Security Guide

Xerox® AltaLink® B8145/B8155/B8170 Multifunction Printer

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

xerox™

2020 Xerox Corporation. All rights reserved. Xerox®, CentreWare®, AltaLink®, Xerox Extensible Interface Platform® are trademarks of Xerox Corporation in the United States and/or other countries. BR# 28402

Other company trademarks are also acknowledged.

Document Version: 1.0 (May 2020).

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

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

Contents

1. Introduction 1-4

Purpose 1-4

Target Audience 1-4

Disclaimer 1-4

2. Product Description 2-5

Physical Components 2-5

Architecture 2-6

User Interface 2-6

Scanner 2-6

Marking Engine 2-6

Controller 2-7

Controller External Interfaces 2-7

Front/Rear Panel USB (Type A) port(s) 2-7

10/100/1000 MB Ethernet TIA-568 Network Connector 2-7

Rear USB (Type B) Target Port 2-7

Optional Equipment 2-8

RJ-11 Analog Fax and Telephone 2-8

Wireless Network Connector 2-8

Bluetooth® MicroAdapter 2-8

Near Field Communications (NFC) Reader 2-8

SMART CARD – CAC/PIV 2-8

Foreign Product Interface 2-8

3. User Data Protection 3-1

User Data Protection While Within Product 3-1

Encryption 3-1

Private Key Management 3-1

Job Data Removal available on standard SSD configuration 3-1

Media Sanitization (Image Overwrite) available with optional HDD configuration 3-1

Immediate Image Overwrite available with optional HDD configuration 3-1

On-Demand Image Overwrite available with optional HDD configuration 3-2

User Data in Transit 3-2

Inbound User Data (Print Job Submission) 3-2

Email Signing and Encryption using S/MIME 3-2
Scanning to Network Repository, Email, Fax Server (Outbound User Data) 3-3
Scanning to User Local USB Storage Product (Outbound User Data) 3-3
Add on Apps – Cloud, Google, DropBox, and others (Outbound User Data) 3-4

4. Network Security 4-5

TCP/IP Ports and Services 4-5
Listening Services (inbound ports) 4-6
Network Encryption 4-7
IPsec 4-7
Wireless 802.11 Wi-Fi Protected Access (WPA) 4-7
TLS 4-8
SNMPv3 4-8
Public Key Infrastructure (PKI) 4-9
Device Certificates 4-9
Trusted Certificates 4-10
Minimum Key Length 4-10
Network Access Control 4-11
802.1x 4-11
Cisco Identity Services Engine (ISE) 4-11
Contextual Endpoint Connection Management 4-12
FIPS140-2 Compliance Validation 4-12
Additional Network Security Controls 4-13
IP Filtering 4-13
Personal Identifiable Information (PII) 4-13

5. Device Security: BIOS, Firmware, OS, Runtime, and Operational Security Controls 5-1

Pre-Boot Security 5-1
BIOS 5-1
Embedded Encryption 5-1
Boot Process Security 5-1
Trusted Boot 5-1
Firmware Integrity 5-2
Runtime Security 5-2
Operational Security 5-2
Firmware Restrictions 5-2
Event Monitoring and Logging 5-3

Configuration Watchdog 5-3
Audit Log 5-3
Security Information Event Management (SIEM) Support 5-4
Operational Security 5-4
Service Technician (CSE) Access Restriction 5-4
Additional Service Details 5-4
Cloning 5-4
Backup and Restore 5-4
EIP Applications 5-5

6. Configuration and Security Policy Management Solutions 6-1

7. Identification, Authentication, and Authorization 7-1
Authentication 7-1
Local Authentication 7-1
Password Policy 7-2
Network Authentication 7-2
Smart Card Authentication 7-2
Convenience Authentication 7-3
Authorization (Role-Based Access Controls) 7-3
Remote Access 7-3
Local Access 7-3

8. Additional Information and Resources 8-1
Security @ Xerox® 8-1
Responses to Known Vulnerabilities 8-1
Additional Resources 8-1

9. Appendix A: Product Security Profiles 9-2
AltaLink® B8145/B8155/B8170 & C8130/C8135/C8145/C8155/C8170 9-2
Physical Overview 9-2
Security Related Interfaces 9-3
Controller Non-Volatile Storage 9-3
Controller Volatile Memory 9-4
Marking Engine Non-Volatile Storage 9-4
Marking Engine Volatile Memory 9-4

10. Appendix B: Security Events 10-1
Xerox AltaLink Security Events 10-1

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.

