# Security Guide

Xerox® AltaLink® B8145/B8155/B8170 Multifunction Printer

Xerox® AltaLink® C8130/C8135/C8145/C8155/C8170 Color Multifunction Printer

Document Version: 3.5 (May 2023).

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

# Revision History

| Version | Date | Details |
|---|---|---|
| **1.0** | **Dec 2019** | **Initial Atl2.0/SW v105.ppp.xxx.xxxx & Atl2.1/SW v1111.ppp.xxx.xxxx version** |
| **2.2** | **March 2021** | **Alt2.2/SW v113.ppp.xxx.xxxx updates:**<br>• Updated Immediate Job and Disk Overwrite sections to reflect the ability for user to configure the number of overwrites, see section 3.<br>• Removed “EAP MD5” support from Authentication Methods list, see 802.1x section 4.<br>• Updated and clarified FIPS140-2 Compliance Validation, see section 4.<br>• Added time expiry to Device Certificates, see section 4.<br>• Added support for TL1.3 and updated document as applicable. Refer to Outbound User Data and Outbound Ports in section 3 and TLS in section 4.<br>• Updated and clarified Firmware Integrity, see section 5.<br>• Updated Appendix B: Security Events to remove un-supported events and add new events. |
| **2.5** | **August 2021** | **Atl2.5/v114.ppp.xxx.xxxxx updates:**<br>• Updated Minimum Key Length and Trusted Certificates table, see section 4.<br>• Updated Service Technician (CSE) Access Restriction to indicate the ability to restrict CSE account access, see section 5.<br>• Added new content to Configuration and Security Policy Management Solutions, see section 6: Fleet Orchestrator, Universal Print and Imaging Security.<br>• Added two new options to Authentication, see section 7: Identity Provider (IdP) and Xerox Workplace Cloud.<br>• Updated Appendix B: Security Events to remove un-supported events and add new events. |
| **3.0** | **August 2022** | **Alt3.0/v118.ppp.xxx.xxxx updates:**<br>• Updated FIPS Compliance Validation section 4<br>• Added Security Dashboard, see section 6<br>• Updated Appendix B: Security Events to remove un-supported events<br>• Changed McAfee to Trellix (branding change only) |
| **3.5** | **May 2023** | **Alt3.5/v119.ppp.xxx.xxxx updates:**<br>• **Added OCSP support, see section 4-8**<br>• **Updated TLS, see section 4-4**<br>• Updated Appendix B: Security Events to remove un-supported events and add new events<br>• Included third-party trademark attribution statements |

# Contents

# 1. Introduction

## Purpose

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

## Target Audience

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

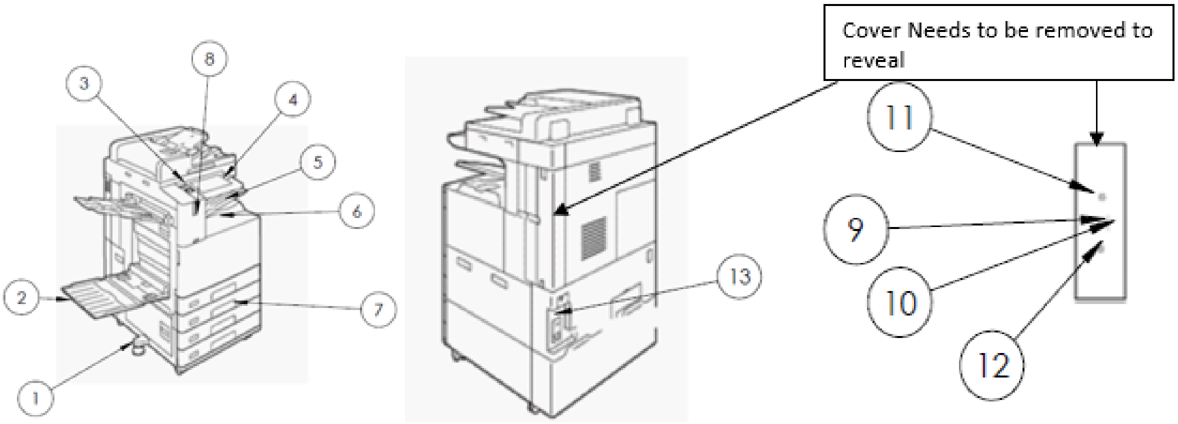
## Disclaimer

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

# 2. Product Description

## PHYSICAL COMPONENTS

Xerox® AltaLink® B8145/B8155/B8170 (Mono MFP) and C8130/C8135/C8145/C8155/C8170 (Color MFP) are very similar and 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 in configuration, however, configurations are not relevant to security and are not discussed.

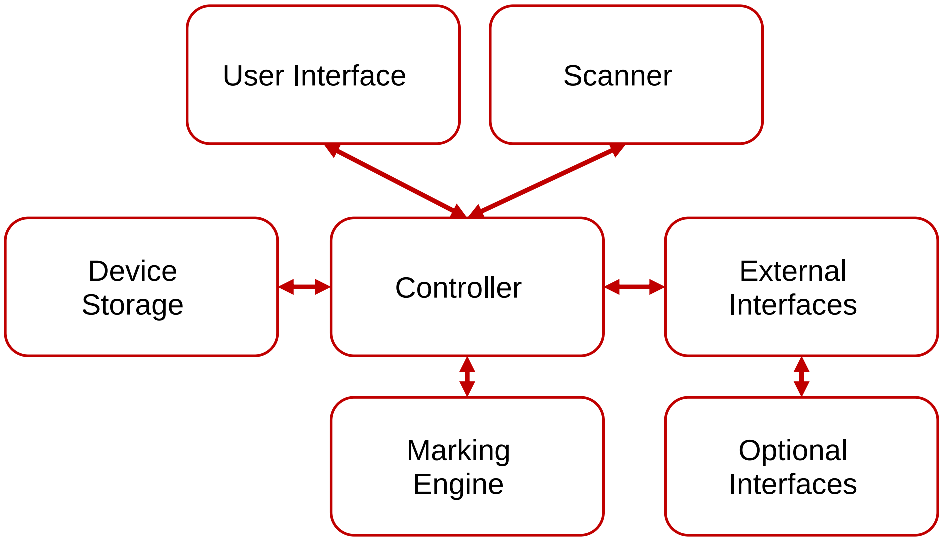


1. Stabilizer
2. Bypass paper feed tray
3. Front USB Port(s)*
4. Touch screen user interface
5. Upper paper tray
6. Lower paper tray
7. Paper feed trays
8. Smart Proximity Sensor
9. Rear USB Port(s)*
10. Optional Wi-Fi Dongle Dongle Port*/Optional Bluetooth microadapter port
11. RJ45 Ethernet connection*
12. Service port
13. AC Power

*Denotes a security related component

## ARCHITECTURE

AltaLink® products share a common architecture which is depicted below. The following sections describe components in detail.



## USER INTERFACE

The user interface detects soft and hard button actuations and provides text and graphical prompts to the user. The user interface is sometimes referred to as the Graphical User Interface (GUI) or Local User Interface (LUI) in order to distinguish it from the remote web server interface, also known as Embedded Web Server (EWS) or WebUI.

The user interface allows users to access product services and functions. Users with administrative privileges can manage the product configuration settings. User permissions are configurable through Role-Based Access Control (RBAC) policies, described in Section 7 Identification, Authentication, and Authorization.

## SCANNER

The scanner converts documents from hardcopy to electronic data. The 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. Standard models are equipped with a Solid-State Drive (SSD). An optional magnetic Hard Disk Drive (HDD) is also available. For model-specific details please see Appendix A: Product Security Profiles.

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

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

## Controller External Interfaces

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

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

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

  Note: Features that use the USB ports (such as Scan To USB) can be disabled independently.
- Connection of optional equipment such as Bluetooth or CAC readers.
- Firmware updates may be submitted through the 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 TIA-568 NETWORK CONNECTOR

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

### REAR USB (TYPE B) TARGET PORT

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

- USB target connector used for printing

  **Note:** This port is used for service Diagnostics and cannot be disabled by a system administrator.

# Optional Equipment

### RJ-11 ANALOG FAX AND TELEPHONE

The embedded Fax service uses the installed embedded fax card to send and receive images over the telephone interface. The Fax card plugs into a custom interface slot on the controller. The Fax telephone lines are connected directly to the Fax card via RJ-11 connectors, and it uses T.30 Fax Modem protocol and will not accept data or voice communication. All remaining Fax-specific features are implemented in software on the controller.

