Xerox®

Security Guide

Personal Class Multi-Function Products & Single-Function Printer

Xerox® Multi-Function Printers	Xerox® Printer
B205, B215	B210

© 2019 Xerox Corporation. All rights reserved. Xerox and Xerox and Design® are trademarks of Xerox Corporation in the United States and/or other countries. BR25497

Other company trademarks are also acknowledged.

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

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

Document Version: 1.0 (July 2019).

Table of Contents

1 Introduction

Purpose

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

Target Audience

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

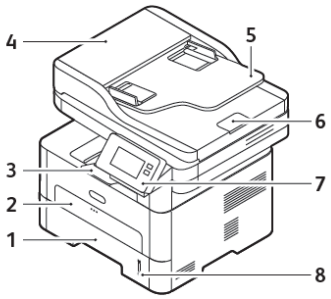
Disclaimer

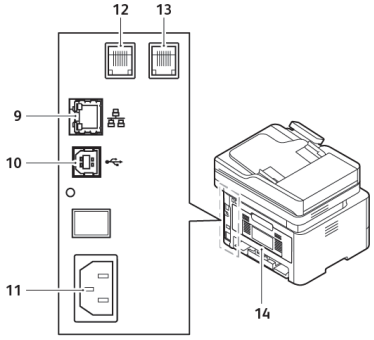
The information in this document is accurate to the best knowledge of the authors and is provided without warranty of any kind. In no event shall Xerox be liable for any damages whatsoever resulting from user's use or disregard of the information provided in this document including direct, indirect,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

2 Product Description

Physical Components

B205/B210/B215 products consist of an input document handler and scanner, marking engine, controller, and user interface. A typical configuration is depicted below. Please note that options including finishers, paper trays, document handers, etc. may vary configuration, however, they are not relevant to security and are not discussed.



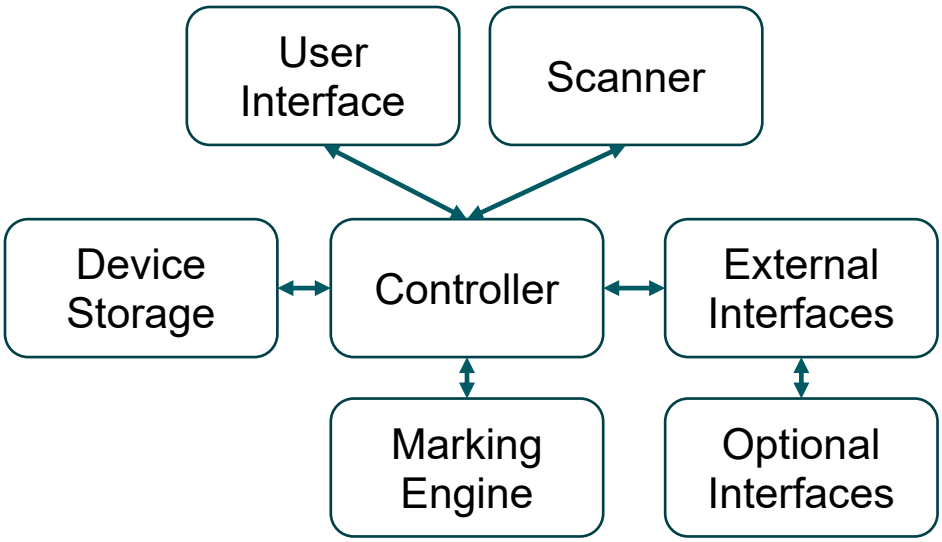


1. Paper Tray 1
2. Manual Feeder Slot
3. Output Tray
4. Document Feeder Cover
5. Document Feeder Input Tray
6. Document feeder Output Support
7. Touchscreen User Interface
8. Paper Level Indicator
9. RJ45 Ethernet connection*
10. Rear USB port
11. AC Power
12. Telephone Line Socket (Line)
13. Extension Telephone Socket (EXT)
14. Rear Cover

*Denotes a security related component

Architecture

B205/B210/B215 products share a common architecture which is depicted below. The following sections describe components in detail.



User Interface

The user interface detects soft and hard button actuations and provides text and graphical prompts to the user. The user interface is sometimes referred to as the Graphical User Interface (GUI) or Local UI (LUI) to distinguish it from the remote web server interface (WebUI).

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

Scanner

The scanner converts documents from hardcopy to electronic data. A document handler moves originals into a position to be scanned. The scanner provides enough image processing for signal conditioning and formatting. The scanner does not store scanned images**.**

Marking Engine

The Marking Engine performs copy/print paper feeding and transport, image marking, fusing, and document finishing. The marking engine is comprised of paper supply trays and feeders, paper transport, LED scanner, xerographics, and paper output and finishing. The marking engine is only accessible to the Controller via inter-chip communication with no other access and does not store user data**.**

Controller

The controller manages document processing using proprietary hardware and algorithms to process documents into high-quality electronic and/or printed reproductions. Documents may be temporarily buffered in RAM during processing. Some models may be equipped with additional storage options such as magnetic Hard Disk Drive (HDD), Solid State Disk (SSD), SD Card, or Flash media. For model specific details please see Appendix A: Product Security Profiles. B205/B210/B215 products encrypt user data and include media sanitization (overwrite) options that ensure that erased data cannot be recovered, described further in section 3 User Data Protection.