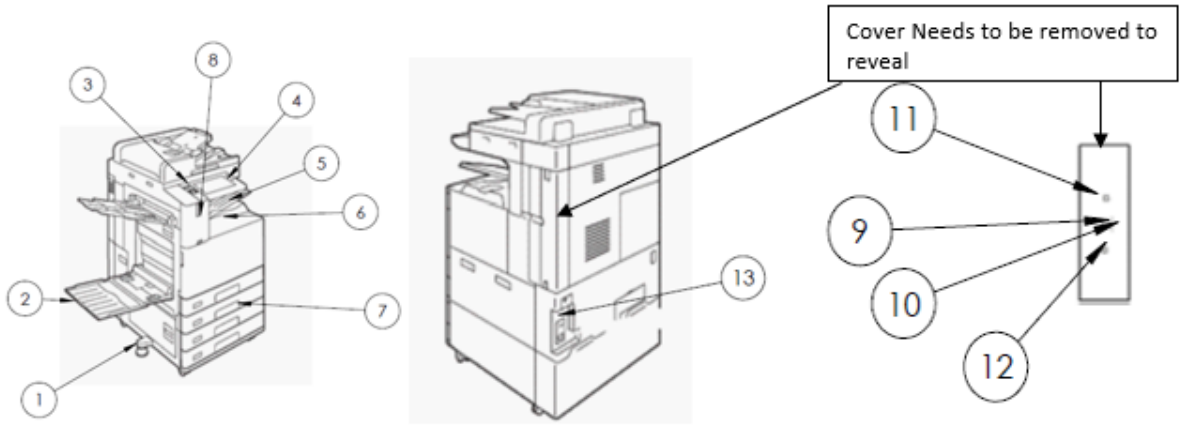
Disclaimer

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 handers, etc. may vary configuration, however, they are not relevant to security and are not discussed.

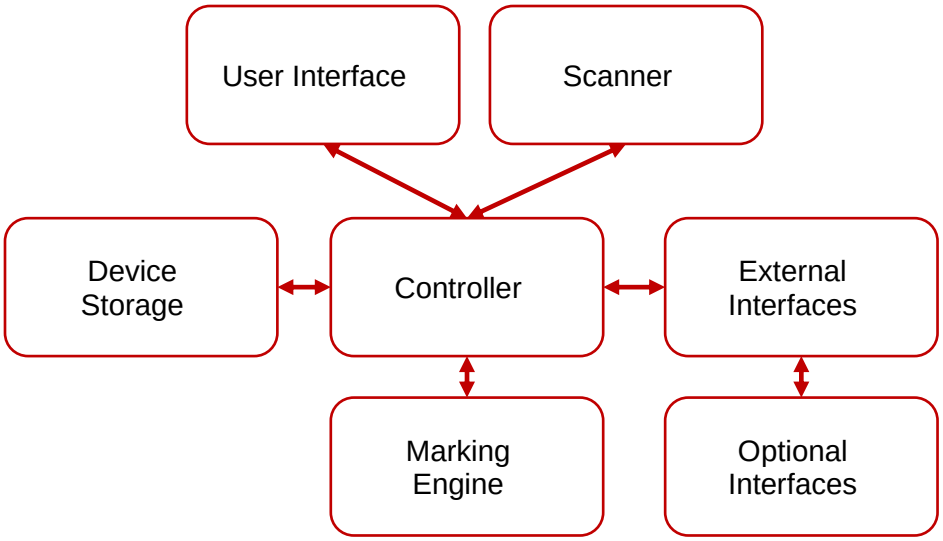


1. Stabilizer
2. Bypass paper feed tray
3. Front USB Port(s)*
4. Touch screen user interface
5. Upper paper tray
6. Lower paper tray
7. Paper feed trays
8. Smart Proximity Sensor
9. Rear USB Port(s)*
10. Optional Wi-Fi Dongle Dongle Port*/Optional Bluetooth microadapter port
11. RJ45 Ethernet connection*
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. A document handler moves originals into a position to be scanned. The scanner provides enough image processing for signal conditioning and formatting. The scanner does not store scanned images.

MARKING ENGINE

The Marking Engine performs copy/print paper feeding and transport, image marking, fusing, and document finishing. The marking engine is comprised of paper supply trays and feeders, paper transport, LED scanner, xerographics, and paper output and finishing. The marking engine is only

accessible to the Controller via inter-chip communication with no other access and does not store user data.

CONTROLLER

The controller manages document processing using proprietary hardware and algorithms to process documents into high-quality electronic and/or printed reproductions. Documents may be temporarily buffered in RAM during processing. Standard models are equipped with a Solid State Drive (SSD). 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 section Network Security.

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

Controller External Interfaces

FRONT/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 confirms 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. 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 read only from an NFC client. The data exchanged is not encrypted and may include information including system network status, IP address and product location. NFC functionality can be disabled using the embedded web server of the product. NFC functionality requires a software plugin that can be obtained from Xerox sales and support.

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

SMART CARD – CAC/PIV

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 ODIO available with HDD configuration.