### WIRELESS NETWORK CONNECTOR

AltaLink® products accept an optional wireless kit that can be installed in the rear USB port.

### BLUETOOTH® MICROADAPTER

AltaLink® products accept an optional Bluetooth MicroAdapter that can be installed in the rear USB port to support iBeacon for AirPrint Discovery.

When enabled and configured, iBeacon enables the Xerox® AltaLink® product to advertise basic printer discovery information, including a routable IP address, via the Bluetooth Low Energy Beacon. There is no user data transfer over Bluetooth. iBeacon functionality can be disabled using the embedded web server of the product.

### NEAR FIELD COMMUNICATIONS (NFC) READER

AltaLink® products come standard with an NFC Chip built into the front panel. This is only read from an NFC client. The data exchanged is not encrypted and may include information including system network status, IP address and product location. NFC functionality can be disabled using the embedded web server of the product. NFC functionality requires a software plugin that can be obtained from Xerox sales and support.

Information shared over NFC includes: IPv4 Address, IPv6 Address, MAC Address, UUID (a unique identifier on the NFC client), and Fully Qualified Domain Name

### SMART CARD – CAC/PIV

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

### 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 local print, scan, fax, or copy jobs or mobile and cloud applications, etc. Xerox products protect user data being processed by employing strong encryption. The standard configuration is sold with SSD.

## User Data Protection While Within Product

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

### ENCRYPTION

All user data being processed or stored to the product is encrypted by default. Encryption cannot be disabled on this family of products.

### PRIVATE KEY MANAGEMENT

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

### JOB DATA REMOVAL AVAILABLE ON STANDARD SSD CONFIGURATION

The Job Data Removal feature is provided to allow security conscious customers the facility to remove all residual image data from the Network Controller, the image system and, if installed, the Embedded Classic Fax card memory. Job Data Removal is being introduced to provide customers with SSD devices the ability to clean up the disk by purging job data (no overwrite) using the same interface as Image and Disk Overwrite available with HDD configuration.

### MEDIA SANITIZATION (IMAGE AND DISK OVERWRITE) AVAILABLE WITH OPTIONAL HDD CONFIGURATION

AltaLink® products equipped with magnetic hard disk drives are compliant with NIST Special Publication 800-88 Rev1: *Guidelines for Media Sanitization*. User data is securely erased using the algorithm as described in the following link:
https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-88r1.pdf

### IMMEDIATE JOB OVERWRITE AVAILABLE WITH OPTIONAL HDD CONFIGURATION

When enabled, Immediate Job Overwrite (IJO) will overwrite any temporary files that were created on the magnetic hard disk that may contain user data. The feature provides continuous automatic overwrite of sensitive data with minimal impact to performance, robust error reporting, and logging via the Audit Log. When enabled, Immediate Job Overwrite (IJO) will overwrite and remove any remnants and temporary files of all print, copy, scan, and fax jobs from the image disk as soon as the job finishes processing. The feature provides continuous automatic overwrite of sensitive data with minimal impact to performance, robust error reporting, and logging via the Audit Log. Supported only in Atl2.2/SW 113.XXX.XXX.XXXX and newer releases, the system administrator can set the number of overwrites from 1 to 3 and each overwrite pass uses different patterns.

### DISK OVERWRITE (SCHEDULED AND ON-DEMAND) AVAILABLE WITH OPTIONAL HDD CONFIGURATION

Complementing the Immediate Job Overwrite is Disk Overwrite (Scheduled and On-Demand). While IJO overwrites individual files, Disk Overwrite wipes entire partitions. The Disk Overwrite feature can be invoked at any time and optionally may be scheduled to run automatically. Supported only in Atl2.2/SW 113.XXX.XXX.XXXX and newer releases, the system administrator can set the number of overwrites from 1 to 7 and each overwrite pass uses different patterns.

## 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 for any print jobs to enabled products. Simply configure Document Encryption to On in the Advanced tab of the print driver at print time. |

### 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 Printer** |
|---|---|---|
| | | **B8145, B8155, B8170, C8130, C8135, C8145, C8155, C8170** |
| **Email S/MIME** | | |
| | Versions | v3 |
| | Digest | SHA1, SHA256, SHA384, SHA512 |
| | Encryption | AES128, AES192, AES256 |

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

AltaLink® multifunction products support scanning of hardcopy documents to external network locations including file repositories and email and facsimile services. In addition to supporting network level encryption including IPsec, Xerox products support the following.

| Protocol | Encryption | Description |
|---|---|---|
| HTTP | N/A | Unencrypted HTTP protocol |
| HTTPS (TLS) | TLS | HTTP encrypted by TLS |
| FTP | N/A | Unencrypted FTP |
| SFTP (SSH) | SSH | FTP encrypted by SSH |
| SMBv3 | Yes | Encryption may be enabled on a Windows share |
| SMBv2 | N/A | Unencrypted SMB |
| SMBv1 | N/A | (Not used as a transport protocol. Used for network discovery only) |
| SMTP (email) | S/MIME | The product uses SMTP to transmit data to the email server. Email authentication, encryption, and signing are supported. Please refer to the Network Security section of this document for details. |

### SCANNING TO USER LOCAL USB STORAGE PRODUCT (OUTBOUND USER DATA)

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

| | | **AltaLink® Multifunction Printer** |
|---|---|---|
| | | **B8145, B8155, B8170**<br>**C8130, C8135, C8145, C8155, C8170** |
| **Local Data Encryption** | | AES-256 |
| Federal Information Protection Standard 140-2 | | Yes |
| Media Sanitization NIST 800-171 (Image Overwrite) | | Models with magnetic HDD. See Appendix A: Product Security Profiles |
| **Print Submission** | | |
| | IPPS (TLS) | Supported |
| | HTTPS (TLS) | Supported |
| | Xerox Print Stream Encryption | Supported |
| **Scan to Repository Server** | | |
| | HTTPS (TLS) | 1.0, 1.1, 1.2, 1.3[1] |
| | SFTP (SSH) | SSH-2 |

[1] Supported only in Atl2.2/SW 113.XXX.XXX.XXXX and newer releases

| | | |
|---|---|---|
| | SMB (unencrypted) | v1, v2, v3 |
| | SMB (with share encryption enabled) | v3 |
| | HTTP (unencrypted) | Supported |
| | FTP (unencrypted) | Supported |
| **Scan to Fax Server** | | |
| | HTTPS (TLS) | 1.0, 1.1, 1.2, 1.3[2] |
| | SFTP (SSH) | SSH-2 |
| | SMB (unencrypted) | v1, v2, v3 |
| | SMB (with share encryption enabled) | v3 (Dialect 3.00, 3.02, 3.1.1) |
| | S/MIME | Supported |
| | HTTP (unencrypted) | Supported |
| | FTP (unencrypted) | Supported |
| | SMTP (unencrypted) | Supported |
| **Scan to Email** | | |
| | S/MIME | Supported |
| | SMTP (unencrypted) | Supported |
| | TLS (StartTLS) | Supported |

### ADD ON APPS – CLOUD, GOOGLE, DROPBOX, AND OTHERS (OUTBOUND USER DATA)

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

[2] Supported only in Atl2.2/SW 113.XXX.XXX.XXXX and newer releases

# 4. Network Security

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

## TCP/IP Ports and Services

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

| Inbound (Listening Services) | Outbound (Network Client) |
|---|---|
| **Print Services**<br>LPR, IPPs (TLS), Raw IP, etc. | **Built-in Scan Services**<br>FTP, HTTP & HTTPS (TLS), SMB, SMTP & SMTPS, POP3, etc. |
| **Management Services**<br>SNMP, Web interface, Web Services, etc. | **Authentication Services**<br>LDAP & LDAPS, SMB, Kerberos and Azure. |
| **Infrastructure and Discovery Services**<br>IPsec, WSD, mDNS, Bonjour, etc. | **Infrastructure**<br>IPsec, DHCP and DHCPv6, etc. |
| | **Cloud Services**<br>Dropbox, Google Drive, OneDrive, and several others |