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

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

Controller External Interfaces

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

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

  Note that features that use the front USB ports (such as Scan To USB) can be disabled independently or restricted using role-based access controls.

- Connection of optional equipment such as NFC or CAC readers.
- Firmware updates may be submitted through the front USB ports. (Note that the product must be configured to allow local firmware updates, or the update will not be processed.

10/100/1000 MB Ethernet RJ-45 Network Connector
This is a standard RJ45 Ethernet network connector and confirms to IEEE Ethernet 802.3 standards.

Rear USB (Type B) Target port
A USB type B port located on the controller board at the rear of the product. This port supports the following:

- USB target connector used for printing

Note: This port can be disabled completely by a system administrator.

Optional Equipment

RJ-11 Analog Fax and Telephone

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

Wireless Network Connector

B205/B210/B215 products include an embedded wireless module.

Near Field Communications (NFC) Reader

The B205/B210/B215 system does not support Near Field Communications.

SMART CARD – CAC/PIV

The B205/B210/B215 system does not support Smart Cards.

Foreign Product Interface

The B205/B210/B215 system does not support Foreign Product Interface.

3 User Data Protection

Xerox printers and multifunction products receive, process, and may optionally store user data from several sources including as local print, scan, fax, or copy jobs or mobile and cloud applications, etc. Xerox products protect user data being processed by employing strong encryption. When the data is no longer needed, the Image Overwrite (IIO) feature automatically erases and overwrites the data on magnetic media, rendering it unrecoverable. As an additional layer of protection, an extension of IIO called On-Demand Image Overwrite (ODIO) can be invoked to securely wipe all user data from magnetic media.

User Data protection while within product

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

Encryption

All user data being processed or stored to the product is encrypted by default. Note that encryption may be disabled to enhance performance on B205/B210/B215 products (though this is not recommended in secure environments). Xerox B205/B210/B215 products do not have such an option.

The algorithm used in the product is AES-256. The encryption key is automatically created at start up and stored in the RAM. The key is deleted by a power-off, due to the physical characteristics of the RAM.

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

Media Sanitization (Image Overwrite)

The B205/B210/B215 system does not use magnetic hard disk drives. All Memory is NAND Flash or DDR3 SDRAM. The B205/B210/B215 system does not support Image Overwrite.

Note: Solid State storage media such as Solid-State Disk, eMMC, SD-Card, and Flash media cannot be completely sanitized by multi-pass overwriting methods due to the memory wear mapping that occurs. (Additionally, attempts to do so would also greatly erode the operational lifetime of solid state media). Solid State media is therefore not recommended for use in highly secure environments. Please refer to NIST-800-88 “Table A-8: Flash Memory-Based Storage Product Sanitization” for technical details.

Immediate Image Overwrite
The B205/B210/B215 system does not support Immediate Image Overwrite (IIO).

On-Demand Image Overwrite
The B205/B210/B215 system does not support On-Demand Overwrite (ODIO).

User Data in transit

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

Inbound User Data

Print Job Submission

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

Encrypted Transport	Description
IPPS (TLS)	Submit print jobs via Secure Internet Printing Protocol. This protocol is based on HTTP and utilizes the TLS suite to encrypt data.
HTTPS (TLS)	Securely submit a print job directly to product via the built-in web server.
Xerox Print Stream Encryption	The Xerox Global Print Driver® supports document encryption when submitting Secure Print jobs to enabled products. Simply check the box to Enable Encryption when adding the Passcode to the print job.

Outbound User Data

Scanning to Network Repository, Email, Fax Server

B205/B215 multifunction products support scanning of hardcopy documents to external network locations including file repositories and email and facsimile services. In addition to supporting network level encryption including IPSec and WPA Xerox products support the following.

Protocol	Encryption	Description
FTP	N/A	Unencrypted FTP.
SMBv3	Optional	Encryption may be enabled on a Windows share. B205/B210/B215 products currently support SMB encryption. B205/B210/B215 products do not currently support SMB encryption.
SMBv2	N/A	Unencrypted SMB
SMBv1	N/A	(Not used as a transport protocol. Used for network discovery only)
SMTP (email)	S/MIME	The product uses SMTP to transmit data to the email server. Email authentication, encryption, and signing are supported. Please refer to the Network Security section of this document for details.

Scanning to User Local USB Storage Product

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

Add on Apps- Cloud, Google, DropBox, and others

The Xerox App Gallery® contains several additional applications that extend the capabilities of Xerox products. Discussion of App security is beyond the scope of this document. Xerox Apps utilize the security framework provided by the 3rd party vendor. (For example, Microsoft O365 or Google apps would utilize Microsoft & Google's security mechanisms respectively). Please consult documentation for individual Apps and 3rd party security for details.