MEDIA SANITIZATION (IMAGE 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 a the algorithm as described in the following link:
https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-88r1.pdf

IMMEDIATE IMAGE OVERWRITE AVAILABLE WITH OPTIONAL HDD CONFIGURATION

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

ON-DEMAND IMAGE OVERWRITE AVAILABLE WITH OPTIONAL HDD CONFIGURATION

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

User Data in Transit

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

INBOUND USER DATA (PRINT JOB SUBMISSION)

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

Encrypted Transport	Description
IPPS (TLS)	Submit print jobs via Secure Internet Printing Protocol. This protocol is based on HTTP and utilizes the TLS suite to encrypt data.
HTTPS (TLS)	Securely submit a print job directly to product via the built-in web server.
Xerox Print Stream Encryption	The Xerox Global Print Driver® supports document encryption 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
		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
		B8145, B8155, B8170 **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
	SFTP (SSH)	SSH-2
	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, 1.2
	SFTP (SSH)	SSH-2
	SMB (unencrypted)	v1, v2, v3
	SMB (with share encryption enabled)	V3
	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.

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

LISTENING SERVICES (INBOUND PORTS)

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

Port	Type	Service Name
80 or 443	TCP	HTTP including: Web User Interface Web Services for Products (WSD) WebDAV
68	UDP	DHC ACK Response to DHCP
88	UDP	Kerberos
110	TCP	POP3
139	TCP	NETBIOS
161	TCP	SNMP
162	TCP	SNMP Trap
137	UDP	NETBIOS (Name Service)
138	UDP	NETBIOS (Datagram Service)
161	UDP	SNMP
427	TCP/UDP	SLP
443	TCP	HTTPS – HTTP over TLS, IPPS
445	TCP	SMB
500 & 4500	TCP/UDP	IPsec
515	TCP	LPR
631	TCP	IPP
3702	TCP/UDP	WSD (Discovery)
4000	TCP	ThinPrint
5353	TCP/UDP	mDNS
5354	TCP	mDNS Responder IPC
9100	TCP	Raw IP (also known as JetDirect, AppSocket or PDL-datastream)
5909-5999	TCP	Remote Access to local display panel. Port is randomly selected and communications encrypted with TLS 1.2
51333	TCP	Device File Distribution downloads
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
		B8145, B8155, B8170, **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 WiFi support WPA2 Personal, WPA2 Enterprise, and Mixed Mode compliant with IEEE 802.11i. The wireless network adapters used in Xerox products are certified by the Wi-Fi Alliance.

		AltaLink® Multifunction
		B8145, B8155, B8170, **C8130, C8135, C8145, C8155, C8170**
Wi-Fi (802.11)		
	No Encryption	Supported
	WEP	RC4
	WPA2 Personal (PSK)	CCMP (AES), TKIP, TKIP+CCMP (AES), PMF (Protected Management Frame) optional support
	WPA2 Enterprise	CCMP (AES), TKIP, TKIP+CCMP (AES) PEAPv0 MS-CHAPv2 EAP-TLS EAP-TTLS/PAP EAP-TTLS/MS-CHAPv2

		EAP-TTLS/EAP-TLS PMF (Protected Management Frame) optional support
	BSSID Roaming Restriction	Supported

TLS

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

		AltaLink® Multifunction
		B8145, B8155, B8170, **C8130, C8135, C8145, C8155, C8170**
TLS		
	TLS Versions	TLS 1.2 (recommended) TLS 1.1 and TLS 1.2, or TLS 1.0, TLS 1.1 and TLS 1.2 (default)
	TLS Hash Algorithms	SHA-256 and above (recommended) SHA-1, SHA-256 and above (default)

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
		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 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 CAs 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 **B8145, B8155, B8170,** **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
		B8145, B8155, B8170, C8130, C8135, C8145, C8155, C8170
Trusted Certificates (CA & Peer device)		
	Minimum Length RSA Restriction Options	None, 1024, 2048
	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 Signing	Supported

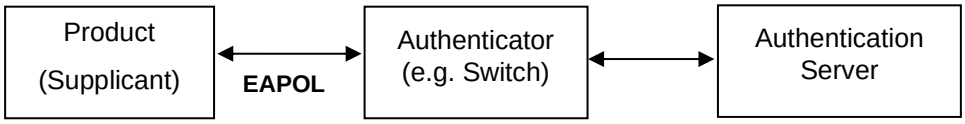
MINIMUM KEY LENGTH

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

Network Access Control

802.1X

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



		AltaLink® Multifunction
		B8145, B8155, B8170, **C8130, C8135, C8145, C8155, C8170**
Network Access Control		
	802.1x	Supported
	Authentication Methods	EAP-MD5, 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 level of access to printers and other end points in your network. As an example, you and your employees can get full printer access when accessing the network from a corporate workstation but be granted limited printer access when accessing the network from your personal Apple® iPhone®.