### LISTENING SERVICES (INBOUND PORTS)

The following table summarizes all potentially open ports on the product. These ports can be enabled/disabled within the product configuration. Some ports can be configured to a different value for some features/protocols.

| Port | Type | Service Name |
|---|---|---|
| 80 or 443 | TCP | HTTP including:<br>Web User Interface<br>Web Services for Products (WSD)<br>WebDAV |
| 68 | UDP | DHC ACK Response to DHCP |
| 88 | UDP | Kerberos |
| 110 | TCP | POP3 |
| 139 | TCP | NETBIOS |
| 161 | TCP | SNMP |
| 162 | TCP | SNMP Trap |
| 137 | UDP | NETBIOS (Name Service) |
| 138 | UDP | NETBIOS (Datagram Service) |
| 161 | UDP | SNMP |
| 427 | TCP/UDP | SLP |
| 443 | TCP | HTTPS – HTTP over TLS, IPPS |
| 445 | TCP | SMB |
| 500 & 4500 | TCP/UDP | IPsec |
| 515 | TCP | LPR |
| 631 | TCP | IPP |
| 3702 | TCP/UDP | WSD (Discovery) |
| 4000 | TCP | ThinPrint |
| 5353 | TCP/UDP | mDNS |
| 5354 | TCP | mDNS Responder IPC |
| 9100 | TCP | Raw IP (also known as JetDirect, AppSocket or PDL-datastream) |
| 5909-5999 | TCP | Remote Access to local display panel. Port is randomly selected, and communications encrypted with TLS 1.2 or 1.3 |
| 51333 | TCP | File Sharing through Fleet Orchestrator |
| 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® products support IPsec for both IPv4 and IPv6 protocols.

| | | **AltaLink® Multifunction Printer** |
|---|---|---|
| | | **B8145, B8155, B8170,**<br>**C8130, C8135, C8145, C8155, C8170** |
| **IPsec** | | |
| | Supported IP Versions | IPv4, IPv6 |
| | Key exchange authentication method | Preshared Key & digital signature authentication (device authentication certificate, server validation certificate) |
| | Transport Mode | Transport & Tunnel mode |
| | Security Protocol | ESP & AH |
| | ESP Encryption Method | AES, Null |
| | ESP Authentication Methods | SHA1, SHA256, None |

### WIRELESS 802.11 WI-FI PROTECTED ACCESS (WPA)

Products equipped with Wi-Fi support WPA3 Personal, WPA3 Personal Transitional, WPA3 Enterprise, WPA3 Enterprise 192-bit mode, WPA2 Personal, WPA2 Enterprise, and Mixed Mode. The wireless network adapters used in Xerox products are certified by the Wi-Fi Alliance.

| | | **AltaLink® Multifunction Printer** |
|---|---|---|
| | | **B8145, B8155, B8170,**<br>**C8130, C8135, C8145, C8155, C8170** |
| **Wi-Fi (802.11)** | | |
| | No Encryption | Supported |
| | WEP | RC4 |
| | WPA2 Personal (PSK) | CCMP (AES), TKIP, TKIP+CCMP (AES),<br>PMF (Protected Management Frame) support optional<br>Password-based authentication via Pre-Shared Key (PSK) |
| | WPA2 Enterprise | CCMP (AES), TKIP, TKIP+CCMP (AES)<br>PEAPv0 MS-CHAPv2<br>EAP-TLS |

| | | |
|---|---|---|
| | | EAP-TTLS/PAP<br>EAP-TTLS/MS-CHAPv2<br>EAP-TTLS/EAP-TLS<br>PMF (Protected Management Frame) support optional |
| | WPA3 Personal (SAE) | CCMP (AES)<br>PMF (Protected Management Frame) support required<br>Password-based authentication via Simultaneous Authentication of Equals (SAE) |
| | WPA3 Personal Transitional | WPA3 / WPA2 Personal<br>CCMP (AES)<br>PMF (Protected Management Frame) support optional<br>Password-based authentication: WPA3-SAE/ WPA2-PSK |
| | WPA3 Enterprise | CCMP (AES)<br>PEAPv0 MS-CHAPv2<br>EAP-TLS<br>EAP-TTLS/PAP<br>EAP-TTLS/MS-CHAPv2<br>EAP-TTLS/EAP-TLS<br>Server certificate validation required<br>PMF (Protected Management Frame) support required |
| | WPA3 Enterprise- 192 bit | AES-GCMP-256<br>EAP-TLS<br>EAP-TTLS/EAP-TLS<br>Server certificate validation required<br>PMF (Protected Management Frame) support required |
| | BSSID Roaming Restriction | Supported |

### TLS

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

| | **AltaLink® Multifunction Printer** |
|---|---|
| | **B8145, B8155, B8170,**<br>**C8130, C8135, C8145, C8155, C8170** |
| **TLS** | |

| | | |
|---|---|---|
| | TLS Versions | TLS 1.2 (recommended)<br>TLS 1.1 and TLS 1.2 (default), or<br>TLS 1.0, TLS 1.1 and TLS 1.2<br>Note: In FIPS CCC mode TLS 1.0 or 1.1 are not supported. |
| | | Include or not include TLS 1.3 setting<br>Note: Do not include TLS 1.3 if some features require servers that do not support TLS 1.3 |
| | TLS Hash Algorithms | SHA-256 and above (recommended)<br>SHA-1, SHA-256 and above (default)<br>Note: The setting does not apply to Scan to Cloud and Print from Cloud features other than for authentication. |

### SNMPV3

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

Message integrity to ensure that a packet has not been tampered with in transit

Authentication to verify that the message is from a valid source

Encryption of packets to prevent unauthorized access

| | | **AltaLink® Multifunction Printer** |
|---|---|---|
| | | **B8145, B8155, B8170, C8130, C8135, C8145, C8155, C8170** |
| **SNMPv3** | | |
| | Digest | SHA1, MD5 |
| | Encryption | DES, AES128 |

## Public Key Infrastructure (PKI)

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

### DEVICE CERTIFICATES

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

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

The Xerox device certificate, which is the default device certificate installed on the MFP, is issued by the Xerox Root CA embedded in the MFP firmware. The Xerox device certificate details are configurable and can be recreated as needed by the device administrator. The default expiry date is such that the expiry is at 397 days to meet current CA/browser standards, however the default can be overridden in configuration.

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

| | | **AltaLink® Multifunction Printer** |
|---|---|---|
| | | **B8145, B8155, B8170,**<br>**C8130, C8135, C8145, C8155, C8170** |
| **Device Certificates** | | |
| | Certificate Length | Up to 4096 (for RSA certificates) |
| | Default Device Certificate | ECDSA P-384 |
| | Supported Hashes | SHA256 |
| | Product Web Server | Supported |
| | IPPS Printing | Supported |
| | 802.1X Client | Supported |
| | IPsec | Supported |
| | SFTP | Supported |

## TRUSTED CERTIFICATES

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

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

| | | **AltaLink® Multifunction Printer** |
|---|---|---|
| | | **B8145, B8155, B8170,**<br>**C8130, C8135, C8145, C8155, C8170** |
| **Trusted Certificates (CA & Peer device)** | | |
| | Minimum RSA Key Length Restriction Options | None, 1024, 2048, 4096 |
| | Minimum ECDSA Key Length Restriction Options | 256, 384 |
| | Maximum Length | 4096 |
| | Supported Hashes | SHA1/224/256/384/512 |
| | IPsec | Supported |
| | LDAP | Supported |
| | Scanning (HTTPS/TLS) | Supported |
| | Scanning (SFTP/SSH) | Used for audit log transfer |
| | 802.1X Client | Supported |
| | Email Signing | Supported |
| | Email Encryption | Supported |
| | Email (STARTLS) | Supported |
| | OCSP Validation | Supported |

## MINIMUM KEY LENGTH

An administrator can independently specify the minimum encryption key length for RSA and ECDSA certificates used for encryption by the device. When a user imports a certificate to the device, that certificate’s key length is validated against the minimum requirements. Certificates with key lengths that are less than the minimum key-length requirements are not installed, and a message alerts the user to the discrepancy. Additionally, a user is not able to change the device minimum key-length setting, if doing so would invalidate a certificate already installed on the device.

