   "Configured")  |
| 183 | FTP Browse  | User Name<br>Device name<br>Device serial number<br>Completion Status: ("Enabled"   "Disabled"   "Configured")  |
| 184 | SFTP Browse                                       | User Name<br>Device name<br>Device serial number<br>Completion Status: ("Enabled"   "Disabled"   "Configured")  |

## 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")<br>Scheduled<br>On Demand  |
| 101 | Image Overwriting finished                 | Completion: ("Success" / "Failed")  |
| 101 | Self-Test                                  | Completion: ("Success" / "Failed")<br>Checksum of ROM image 1<br>Checksum of ROM image 2  |
| 201 | Login                                      | User name<br>Completion: ("Success" / "Failed Invalid User ID" /<br>"Failed Invalid Password" / "Failed")<br>Host Name or IP Address<br>Method: ("Local" / "Remote" / "Convenience" ,<br>"Custom")<br>Role: ("System Administrator" / "Customer Engineer" /<br>"Casual Operator") |
| 201 | Logout                                     | User name<br>Completion: ("Success" / "Failed")   |
| 201 | Locked System Administrator Authentication | Count of Remaining Authentication Failures  |
| 201 | Detected Continuous Authentication Fail    | User name<br>Protocol: ("SNMPv3" / "EWS")<br>Count of Remaining Authentication Failures   |
| 301 | Audit Log                                  | User name<br>Completion: ("Enabled" / "Disabled")   |
| 401 | Print                                      | User name<br>Completion: ("Completed" / "Completed with Warnings"<br>/ "Cancelled by User" / "Cancelled by Shutdown" /<br>"Aborted" / "Unknown")<br>Root Job UUID<br>Relation: ("Related" / "Owned")<br>Job Accounting ID<br>Action Details<br>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<br>User Role   |
| 501 | Edit User                  | User name<br>User Role<br>ID<br>Password<br>CardID<br>Name<br>Permission<br>Role<br>ICCardID<br>Other  |
| 501 | Delete User                | User Name  |
| 501 | Create Mailbox             | Host Name or IP Address<br>Box Number  |
| 501 | Delete Mailbox             |  |
| 501 | Switch Authentication Mode | Completion: ("Success")<br>New Setting<br>Previous Setting   |
| 501 | Change Security Setting    | Authentication<br>Accounting<br>Image Overwrite<br>HDD Encryption<br>SSL<br>S/MIME<br>IPSEC<br>SNMPv3<br>802.1x<br>Certificate Verify Mode<br>Maintainer Password<br>SmartCard<br>FIPS140<br>Self Test |

|     |                                |  |
|-----|--------------------------------|--|
|     |                                | Auto Clear Timer<br>Service Rep. Restricted Operation<br>Print Reports Button<br>External Code Integrity Check<br>Authorization<br>NFC   |
| 501 | View Security Setting          | Access Method: ("Local" / "EWS" )<br>Host Name or IP Address   |
| 501 | Change Contract Type           | User name<br>Completion: ("Success" / "Failed" / "Aborted")  |
| 501 | Change Geographic Region       |  |
| 501 | Enter Activation Code          | Completion: ("Success")  |
| 501 | Change Job Setting             | Completion: ("Success")<br>Function Name: ("Delay Print" / "Private Print")  |
| 601 | Change Billing Impression Mode | Completion: ("Success" / "Failed")<br>Designated Mode ("A3 Mode" / "A4 Mode")<br>Billing Meter Values                                    |
| 601 | Import Certificate             | User name<br>Completion: ("Success" / "Failed")<br>Category: ("RootCA" / "DeviceEE" / "SSCEE")<br>Key Size<br>Issuer DN<br>Serial Number |
| 601 | Delete Certificate             |  |
| 601 | Add Address Entry              | Host Name or IP Address<br>Registration Number   |
| 601 | Delete Address Entry           |  |
| 601 | Edit Address Entry             |  |
| 601 | Import Address Book            | Host Name or IP Address  |
| 601 | Export Address Book            |  |
| 601 | Clear Address Book             | Host Name or IP Address  |
| 601 | Export Audit Log               |  |
| 601 | Install Custom Service         | Completion: ( "Failed")<br>Host Name or IP Address<br>Custom Service Name  |
| 601 | Install Embedded Plug-in       | Host Name or IP Address<br>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")<br>ROM Type: ("IOT" / "UI" / "Controller" / "FAX")<br>New Version<br>Previous Version |
| 701 | Trusted Communication | Completion: ("Failed")<br>Protocol Name: ("SSL/TLS" / "IPSEC" / "S/MIME")                                     |

## Free Manuals Download Website

<http://myh66.com>

<http://usermanuals.us>

<http://www.somanuals.com>

<http://www.4manuals.cc>

<http://www.manual-lib.com>

<http://www.404manual.com>

<http://www.luxmanual.com>

<http://aubethermostatmanual.com>

Golf course search by state

<http://golfingnear.com>

Email search by domain

<http://emailbydomain.com>

Auto manuals search

<http://auto.somanuals.com>

TV manuals search

<http://tv.somanuals.com>