Cisco ISE allows you to deploy the following controls and monitoring of Xerox products: Automatically provision and grant network access rights to printers and MFPs to prevent inappropriate access (including automatically tracking new printing products connecting to the network):

- Block non-printers from connecting on ports assigned to printers
- Prevent impersonation (aka spoofing) of a printer/MFP
- Automatically prevent connection of non-approved print products
- Smart rules-based policies to govern user interaction with network printing products

Provide simplified implementation of security policies for printers and MFPs by:

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

Automated access to policy enforcement

- Provide extensive reporting of printing product network activity

		AltaLink® Multifunction
		B8145, B8155, B8170, **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.

FIPS140-2 COMPLIANCE VALIDATION

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

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

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 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's Boot Guard and the Unified EFI Forum/Microsoft specified (UEFI) BIOS approach to ensure a verified Chain of Trust is utilized to perform the 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.

Runtime Security

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

Executable control prevents unauthorized code from executing. Xerox has defined a whitelist of executable programs; software that is not on the secure whitelist is not allowed to execute. McAfee 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 McAfee® ePolicy Orchestrator® (ePO).

Operational Security

FIRMWARE RESTRICTIONS

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

Local Firmware Upgrade via USB port:
Xerox service technicians can update product firmware using a USB port and specially configured USB thumb drive.

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

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

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

Controller

Marking Engine

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 updates and various upgrade methods supported, please see the System Administrator Guide.

Event Monitoring and Logging

CONFIGURATION WATCHDOG

The Atlantis 2.1 firmware allows Administrators to configure the periodic monitoring of up to 34 security-related settings. If, during a check, a monitored security setting is discovered to have been changed, the system will automatically reset it. In the case that remediation is unsuccessful, an email alert is generated, and the event is captured in the Audit Log (see below for information on the Audit Log). For a list of the security settings covered, please see the System Administrator Guide.

AUDIT LOG

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

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

AltaLink® products currently support over a hundred unique events. A maximum of 15,000 events can be stored on the device. When the Audit Log reaches 13,500 entries (90% "full"), an email alert will be sent. 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 McAfee 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.

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.

BACKUP AND RESTORE

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

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

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

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 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

LOCAL AUTHENTICATION

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

Note: User names and passwords stored in the user database are not transmitted over the network 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 (including TLS 1.2)

SMART CARD AUTHENTICATION

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

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

Smart Cards	
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.

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.

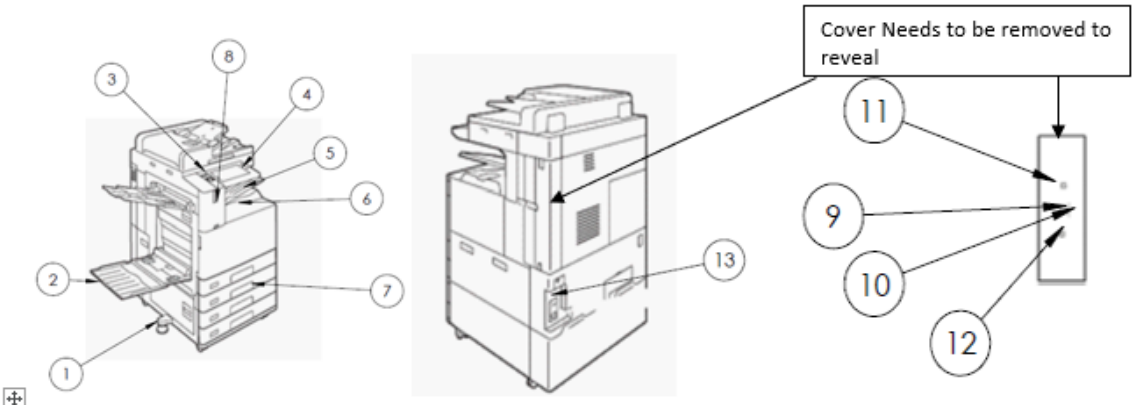
Security Resource	URL
Frequently Asked Security Questions	https://www.xerox.com/en-us/information-security/frequently-asked-questions
Common Criteria Certified Products	https://security.business.xerox.com/en-us/documents/common-criteria/
Current Software Release Quick Lookup Table	https://www.xerox.com/security
Bulletins, Advisories, 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	8.	Smart Proximity Sensor
2.	Bypass paper feed tray	9.	Rear USB Port(s)*
3.	Front USB Port(s)*	10.	Optional Wi-Fi Dongle Dongle Port*/Optional Bluetooth microadapter port
4.	Touch screen user interface	11.	RJ45 Ethernet connection*
5.	Upper paper tray	12.	Service port
6.	Lower paper tray	13.	AC Power
7.	Paper feed trays		