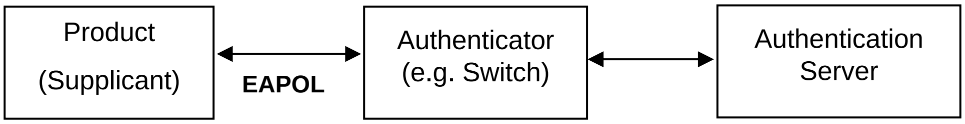
### ONLINE CERTIFICATE STATUS PROTOCOL (OCSP)

OCSP is supported to validate server certificates and related signing chains. OCSP validation is implemented for smart card authentication, and also when the product is enabled for FIPS with CC Mode, for CC related features.

## 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 Printer** |
|---|---|---|
| | | **B8145, B8155, B8170,**<br>**C8130, C8135, C8145, C8155, C8170** |
| **Network Access Control** | | |
| | 802.1x | Supported |
| | Authentication Methods | PEAPv0/EAP MSCHAPv2, EAP-MSCHAPv2, EAP-TLS |

### CISCO IDENTITY SERVICES ENGINE (ISE)

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

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

Once classified, endpoints can be authorized to the network and granted access based on their profile signature. For example, guests to your network will have different levels of access to printers and other endpoints 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 Printer** |
|---|---|---|
| | | **B8145, B8155, B8170,**<br>**C8130, C8135, C8145, C8155, C8170** |
| **Network Access Control** | | |
| | Cisco ISE | Supported |

### CONTEXTUAL ENDPOINT CONNECTION MANAGEMENT

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

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

### FIPS140-3 COMPLIANCE VALIDATION

When enabled for FIPS 140-3, cryptographic functions are FIPS 140-3 compliant and performed from within a FIPS validated module, except those acknowledged as exceptions during FIPS 140-3 enablement.  When also enabled with CC compliance, some cryptographic functions are further restricted to the requirements of Common Criteria.

.

## Additional Network Security Controls

### IP FILTERING

The devices contain a static host-based firewall that provides the ability to prevent unauthorized network access based on IP address and/or port number. Filtering rules can be set by the SA using the Embedded Web Server. An authorized SA can create rules to (Accept/Reject/Drop) for ALL or a range of IP addresses. In addition to specifying IP addresses to filter, an authorized SA can enable/disable all traffic over a specified transport layer port.

### PERSONAL IDENTIFIABLE INFORMATION (PII)

Personal Identifiable Information (PII) can be entered or stored into the device through several means: address book, scan templates, device description, display device information, audit logs, and engineering logs. The PII is encrypted on the device and it is not readable outside of the operation of the device. The Admin controls the ability of users to enter data, and controls the accessibility of logs, or they may be resident.

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

AltaLink® products have robust security features that are designed to protect the system from a wide range of threats. Below is a summary of some of the key security controls.

## Pre-Boot Security

### BIOS

The embedded BIOS used in AltaLink® products cannot be accessed by users. Unlike devices such as desktop and laptop computers that have a BIOS that can be accessed via a keystroke on startup, the BIOS of AltaLink® 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® products do not offer such a method to clear or reset the BIOS. (Note that configuration settings may be reset to factory defaults by an authorized administrator, however, this does not impact BIOS settings).

BIOS updates can be securely applied by device firmware updates. Firmware is protected from tampering by use of digital signatures (discussed later in this section).

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

### EMBEDDED ENCRYPTION

AES 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 always enabled by default. Media encryption and sanitization are discussed in Section 3 User Data Protection.

## Boot Process Security

### TRUSTED BOOT

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

## FIRMWARE INTEGRITY

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

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

Although there is ongoing firmware verification with the Trellix™ Embedded Control (formerly known as McAfee Embedded Control), an administrator can at any time invoke a check on the current executable software on the machine to verify it has not been altered or replaced. This complies with Common Criteria Certification requirements. This Software Verification Test can be invoked at the WebUI at any time. This feature utilizes FIPS 1403and CCC approved SHA256 digests of the software to validate its integrity.

## FIRMWARE RESTRICTIONS

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

Local Firmware Upgrade via USB port:
Xerox service technicians typically update product firmware using a USB port and a specially configured USB thumb drive for recovering non-functional machines or use a laptop with special serial cables and a network cable for recovering non-functional machines.

Network Firmware Update:
Product system administrators can update product firmware using the Embedded Web Server. The ability to apply a firmware update is restricted to roles with system administrator or Xerox service permissions. Firmware updates can be disabled by a system administrator.

Xerox Remote Services Firmware Update:
Xerox Remote Services can update product firmware securely over the internet using HTTPS. This feature can be disabled, scheduled, and includes optional email alerts for system administrators.

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

Controller

Marking Engine

Scanner

Document Feeder

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

High Capacity Feeder (No description on high capacity feeder is provided in this document because user’s image data will not be stored in it.)

High Capacity Stacker (No description on high capacity stacker is provided in this document because user’s image data will not be stored in it.)

Interface Module (No description on interface module is provided in this document because user’s image data will not be stored in it.)

The downloading function can be disabled by a system administrator from the Local UI or the Embedded Web Server.

For additional information on Firmware update methods such as lpr, raw tcp/ip printing, Fleet Orchestrator, and various upgrade methods supported, please see the System Administrator Guide.

## Runtime Security

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

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

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

## Event Monitoring and Logging

### CONFIGURATION WATCHDOG

The Atlantis 2.1 firmware allows Administrators to configure the periodic monitoring of multiple security related areas, each with one or more settings, totaling over 75 individual settings. If, during a check, a monitored security setting is discovered to have been changed, the system will automatically remediate it. In the case that remediation is unsuccessful, an email alert is generated, and the event is captured in the Audit Log (see below for information on the Audit Log). For a list of the security settings covered, please see the System Administrator Guide.

### AUDIT LOG

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

| Field | Description |
|---|---|
| **Index** | A unique value that identifies the event |
| **Date** | The date that the event happened in mm/dd/yy format |
| **Time** | The time that the event happened in hh:mm:ss format |
| **ID** | The type of event. The number corresponds to a unique description |
| **Description** | An abbreviated description of the type of event |
| **Additional Details** | Columns 6–10 list other information about the event, such as:<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 over two hundred unique events. A maximum of 15,000 events can be stored on the device. When the Audit Log reaches 13,500 entries (90% “full”), an email alert will be sent. When it reaches 28,500 events, the device will send another message stating there have been 15,000 events since the last alert. The device will keep alerting at 15,000 event intervals. When the number of events exceeds 15,000, audit log events will be deleted in order of timestamp, and then new events will be recorded. The audit log can be exported at any time by a user with administrative privileges. Note that as a security precaution, audit log settings and data can only be accessed via HTTPS and Audit Log can’t be disabled on this version of AltaLink® products.

### SECURITY INFORMATION EVENT MANAGEMENT (SIEM) SUPPORT

Xerox® AltaLink® supports the ability to directly connect to industry leading security and event management (SIEM) systems. Once configured, Xerox® AltaLink® B & C 81XX MFPs send security information, along with the event severity, to the SIEM system for processing and reporting. Events are generated as they occur and are transmitted in Common Event Format (CEF), which a SIEM system can interpret. The firmware supports connection to Trellix Enterprise Security Manager, LogRhythm, and Splunk Enterprise Security.

## Operational Security

### SERVICE TECHNICIAN (CSE) ACCESS RESTRICTION

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

If users require additional restrictions on the Customer Service Engineer Account, a setting is available within the Embedded Web Server to lock these services accounts. A qualified Xerox Service technician will need the machine administrator to grant access to service the machine.

### ADDITIONAL SERVICE DETAILS

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

### CLONING

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

### BACKUP AND RESTORE

Like cloning, backup and restore, can capture (copy) certain system and device-specific settings in a backup file. Backup files are similar to clone files as they are encrypted and digitally signed. This file may be reapplied to the same device at any time. Access to both create and restore a backup file can be restricted using role-based access controls. Backup files can only be created and applied through the Embedded Web Server. This backup can be stored at the device or exported, and the exported file is encrypted and signed.