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

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

Xerox AltaLink Security Events

ID	Event	Description
1	System Startup	Device Name Device Serial Number
2	System Shutdown	Device Name Device Serial Number
3	Standard ODIO Started	Device Name Device Serial Number
4	Standard ODIO Complete	Device Name Device Serial Number Overwrite Status
5	Print Job	Job Name User Name Source Service Name Completion Status IIO Status Accounting User ID Accounting Account ID
6	Network Scan Job	Job Name User Name Completion Status IIO status Accounting User ID Accounting Account ID Total Number Net Destination Net Destination
7	Server Fax Job	Job Name User Name Completion Status IIO Status Accounting User ID Accounting Account ID Total Fax Recipient Phone Numbers Fax Recipient Phone Numbers Net Destination
8	iFax	Job Name User Name Completion Status IIO Status Accounting User ID Accounting Account ID Total Number of SMTP Recipients

		SMTP Recipients
9	Email Job	Job Name User Name Completion Status IIO Status Accounting User ID Accounting Account ID Encryption On or Off Total Number of SMTP Recipients SMTP Recipients
10	Audit Log Disabled	Device Name Device Serial Number
11	Audit Log Enabled	Device Name Device Serial Number
12	Copy Job	Job Name User Name Completion Status IIO Status Accounting User ID Accounting Account ID
13	Embedded Fax	Job Name User Name Completion Status IIO Status Accounting User ID Accounting Account ID Total Fax Recipient Phone Numbers Fax Recipient Phone Numbers
14	LAN Fax Job	Job Name User Name Completion Status IIO Status Accounting User ID Accounting Account ID Total Fax Recipient Phone Numbers Fax Recipient Phone Numbers
16	Full ODIO Started	Device Name Device Serial Number
17	Full ODIO Complete	Device Name Device Serial Number Overwrite Status
20	Scan to Mailbox Job	Job Name or Directory Name User Name Completion Status IIO Status
21	Delete File/Directory	Job Name or Directory Name User Name Completion Status IIO Status

23	Scan to Home	User Name Device Name Device Serial Number Completion Status (Enabled/Disabled)
24	Scan to Home Job	Job Name or Directory Name User Name Completion Status (Normal/Error) IIO Status Accounting User ID Name Accounting Account ID Name Total Number Net Destination Net Destination
25	Copy Store Job	Job Name or Directory Name User Name Completion Status (Normal/Error) IIO Status
26	PagePack Login	Device Name Device Serial Number Completion Status: Success (if Passcode is okay) Failed (if Passcode is not okay) Locked Out (if max attempts exceed 5) Time Remaining: Hrs (Remaining for next attempt) Min (Remaining for next attempt)
27	Postscript Passwords	Device Name Device Serial Number Startup Mode or System Params Password or Start Job Password
29	Network User Login	User Name Device Name Device Serial Number Completion Status (Success/Failed)
30	SA Login	User Name Device Name Device Serial Number Completion Status (Success/Failed)
31	User Login	User Name Device Name Device Serial Number Completion Status (Success/Failed)
32	Service Login	Service Name Device Name Device Serial Number Completion Status (Success/Failed)
33	Audit Log Download	User Name Device Name Device Serial Number Destination (WebUI, USB drive)

		Completion Status (Success/Failed)
34	IIO Feature Status	User Name Device Name Device Serial Number IIO Status (Enabled/Disabled)
35	SA Pin Changed	User Name Device Name Device Serial Number Completion Status
36	Audit Log Saved	User Name Device Name Device Serial Number Completion Status
38	X509 Certificate	User Name Device Name Device Serial Number Completion Status (Created/Uploaded/Downloaded)
39	IP Sec	User Name Device Name Device Serial Number Completion Status (Configured/Enabled/Disabled/Terminated)
40	SNMPv3	User Name Device Name Device Serial Number Completion Status (Configured/Enabled/Disabled/Terminated)
41	IP Filtering Rules	User Name Device Name Device Serial Number Completion Status (Rule Added/Rule Edited/Rule Deleted)
42	Network Authentication	User Name Device Name Device Serial Number Completion Status (Configured/Enabled/Disabled)
43	Device Clock	User Name Device Name Device Serial Number Completion Status (Time Zone Changed/Date/Time Changed/Time Format Changed/Date Format Changed)
44	SW Upgrade	User Name Device Name Device Serial Number Completion Status (Success/Failed)
45	Cloning	User Name Device Name Device Serial Number Completion Status
46	Scan Metadata Validation	Device Name Device Serial Number

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

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

71	USB Port Enable/Disable	User Name Device Name Device Serial Number USB Port ID Completion Status (Enabled/Disabled)
72	Scan to USB	User Name Device Name Device Serial Number Completion Status (Enabled/Disabled)
73	System Log Download	Username Device Name File Names Downloaded Destination (IP address or USB device) Completion Status (Success/Failed)
74	Scan to USB Job	Job Name User Name Completion Status IIO Status Accounting User ID Name Accounting Account ID Name
75	Remote UI Feature	User Name Device Name Device Serial Number Completion Status (Enabled/Disabled/Configured)
76	Remote UI Session	User Name Device Name Device Serial Number Completion Status (Initiated/Terminated) Remote Client IP Address
77	Remote Scan Feature (Driver)	User Name Device Name Device Serial Number Completion Status (Enable/Disable)
78	Remote Scan Job Submitted (Driver)	User Name (at client if available) IP Address of Submitting Client Device Name Device Serial Number Job Name (if accepted) Completion Status (Accept/Reject/Request)
79	Scan to Web Service Job Remote Scan Job Completed (Driver)	Job name User Name Accounting User ID Name Accounting Account ID Name Completion Status (Destination)
80	SMTP Connection Encryption	User Name Device name Device Serial Number

		Completion Status (Enabled for STARTLS/ Enabled for STARTLS if available/ Enabled for TLS/Disabled/Configured)
81	Email Domain Filtering Rule	User Name Device Name Device Serial Number Completion Status (Feature Enabled/Feature Disabled/Rule Added/Rule Deleted)
82	Software Self Test Started	Device Name Device Serial Number
83	Software Self Test Complete	Device Name Device Serial Number Completion Status (Success/Failed/Cancelled)
84	McAfee Security State	User Name Device Name Device Serial Number Security Mode (Enhanced Security/Integrity Control) Completion Status (Enabled/Disabled/Pending)
85	McAfee Security Event	Device Name Device Serial Number Type (Read/Modify/Execute/Deluge) McAfee Message Text
87	McAfee Agent	User Name Device Name Device Serial Number Completion Status (Enabled/Disabled)
88	Digital Certificate Import Failure	Device Name Device Serial Number Email Address of Requestor (if available) Failure Reason (Invalid Address/Invalid Certificate/Invalid Signature)
89	User Name Add/Delete	User Name (Managing User Names) Device Name Device Serial Number User Name Added or Deleted Completion Status (Created/Deleted)
90	User Name Password Change	User Name (Managing Passwords) Device Name Device Serial Number User Name Affected Completion Status (Password Modified)
91	eFax Job Secure Print Passcode	User Name (Managing Passcodes) Device Name Device Serial Number Completion Status (Passcode Created/Changed)
92	Scan2Mailbox Folder Password Change	User Name (Managing Passwords) Device Name Device Serial Number

		Folder Name Completion Status (Password was Changed)
93	eFax Mailbox Passcode	User Name (Managing Passcodes) Device Name Device Serial Number Completion Status (Passcode Created/Changed)
94	FTP/SFTP Filing Passive Mode	User Name Device Name Device Serial Number Completion Status (Enabled/Disabled)
95	eFax Forwarding Rule	User Name Device Name Device Serial Number Fax Line 1 or 2 (if applicable) Completion Status (Rule Edit/Rule Enabled/Rule Disabled)
96	EIP Weblets Allow Install	User Name Device Name Device Serial Number Completion Status (Enable Installation/Block Installation)
97	EIP Weblets Install	User Name Device Name Device Serial Number Weblet Name Action (Install/Delete) Completion (Success/Fail)
98	EIP Weblets Enable	User Name Device Name Device Serial Number Weblet Name Completion Status (Enable/Disable)
99	Network Connectivity	User Name Device Name Device Serial Number Completion Status (Enable Wireless/Disable Wireless/ Configure Wireless/Enable Wired/Disable Wired/ Configure Wired/Enable WiFi Direct/Disable WiFi Direct/Configure WiFi Direct)
100	Address Book Permissions	User Name Machine Name Machine serial number Completion Status (SA Only/Open Access Enabled WebUI)/ (SA Only/Open Access Enabled LocalUI)
101	Address Book Export	User Name Machine Name Machine Serial Number
102	SW Upgrade	User Name Device Name Device Serial Number Completion Status (Enable Installation/Disable Installation)

103	Supplies Plan Activation	Device Name Device Serial Number Completion Status Success (if Passcode is okay) Failed (if Passcode is not okay) Locked out (if Max Attempts Exceed 5) Time Remaining Hrs (remaining for next attempt) Min (remaining for next attempt)
104	Plan Conversion	Device Name Device Serial Number Completion Status Success (if Passcode is okay) Failed (if Passcode is not okay) Locked out (if Max Attempts Exceed 5) Time Remaining Hrs (remaining for next attempt) Min (remaining for next attempt)
105	IPv4	User Name Device Name Device Serial Number Completion Status (Enabled Wireless/Disabled Wireless/ Configured Wireless/Enabled Wired/Disabled Wired/ Configured Wired)
106	SA PIN Reset	Device Serial Number Completion Status (Success/Failed)
107	Convenience Authentication Login	User Name Device Name Device Serial Number Completion Status (Success/Failed)
108	Convenience Authentication	User Name Device Name Device Serial Number Completion Status (Enabled/Disabled/Configured)
109	eFax Passcode Length	User Name (Managing Passcodes) Device Name Device Serial Number Completion Status (Passcode Length Changed)
110	Custom Authentication Login	User Name Device Name Device Serial Number Completion Status (Success/Failed)
111	Custom Authentication	User Name Device Name Device Serial Number Completion Status (Enabled/Disabled/Configured)
112	Billing Impression Mode	User Name Device Name Device Serial Number