### 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. Discussion of individual EIP application security is beyond the scope of this document. EIP applications utilize the security framework provided by the Third-party vendor and the EIP configuration of the product. Please consult documentation for individual EIP application as provided by the Third-party vendor for security details.

# 6. Configuration and Security Policy Management Solutions

This section describes various functionality available in the Xerox® AltaLink® products that help create and document operational workflows for network security management and orchestration.

## SECURITY DASHBOARD

Using a structured approach based on NIST recommended grouping of security features (Authentication, Confidentiality, Integrity, and Availability), the Security Dashboard has been created to assist System Administrators, and to provide a quick overview of this AltaLink MFP's security settings. All security settings are displayed on a single Embedded Web Server page, with links to the appropriate web pages for easy access and easy configuration.

## XEROX DEVICE MANAGER AND XEROX® CENTREWARE® WEB

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

## FLEET ORCHESTRATOR

Fleet Orchestrator allows the System Administrator to configure many devices in similar ways, automatically. After a device is configured, the System Administrator can distribute clone files with configuration settings to other devices in its Trust Community. The System Administrator sets up schedules to share configuration settings and files regularly and automatically. Additionally, the System Administrator can configure Fleet Orchestrator to reapply files on a given schedule to keep the configuration of the devices consistent. Auto-Assembly builds on Fleet Orchestrator by enabling devices to find and join a Trust Community in their network. This automates the addition of devices to the Trust Community for the System Administrator.

## UNIVERSAL PRINT

This option enables Microsoft Universal Print which leverages Microsoft Azure AD security mechanisms. The MFP uses public/private key exchange to request an OAUTH2 access token issued by Azure. The MFP generates a JSON Web Token and signs it with its certificate private key. The Azure-generated access token provides the MFP access to the Azure cloud. Individual Universal Print users are provided authorization to the MFP by the Azure Administrator. All the data in transit is encrypted using HTTPS with TLS 1.2.

## IMAGING SECURITY

Xerox® AltaLink® 2.5 release offers a new innovative feature called Imaging Security. This new feature helps customers protect sensitive information from intentional or unintentional disclosure by utilizing a proprietary Infra-red printing technology to mark documents and take action based on the presence of an IR mark. Customers may choose to mark all Copy jobs and/or all Print or Secure Print jobs. This method of marking can prevent the accidental disclosure of sensitive documents and ease our customers’ concerns around sensitive document management. For additional information on how to use this feature, please see the System Administrator Guide.

# 7. Identification, Authentication, and Authorization

AltaLink® products offer a range of authentication and authorization options to support various environments.

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

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

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

## Authentication

Xerox® AltaLink® devices support the following authentication mode:

Local Authentication

Network Authentication

Smart Card Authentication (CAC, PIV, SIPR, etc.)

Convenience Authentication

Xerox Workplace Cloud

Identity Provider (IdP) – Validate on Cloud

### LOCAL AUTHENTICATION

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

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

### PASSWORD POLICY

The following password attributes can be configured:

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

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

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

### NETWORK AUTHENTICATION

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

| Network Authentication Providers | |
|---|---|
| **Kerberos (Microsoft Active Directory)** | Supported |
| **Kerberos (MIT)** | Supported |
| **SMB NTLM Versions Supported** | NTLMv2 |
| **LDAP Versions Supported** | Version 3 |

### SMART CARD AUTHENTICATION

Smart Card authentication is considered very secure due to the nature of the Smart Card architecture and potential levels of encryption of data on the card itself. It provides two-factor security: 1) a PIN is required to unlock the smart card and 2) the user's smart card credential is authenticated over the network using Kerberos PKINIT authentication.

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

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

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

### CONVENIENCE AUTHENTICATION

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

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

Some examples of third-party convenience authentication providers include:

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

Pharos Print Management Solutions https://pharos.com

YSoft SafeQ https://www.ysoft.com/en

Contact your Xerox sales representative for details and other options.

### XEROX WORKPLACE CLOUD

This option enables cloud-based authentication. The printer connects directly to the Xerox® Workplace Cloud solution. This method provides multiple options for authentication. For additional information on how to use this feature, please see the System Administrator Guide.

### IDENTITY PROVIDER (IDP) – VALIDATE ON CLOUD

This option enables cloud-based authentication through an identity provider (IdP). The device establishes a secure connection with the IdP, then passes the user credentials to the IdP for authentication.

The IDP service's certificate authority (CA) chain of trust certificate(s) is used by the MFP to validate the IDP service's server authentication certificate. The IdP issues a SAML token on a per session basis for the user to access their authorized services. This token is destroyed after each session.

## Authorization (Role-Based Access Controls)

AltaLink® 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, plex, etc.). Only security-related permissions are discussed here.

### REMOTE ACCESS

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

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

### LOCAL ACCESS

Without RBAC permissions defined, basic information such as model, serial number, software version, IP address, and host name can be viewed without authentication. This can be disabled by disallowing access to device settings for unauthenticated users.

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

# 8. Additional Information and Resources

## Security @ Xerox®

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

## Responses to Known Vulnerabilities

Xerox has created a document which details the Xerox Vulnerability Management and Disclosure Policy used in discovery and remediation of vulnerabilities in Xerox software and hardware. It can be downloaded from this page: https://www.xerox.com/information-security/information-security-articles-whitepapers/enus.html

## Additional Resources

Below are additional resources.

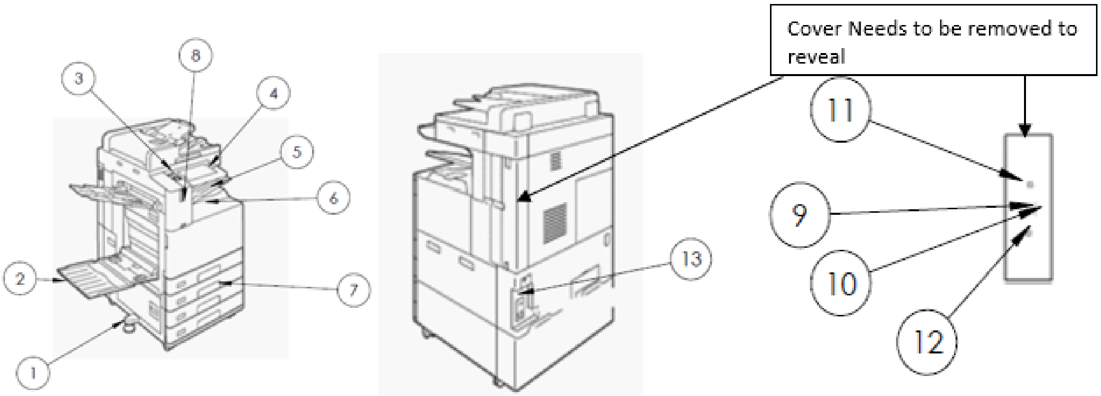
| Security Resource | URL |
|---|---|
| Frequently Asked Security Questions | https://www.xerox.com/en-us/information-security/frequently-asked-questions |
| Common Criteria Certified Products | https://security.business.xerox.com/en-us/documents/common-criteria/ |
| Current Software Release Quick Lookup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

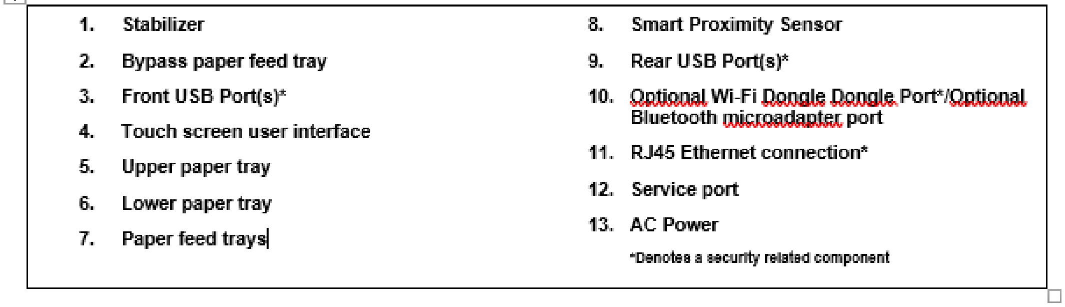
# 9. Appendix A: Product Security Profiles

This appendix describes specific details of each AltaLink® product.

## AltaLink® B8145/B8155/B8170 & C8130/C8135/C8145/C8155/C8170

### PHYSICAL OVERVIEW





1. Stabilizer
2. Bypass paper feed tray
3. Front USB Port(s)*
4. Touch screen user interface
5. Upper paper tray
6. Lower paper tray
7. Paper feed trays
8. Smart Proximity Sensor
9. Rear USB Port(s)*
10. Optional Wi-Fi Dongle Dongle Port*/Optional Bluetooth microadapter port
11. RJ45 Ethernet connection*
12. Service port
13. AC Power

*Denotes a security related component

.

## SECURITY RELATED INTERFACES

| Security Related Interfaces | |
|---|---|
| **Ethernet** | 10/100/1000 MB Ethernet interface. |
| **Optional Wi-Fi Dongle** | Supports optional 802.11 Dongle. |
| **Optional Bluetooth MicroAdapter** | Supports optional iBeacon support for AirPrint Discovery through Bluetooth Low Energy Beacons. |
| **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 & Rear 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 based on services.<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. |

## CONTROLLER NON-VOLATILE STORAGE

| Model | Size | Type | Use | User Data | How to Clear |
|---|---|---|---|---|---|
| **B8170, B8155, B8145, C8130, C8135, C8145, C8155, C8170** | 120 GB or higher | SSD* | Contains User Data (e.g., Print, Scan, Fax) and Configuration Settings. This data is encrypted, and Encryption is always on | Yes | Factory Reset |
| **B8170, B8155, B8145, C8130, C8135, C8145, C8155, C8170** | 320 GB or higher | HDD** | Contains User Data (e.g., Print, Scan, Fax) and Configuration Settings. This data is encrypted, and Encryption is always on | Yes | Factory Reset |

*SSD: Solid State Drive, is a Standard Configuration **HDD: Magnetic Hard Disk Drive, is a purchasable option

### CONTROLLER VOLATILE MEMORY

| Model | Size | Type | Use | User Data | How to Clear |
|---|---|---|---|---|---|
| **B8170, B8155, B8145, C8130, C8135, C8145, C8155** | 4 GB | DDR3 DRAM | Executable code, Printer control data, temporary storage of job data | Yes | Power off system |
| **C8170** | 8 GB | DDR3 DRAM | Executable code, Printer control data, temporary storage of job data | Yes | Power off system |

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

### MARKING ENGINE NON-VOLATILE STORAGE

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

### MARKING ENGINE VOLATILE MEMORY

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

# 10. Appendix B: Security Events

## AltaLink Security Events

| ID | Event | Description |
|---|---|---|
| 1 | System Startup | Device Name<br>Device Serial Number |
| 2 | System Shutdown | Device Name<br>Device Serial Number |
| 3 | Standard Disk Overwrite Started | Device Name<br>Device Serial Number |
| 4 | Standard Disk Overwrite Complete | Device Name<br>Device Serial Number<br>Overwrite Status |
| 5 | Print Job | Job Name<br>User Name<br>Source Service 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 |
| 9 | Email Job | Job Name<br>User Name<br>Completion Status<br>IIO Status<br>Accounting User ID<br>Accounting Account ID<br>Encryption On or Off<br>Total Number of SMTP Recipients |

|  |  |  |
|---|---|---|
|  |  | 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 | Job Name<br>User Name<br>Completion Status<br>IIO Status<br>Accounting User ID<br>Accounting Account ID |
| 13 | Embedded 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 |
| 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 |
| 16 | Full Disk Overwrite Started | Device Name<br>Device Serial Number |
| 17 | Full Disk Overwrite Complete | Device Name<br>Device Serial Number<br>Overwrite Status |
| 20 | Scan to Mailbox Job | Job Name or Directory Name<br>User Name<br>Completion Status<br>IIO Status |
| 21 | Delete File/Dir | Service (Print/Scan To Mailbox)<br>Job Name or Directory Name<br>User Name<br>Completion Status<br>IIO Status |
| 23 | Scan to Home | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Enabled/Disabled) |
| 24 | Scan to Home Job | Job Name or Directory Name<br>User Name<br>Completion Status (Normal/Error)<br>IIO Status |

| | | |
|---|---|---|
| | | Accounting User ID Name<br>Accounting Account ID Name<br>Total Number Net Destination<br>Net Destination |
| 26 | PagePack Login | Device Name<br>Device Serial Number<br>Completion Status:<br>Success (if Passcode is okay)<br>Failed (if Passcode is not okay)<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>Startup Mode or System Params Password or Start Job Password |
| 29 | Network User Login | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Success/Failed) |
| 30 | SA Login | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Success/Failed) |
| 31 | User Login | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Success/Failed) |
| 32 | Service Login Diagnostics | Service Name<br>Device Name<br>Device Serial Number<br>Completion Status (Success/Failed) |
| 33 | Audit Log Download | User Name<br>Device Name<br>Device Serial Number<br>Destination (WebUI, USB drive)<br>Completion Status (Success/Failed) |
| 34 | Immediate Job Overwrite Enablement | User Name<br>Device Name<br>Device Serial Number<br>IIO Status (Enabled/Disabled) |
| 35 | SA Pin Changed | User Name<br>Device Name<br>Device Serial Number<br>Completion Status |
| 36 | Audit Log File Saved | User Name<br>Device Name<br>Device Serial Number<br>Completion Status |

| | | |
|---|---|---|
| 37 | Force Traffic over Secure Connection (HTTPS) | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Enabled/Disabled/Terminated) |
| 38 | Security Certificate | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Created/Uploaded/Downloaded/Deleted) |
| 39 | IPsec | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Configured/Enabled/Disabled/Terminated) |
| 40 | SNMPv3 | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Configured/Enabled/Disabled/Terminated) |
| 41 | IP Filtering Rules | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Rule Added/Rule Edited/Rule Deleted) |
| 42 | Network Authentication Configuration | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Configured/Enabled/Disabled) |
| 43 | Device Clock | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Time Zone Changed/Date/Time Changed/Time Format Changed/Date Format Changed) |
| 44 | Software Upgrade | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Success/Failed) |
| 45 | Clone File Operations | User Name<br>Device Name<br>Device Serial Number<br>Completion Status |
| 46 | Scan Metadata Validation | Device Name<br>Device Serial Number<br>Completion Status (Success/Failed) |
| 47 | Xerox Secure Access Configuration | 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 Login | User Name (if valid Card and Password are entered) |

| | | |
|---|---|---|
| | | Device Name<br>Device Serial Number<br>Completion Status (Success/Failed) |
| 50 | Process Terminated | Device Name<br>Device Serial Number<br>Process Name<br>Termination Reason |
| 51 | Scheduled Disk Overwrite Configuration | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Enabled/Disabled)<br>Schedule Mode Configured<br>Schedule Frequency Configured<br>Schedule Day Of Week Configured<br>Schedule Day Of Month Configured<br>Schedule Minute Of Day Configured |
| 53 | Saved Job Backup | File Name<br>User Name<br>Completion Status (Normal/Error)<br>IIO Status |
| 54 | Saved Job Restore | File Name<br>User Name<br>Completion Status (Normal/Error)<br>IIO Status |
| 57 | Session Timer Logout | Device Name<br>Device Serial Number<br>Interface (WebUI, LUI, CAC)<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 (WebUI, LUI, CAC) (Timer affected by change)<br>User Name (who made this change)<br>Session IP (if available)<br>Completion Status (Success/Failed) |
| 59 | User Permissions | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Enabled/Disabled/Configured)<br>Interface (WebUI, LUI, CAC, SNMP)<br>Session IP Address (if available) |
| 60 | Device Clock NTP Configuration | Device Name<br>Device Serial Number<br>Enable/Disable/Config NTP<br>NTP Server IP Address/Hostname<br>Server Port<br>Completion Status (Success/Failed) |