		Mode Set to (A4 Mode/A3 Mode) Completion Status (Success/Failed)
114	Device Cloning	User Name Device Name Device Serial Number Completion Status (Enable for Encrypted Files Only/Disable)
115	Save for Reprint Job	Job Name User Name Print from USB/Print from URL Completion Status
116	WebUI Access Configure	Device Name Device Serial Number Completion Status (Standard Access/Open Access/Restricted)
117	System Log Push to Xerox	Username if Authenticated Server Destination URL Log Identifier String (Filename) Completion Status (Success/Failed)
119	Scan to WebDAV Job	Job Name User Name Completion Status IIO status Accounting User ID Name Accounting Account ID Name WebDAV Destination
123	Near Field Communication	User Name Device Name Device Serial Number Completion Status (Enabled/Disabled)
124	Invalid Login Attempt Lockout	Device Name Device Serial Number Interface (WebUI, Local UI) Session IP Address (if available)
125	Protocol Audit Log Enable/Disable	User Name Device Name Device Serial Number Completion Status (Enable/Disable)
126	Display Device Information Configure	User Name Device Name Device Serial Number Completion Status (Configured)
127	Invalid Login Lockout Expires	Device Name Device Serial Number Interface (WebUI) Session IP Address (if available) Count of Invalid Attempts: xx attempts, where xx = the number of attempts
128	Erase Customer Data	Device Serial Number Erase Customer Data Device Serial Number

		Completion Status (Success/Failed)
129	Audit Log SFTP Scheduled Configure	User Name Device Name Device Serial Number Completion Status (Enable/Disable/Configured)
130	Audit Log SFTP Transfer	User Name Device Name Device Serial Number Destination Server Completion Status (File Transmitted)
131	Remote Software Download	User Name Device Name Device Serial Number Completion Status (Enable/Disable)
132	AirPrint & Mopria Scanning	User Name Device Name Device Serial Number Completion Status (Enable/Disable/Configured)
133	AirPrint & Mopria Scan Job Submitted	Job Name (if accepted) User Name (if available) IP Address of Submitting Client Device Name Device Serial Number Completion Status (Accept/Reject Request)
134	AirPrint & Mopria Scan Job Completed	Job Name User Name (if available) Completion Status
136	Remote Services NVM Write	Device Name Device Serial Completion Status (Success/Fail)
137	Remote Services FIK Install	Device Name Device Serial Completion Status (Success/Fail) User-readable names for the features being installed
138	Remote Services Data Push	Device Name Device Serial Completion Status (Success/Fail)
139	Remote Services	User Name Device Name Device Serial Status (Enabled/Disabled)
140	Restore	User Name Device Name Device Serial Number Completion Status (Enable/Disable)
141	Backup-Restore File Downloaded	File Name User Name Interface (WebUI)

		IP Address of the Destination (if applicable) Completion Status (Success/Failed)
142	Backup-Restore Restore Installed	File Name User Name Device Name Device IP address Interface (WebUI) Completion Status (Success/Failed)
143	Google Cloud Services	User Name Device Name Device Serial Number Completion Status (Enabled/Disabled/Configured)
144	User or Group Role Assignment	User Name Device Name Device Serial Number User or Group Name (Assigned) Role Name Action (Added/Removed)
145	User Permission Role	User Name Device Name Device Serial Number Role Name Completion Status (Created/Deleted/Configured)
146	Admin Password Policy Configure	User Name Device Name Device Serial Number
147	Local User Account Password Policy	User Name Device Name Device Serial Number
148	Restricted Admin Login	User Name Device Name Device Serial Number Completion Status (Success/Failed)
149	Grant/Revoke Restricted Admin Rights	User Name (of user making the change) Device Name Device Serial Number User Name (of target user) Action (Grant/Revoke)
150	Manual Session Logout	Device Name Device Serial Number Interface (WebUI, LUI, CAC) User Name (who was logged out) Session IP (if available)
151	IPP	User Name Device Name Device Serial Number Completion Status (Enabled/Disabled/Configured)
152	HTTP Proxy Server	User Name Device Name