| | | |
|---|---|---|
| 61 | Device Administrator Role Permission | User Name (of user making the change)<br>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 Configuration | User Name<br>Device Name<br>Device Serial Number<br>Card Type (SIPR Token, CAC/PIV)<br>Completion Status (Success/Failed) |
| 63 | IPv6 Configuration | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Success/Failed) |
| 64 | 802.1x Configuration | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Enabled/Configured Wired/Disabled) |
| 65 | Abnormal System Termination | Device Name<br>Device Serial Number |
| 66 | Local Authentication Enablement | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Enabled/Disabled) |
| 67 | Web User Interface Login Method | User Name<br>Device Name<br>Device Serial Number<br>Authentication Method Enabled (Network/Local) |
| 68 | FIPS Mode Configuration | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Enable/Disable/Configure) |
| 69 | Xerox Secure Access Login | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Success/Failed) |
| 70 | Print from USB Enablement | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Enabled/Disabled) |
| 71 | USB Port Enable/Disable | User Name<br>Device Name<br>Device Serial Number<br>USB Port ID<br>Completion Status (Enabled/Disabled) |
| 72 | Scan to USB Enablement | User Name<br>Device Name<br>Device Serial Number |

| | | |
|---|---|---|
| | | Completion Status (Enabled/Disabled) |
| 73 | System Log Download | Username<br>Device Name<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 Control Panel Configuration | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Enabled/Disabled/Configured) |
| 76 | Remote Control Panel Session | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Initiated/Terminated)<br>Remote Client IP Address |
| 77 | Remote Scan Feature Enablement | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Enable/Disable) |
| 78 | Remote Scan Job Submitted | User Name (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 | Remote Scan Job Completed | Job Name<br>User Name<br>Accounting User ID Name<br>Accounting Account ID Name<br>Completion Status (Destination) |
| 80 | SMTP Connection Encryption | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Enabled for STARTLS/ Enabled for STARTLS if available/ Enabled for TLS/Disabled/Configured) |
| 81 | Email Domain Filtering Rule | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Feature Enabled/Feature Disabled/Rule Added/Rule Deleted) |
| 82 | Software Verification Test Started | Device Name<br>Device Serial Number |

| | | |
|---|---|---|
| 83 | Software Verification Test Complete | Device Name<br>Device Serial Number<br>Completion Status (Success/Failed/Cancelled) |
| 84 | Trellix Embedded Security State | User Name<br>Device Name<br>Device Serial Number<br>Security Mode (Enhanced Security/Integrity Control)<br>Completion Status (Enabled/Disabled/Pending) |
| 85 | Trellix Embedded Security Event | Device Name<br>Device Serial Number<br>Type<br>(Read/Modify/Execute/Deluge)<br>Trellix Message Text |
| 87 | Trellix Embedded Security Agent | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Enabled/Disabled) |
| 88 | Digital Certificate Import Failure | Device Name<br>Device Serial Number<br>Email Address of Requestor (if available)<br>Failure Reason (Invalid Address/Invalid Certificate/Invalid Signature) |
| 89 | Device User Account Management | User Name (Managing User Names)<br>Device Name<br>Device Serial Number<br>User Name Added or Deleted<br>Completion Status (Created/Deleted) |
| 90 | Device User Account Password Change | User Name (Managing Passwords)<br>Device Name<br>Device Serial Number<br>User Name Affected<br>Completion Status (Password Modified) |
| 91 | Embedded Fax Job Secure Print Passcode | User Name (Managing Passcodes)<br>Device Name<br>Device Serial Number<br>Completion Status (Passcode Created/Changed) |
| 92 | Scan to Mailbox Folder Password | User Name (Managing Passwords)<br>Device Name<br>Device Serial Number<br>Folder Name<br>Completion Status (Password was Changed) |
| 93 | Embedded Fax Mailbox Passcode | User Name (Managing Passcodes)<br>Device Name<br>Device Serial Number<br>Completion Status (Passcode Created/Changed) |
| 94 | FTP/SFTP Filing Passive Mode | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Enabled/Disabled) |

| | | |
|---|---|---|
| 95 | Embedded Fax 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 Disabled) |
| 96 | Allow Weblet Installation | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Enable Installation/Block Installation) |
| 97 | Weblet Installation | User Name<br>Device Name<br>Device Serial Number<br>Weblet Name<br>Action (Install/Delete)<br>Completion (Success/Fail) |
| 98 | Weblet Enablement | User Name<br>Device Name<br>Device Serial Number<br>Weblet Name<br>Completion Status (Enable/Disable) |
| 99 | Network Connectivity Configuration | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Enable Wireless/Disable Wireless/Configure Wireless/Enable Wired/Disable Wired/Configure Wired/Enable WiFi Direct/Disable WiFi Direct/Configure WiFi Direct) |
| 100 | Address Book Permissions | User Name<br>Machine Name<br>Machine Serial Number<br>Completion Status (SA Only/Open Access Enabled WebUI)/ (SA Only/Open Access Enabled LocalUI) |
| 101 | Address Book Export | User Name<br>Machine Name<br>Machine Serial Number |
| 102 | SW Upgrade Policy | User Name<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 okay)<br>Failed (if Passcode is not okay)<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 |

| | | |
|---|---|---|
| | | Completion Status<br>Success (if Passcode is okay)<br>Failed (if Passcode is not okay)<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 Configuration | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Enabled Wireless/Disabled Wireless/Configured Wireless/Enabled Wired/Disabled Wired/Configured Wired) |
| 106 | SA PIN Reset | Device Serial Number<br>Completion Status (Success/Failed) |
| 107 | Convenience Authentication Login | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Success/Failed) |
| 108 | Convenience Authentication Configuration | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Enabled/Disabled/Configured) |
| 109 | Embedded Fax Passcode Length | User Name (Managing Passcodes)<br>Device Name<br>Device Serial Number<br>Completion Status (Passcode Length Changed) |
| 110 | Custom Authentication Login | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Success/Failed) |
| 111 | Custom Authentication Configuration | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Enabled/Disabled/Configured) |
| 112 | Billing Impression Mode | User Name<br>Device Name<br>Device Serial Number<br>Mode Set to (A4 Mode/A3 Mode)<br>Completion Status (Success/Failed) |
| 114 | Clone File Installation Policy | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Enable for Encrypted Files Only/Disable) |
| 115 | Save for Reprint Job | Job Name<br>User Name<br>Source (Print from USB/Print from URL/Print Protocol \| Web UI)<br>Completion Status |

| | | |
|---|---|---|
| 116 | Web User Interface Access Permission | Device Name<br>Device Serial Number<br>Completion Status (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 (Success/Failed) |
| 120 | Mopria Print Enablement | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Enabled/Disabled) |
| 123 | Near Field Communication (NFC) Enablement | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Enabled/Disabled) |
| 124 | Invalid Login Attempt<br>Lockout | Device Name<br>Device Serial Number<br>Interface (WebUI, Local UI \| SNMP \| Remote \| Fax \| Secure Fax)<br>Session IP Address (if available) |
| 125 | Secure Protocol Log Enablement | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Enable/Disable) |
| 126 | Display Device Information Configuration | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Configured) |
| 127 | Successful Login After Lockout Expired | Device Name<br>Device Serial Number<br>Interface (WebU/Local UI)<br>Session IP Address (if available)<br>Count of Invalid Attempts: xx attempts, where xx = the number of attempts |
| 128 | Erase Customer Data | Device Serial Number<br>Erase Customer Data<br>Device Serial Number<br>Completion Status (Success/Failed) |
| 129 | Audit Log SFTP Scheduled Configuration | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Enable/Disable/Configured) |
| 130 | Audit Log SFTP Transfer | User Name<br>Device Name<br>Device Serial Number<br>Destination Server<br>Completion Status (File Transmitted) |
| 131 | Remote Software Download Policy | User Name<br>Device Name<br>Device Serial Number |

| | | |
|---|---|---|
| | | Completion Status (Enabled/Disabled) |
| 132 | AirPrint & Mopria Scanning Configuration | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Enable/Disable/Configured) |
| 133 | AirPrint & Mopria Scan Job Submitted | Job Name (if accepted)<br>User Name (if available)<br>IP Address of Submitting Client<br>Device Name<br>Device Serial Number<br>Completion Status (Accept/Reject Request) |
| 134 | AirPrint & Mopria Scan Job Completed | Job Name<br>User Name (if available)<br>Completion Status |
| 136 | Remote Services NVM Write | Device Name<br>Device Serial<br>Completion Status (Success/Fail) |
| 137 | FIK Install via Remote Services | 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 Enablement | User Name<br>Device Name<br>Device Serial<br>Status (Enabled/Disabled) |
| 140 | Restore Backup Installation Policy | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Enabled/Disabled) |
| 141 | Backup File Downloaded | File Name<br>User Name<br>Interface (WebUI)<br>IP Address of the Destination (if applicable)<br>Completion Status (Success/Failed) |
| 142 | Backup File Restored | File Name<br>User Name<br>Device Name<br>Device IP address<br>Interface (WebUI)<br>Completion Status (Success/Failed) |
| 144 | User Permission Role 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 Configuration | User Name<br>Device Name<br>Device Serial Number<br>Role Name<br>Completion Status (Created/Deleted/Configured) |
| 146 | Admin Password Reset Policy Configuration | User Name<br>Device Name<br>Device Serial Number |
| 147 | Local User Account Password Policy | User Name<br>Device Name<br>Device Serial Number |
| 148 | Restricted Administrator Login | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Success/Failed) |
| 149 | Restricted Administrator Role Permission | User Name (of user making the change)<br>Device Name<br>Device Serial Number<br>User Name (of target user)<br>Action (Grant/Revoke) |
| 150 | Logout | Device Name<br>Device Serial Number<br>Interface (WebUI, LUI, CAC)<br>User Name (who was logged out)<br>Session IP (if available) |
| 151 | IPP Configuration | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Enabled/Disabled/Configured) |
| 152 | HTTP Proxy Server Configuration | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Enabled/Disabled/Configured) |
| 153 | Remote Services Software Download | Device Name<br>Device Serial Number<br>Completion Status (Success/Failed)<br>File Name |
| 154 | Restricted Admin Permission Role Configuration | User Name<br>Device Name<br>Device Serial Number<br>Restricted Admin Role Name<br>Completion Status (Created/Deleted/Configured) |
| 155 | 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) |

| | | |
|---|---|---|
| 156 | Lockdown and Remediate Security Enablement | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Enabled/Disabled) |
| 157 | Lockdown Security Check Complete | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Success/Failed) |
| 158 | Lockdown Remediation Complete | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Success/Failed) |
| 159 | Send Engineering Logs on Data Push | User Name (if available)<br>Device Name<br>Device Serial Number<br>Current Setting (Enabled/Disabled) |
| 160 | Print Submission of Clone Files Policy | User Name (if available)<br>Device Name<br>Device Serial Number<br>Completion Status (Enabled/Disabled/Permanently Removed) |
| 161 | Network Troubleshooting Data Capture | 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 Record 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) |
| 164 | One-Touch App Management | User Name<br>Device Name<br>Device Serial Number<br>1-Touch Application Display Name<br>Action (Install/Un-install)<br>Completion Status (Success/Failed) |
| 165 | SMB Browse Enablement | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Enabled/Disabled/Configured) |
| 166 | Standard Job Data Removal Started | Device Name<br>Device Serial Number |

| | | |
|---|---|---|
| 167 | Standard Job Data Removal Complete | Device Name<br>Device Serial Number<br>Completion Status (Success/Failed) |
| 168 | Full Job Data Removal Started | Device Name<br>Device Serial Number |
| 169 | Full Job Data Removal Complete | Device Name<br>Device Serial Number<br>Completion Status (Success/Failed) |
| 170 | Scheduled Job Data Removal Configuration | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Enable/Disable/Configured/Schedule Frequency Configured/Schedule Minute Of Day Configured/Schedule Day Of Month Configured/Schedule Day Of Week Configured/Schedule Mode Configured) |
| 171 | Cross-Origin Resource Sharing (CORS) | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Enabled/Disabled) |
| 172 | One-Touch App Export | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Success/Failed) |
| 173 | Fleet Orchestrator 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 | Fleet Orchestrator Configuration | User Name<br>Device Name<br>Device Serial Number<br>Trust Operation (Enable/Disable/Configure)<br>Completion Status (Success/Failed) |
| 175 | Fleet Orchestrator - 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 Enablement | 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 |

|  |  |  |
|---|---|---|
|  |  | 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 Configuration | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Enabled/Disabled/Configured) |
| 180 | iBeacon Active | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Enabled/Disabled) |
| 181 | Network Troubleshooting Feature | 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 Configuration | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Configured/Enabled/Disabled) |
| 184 | SFTP Browse Configuration | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Configured/Enabled/Disabled) |
| 189 | Smart Proximity Sensor “Sleep on Departure” Enablement | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Enabled/Disabled) |
| 190 | Cloud Browsing Enablement | User Name<br>Device Name<br>Device Serial Number<br>Feature (Scan to Cloud/Print from Cloud)<br>Interface (WebUI/SNMP)<br>Session IP Address<br>Completion Status (Enabled/Disabled) |
| 192 | Scan to Cloud Job | Job Name<br>User Name<br>Cloud Service<br>Completion Status<br>IIO Status<br>Accounting User ID Name<br>Accounting Account ID Name |
| 193 | Xerox Workplace Cloud Enablement | User Name<br>Device Name |

| | | |
|---|---|---|
| | | Device Serial Number<br>Completion Status (Enabled/Disabled) |
| 194 | Scan to Save FTP and SFTP Credentials Policy Configured | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Never/Always/Prompt) |
| 195 | Card Reader | Device Name<br>Device Serial Number<br>Completion Status (Connected/Disconnected) |
| 196 | EIP App Management | User Name<br>Device Name<br>Device Serial Number<br>App Name<br>Action (Install/Delete)<br>Completion Status (Success/Failed) |
| 197 | EIP App Enablement | User Name<br>Device Name<br>Device Serial Number<br>App Name<br>Completion Status (Enabled/Disabled) |
| 199 | Card Reader Upgrade Policy | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Enabled/Disabled) |
| 200 | Card Reader Upgrade Attempted | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Success/Failed)<br>Card Reader Upgrade File Name<br>Card Reader Serial Number |
| 201 | OCSP Responder Incomplete | User Name<br>Device Name<br>Device Serial Number<br>Service or Feature<br>Certificate Serial Number<br>Responder Address<br>Completion Status (No Connection/Unknown/Internal Error) |
| 202 | OCSP Responder Returns a ‘Revoked’ Status | User Name<br>Device Name<br>Device Serial Number<br>Service or Feature<br>Certificate Serial Number<br>Responder Address |
| 203 | Log Enhancement | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Started/Stopped)<br>Interface (WebUI/Remote Services)<br>IPv4 or IPv6 Address (if available) |

| | | |
|---|---|---|
| 204 | Syslog Server | User Name<br>Device Name<br>Device Serial Number<br>Server Address (if available)<br>Completion Status (Configured/Enabled/Disabled) |
| 205 | TLS Configuration | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Configured) |
| 206 | Security Dashboard Configuration | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Configured) |
| 208 | Canceled Job | Job Name<br>User Name<br>IIO Status<br>Accounting User ID<br>Accounting Account ID |
| 209 | Embedded Accounts | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Enabled/Disabled) |
| 210 | SNMP v1/v2c | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Configured/Enabled/Disabled) |
| 211 | Xerox Workplace Cloud Management | User Name<br>Device Name<br>Device Serial Number<br>Completion Status (Enabled/Disabled) |
| 216 | Infrared Security Configuration | User Name<br>Device Name<br>Device Serial Number<br>Action (Mark Feature Setup/Marking Setup/Mark Detection Setup)<br>Completion Status (Configured/Enabled/Disabled) |
| 217 | Infrared Security Mark Detected | User Name<br>Device Name<br>Device Serial Number<br>Job Name<br>Detected Mark Symbol Type<br>Detected Mark Symbol Label<br>Detection App (Copy/Email/ScanTo/Workflow Scanning)<br>Completion Status (Job Inhibited & Email Sent/Job Inhibited Only/Only Email Sent/Audit Log Only) |
| 218 | Universal Print Enablement | User Name<br>Device Name<br>Device Serial Number<br>Universal Print Completion Status (Enabled/Disabled)<br>Session IP Address (If Available) |

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