		Device Serial Number Completion Status (Enabled/Disabled/Configured)
153	Remote Services Software Download	Device Name Device Serial Number File Name
154	Restricted Admin Permission Role	User Name Device Name Device Serial Number Restricted Admin Role Name Completion Status (Created/Deleted/Configured)
155	EIP Weblet Installation Security Policy	User Name Device Name Device Serial Number Policy (Allow Installation of Encrypted Weblets/Allow Installation of Both Encrypted and Unencrypted Weblets)
156	Lockdown and Remediate Security	User Name Device Name Device Serial Number Completion Status (Enabled/Disabled)
157	Lockdown Security Check Complete	User Name Device Name Device Serial Number Completion Status (Success/Failed)
158	Lockdown Remediation Complete	User Name Device Name Device Serial Number Completion Status (Success/Failed)
159	Send Engineering Logs on Data Push	User Name (if available) Device Name Device Serial Number Current Setting (Enabled/Disabled)
160	Allow the Print Submission of Clone Files	User Name (if available) Device Name Device Serial Number Completion Status (Enabled/Disabled)
161	Network Troubleshooting Start/Stop	User Name Device Name Device Serial Number Completion Status (Started/Stopped)
162	Network Troubleshooting Data Download	User Name File Name (of downloaded file) Device Name Device Serial Number Destination (IP Address) Completion Status (Success/Failed)
163	DNS-SD Text File Download	User Name File Name (of downloaded file) Device Name Device Serial Number

		Destination (IP address) Completion Status (Success/Failed)
164	1-Touch App Management	User Name Device Name Device Serial Number 1-Touch Application Display Name Action (Install/Un-install) Completion Status (Success/Failed)
165	SMB Browse	User Name Device Name Device Serial Number Completion Status (Enabled/Disabled/Configured)
166	Job Data Removal Standard Started	Device Name Device Serial Number
167	Job Data Removal Standard Complete	Device Name Device Serial Number Completion Status (Success/Failed)
168	Job Data Removal Full Started	Device Name Device Serial Number
169	Job Data Removal Full Complete	Device Name Device Serial Number Completion Status (Success/Failed)
170	Scheduled Job Data Removal Configure	User Name Device Name Device Serial Number Completion Status (Enable/Disable/Configured)
171	Cross-Origin Resource Sharing (CORS)	User Name Device Name Device Serial Number Completion Status (Enable/Disable)
172	1-Touch App Export	User Name Device Name Device Serial Number Completion Status (Success/Failed)
173	Device File Distribution Trust Operations	User Name Device Name Device Serial Number Member Name Member Serial Number TC Lead Device Name TC Lead Serial Number Trust Operation (Grant/Revoke) Completion Status (Success/Failed)
174	Device File Distribution Feature	User Name Device Name Device Serial Number Trust Operation (Enable/Disable/Configure) Completion Status (Success/Failed)

175	Device File Distribution – Store File for Distribution	User Name Device Name Device Serial Number File type (SWUP/Clone/Add-On) File Name
176	Xerox Configuration Watchdog	User Name Device Name Device Serial Number Completion Status (Enabled/Disabled)
177	Xerox Configuration Watchdog Check Complete	User Name (if available, SYSTEM, if executed as a scheduled event) Device Name Device Serial Number Completion Status (Success/Failed)
178	Xerox Configuration Watchdog Remediation Complete	User Name (if available, SYSTEM, if executed as a scheduled event) Device Name Device Serial Number Completion Status (Success/Failed)
179	ThinPrint Feature	User Name Device Name Device Serial Number Completion Status (Enabled/Disabled/Configured)
180	Beaconing for iBeacon for AirPrint Discovery	User Name Device Name Device Serial Number Completion Status (Enabled/Disabled)
181	Network Troubleshooting	User Name Device Name Device Serial Number Completion Status (Installed/Uninstalled)
182	POP3 Connection Encryption (TLS)	User Name Device Name Device Serial Number Completion Status (Enabled/Disabled/Configured)
183	FTP Browse	User Name Device Name Device Serial Number Completion Status (Configured/Enabled/Disabled)
184	SFTP Browse	User Name Device Name Device Serial Number Completion Status (Configured/Enabled/Disabled)
189	Smart Proximity Sensor Sleep on Departure	User Name Device Name Device Serial Number Completion Status (Enabled/Disabled)
190	Cloud Service	User Name Device Name Device Serial Number Completion Status (Enabled/Disabled)

192	Scan to Cloud Job	Job Name User Name Cloud Service Completion Status IIO Status Accounting User ID Name Accounting Account ID Name
193	Xerox Workplace Cloud	User Name Device Name Device Serial Number Completion Status (Enabled/Disabled)
194	Scan to Save FTP and SFTP Credentials Policy	User Name Device Name Device Serial Number Completion Status (Never/Always/Prompt)
195	Card Reader	Device Name Device Serial Number Completion Status (Connected/Disconnected)
196	EIP Apps	User Name Device Name Device Serial Number App Name Action (Install/Delete) Completion Status (Success/Failed)
197	EIP Apps	User Name Device Name Device Serial Number App Name Action (Install/Delete) Completion Status (Enabled/Disabled)
204	Syslog Server	User Name Device Name Device Serial Number Server IPv4 Address (if available) Server IPv6 Address (if available) Completion Status (Configured/Enabled/Disabled)
205	TLS (Version and/or Hash)	User Name Device Name Device Serial Number Completion Status (Configured)