	Xerox® Multifunction B215	Xerox® Multifunction B205	Xerox® Printer B210
Local Data Encryption (HDD, SDD, IC, SD Card)	AES-256	AES-256	AES-256
Federal Information Protection Standard 140-2	NO	NO	NO

Media Sanitization NIST 800-171 (Image Overwrite)		All models use magnetic HDD	Models with magnetic HDD. See Appendix A: Product Security Profiles	Models with magnetic HDD. See Appendix A: Product Security Profiles
Print Submission				
	IPPS (TLS)	Supported	Supported	Supported
	HTTPS (TLS)	Supported	Supported	Supported
	Xerox Print Stream Encryption	Supported	(Not currently supported)	(Not currently supported)
Scan to Repository Server				
	SMB (unencrypted)	v1, v2, v3	v3	(Not Applicable)
	SMB (with share encryption enabled)	V3	(Not currently supported)	(Not Applicable)
	FTP (unencrypted)	Supported	(Not currently supported)	(Not Applicable)
Scan to Fax Server				
	SMB (unencrypted)	v1, v2, v3	v3	(Not Applicable)
	SMB (with share encryption enabled)	V3	(Not currently supported)	(Not Applicable)
	S/MIME	Supported	(Not currently supported)	(Not Applicable)
	FTP (unencrypted)	Supported	(Not currently supported)	(Not Applicable)
	SMTP (unencrypted)	Supported	Supported	(Not Applicable)
Scan to Email				
	S/MIME	Supported	(Not currently supported)	(Not Applicable)
	SMTP (unencrypted)	Supported	Supported	(Not Applicable)

4 Network Security

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

TCP/IP Ports & Services

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

Inbound (Listening Services)		Out Bound (Network Client)
Print Services LPR, IPP, Raw IP, etc. Management Services SNMP, Web interface, WebServices etc. Infrastructure & Discovery Services IPSEC, SSDP, WSD, mDNS, NetBIOS, etc.		Built-in Scan Services FTP, HTTP, SMB, CIFS, SMTP & SMTPS, etc. Authentication Services LDAP & LDAPS, SMB, Kerberos. Infrastructure ISAKMP (IPSec), DHCP & DHCPv6, etc.

Listening services (inbound ports)

The following table summarizes all potentially open ports on the product. These ports can be enabled/disabled within the product configuration.

Port	Type	Service Name
80 or 443	TCP	HTTP including: Web User Interface Web Services for Products (WSD) WebDAV
631 or 443	TCP	HTTP (IPP)
137	UDP	NETBIOS (Name Service)
138	UDP	NETBIOS (Datagram Service)
161	UDP	SNMP
427	TCP/UDP	SLP
445	TCP	CIFS
500 & 4500	UDP	IPSec
515	TCP	LPR

631	TCP	IPP
1900	UDP	SSDP
3702	TCP	WSD (Discovery)
5353	UDP	mDNS
9100	TCP	Raw IP (also known as JetDirect, AppSocket or PDL-datastream)
5909-5999	TCP	Remote Access to local display panel. Port is randomly selected and communications encrypted with TLS 1.2.
53202	TCP	WSD Transfer
53303	TCP	WSD Print
53404	TCP	WSD Scan

Network Encryption

IPSec

Internet Protocol Security (IPsec) is a network security protocol capable of providing encryption and authentication at the packet level. B205/B210/B215 products support IPSec for both IPv4 and IPv6 protocols.

		Xerox® Multifunction B215	Xerox® Multifunction B205	Xerox® Printer B210
IPSec				
	Supported IP Versions	IPv4, IPv6	IPv4, IPv6	IPv4, IPv6
	Key exchange authentication method	Preshared Key	Preshared Key	Preshared Key
	Transport Mode	Transport mode only	Transport & Tunnel mode	Transport mode only
	Security Protocol	ESP only	ESP & AH	ESP only
	ESP Encryption Method	AES, 3DES, DES	AES, 3DES, Null	AES, 3DES, DES
	ESP Authentication Methods	SHA1, SHA256, None	SHA1, SHA256, None	SHA1, SHA256, None

Wireless 802.11 Wi-Fi Protected Access (WPA)

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

		Xerox® Multifunction B215	Xerox® Multifunction B205	Xerox® Printer B210
Wi-Fi (802.11)				
	No Encryption	Supported	Supported	Supported
	WEP	RC4	RC4	RC4
	WPA2 Personal (PSK)	CCMP (AES), TKIP, TKIP+CCMP (AES)	CCMP (AES), TKIP, TKIP+CCMP (AES)	CCMP (AES), TKIP, TKIP+CCMP (AES)
	WPA2 Enterprise	Not Supported	Not Supported	Not Supported
	BSSID Roaming Restriction	Supported	(Not Currently Supported)	(Not Currently Supported)

TLS

B205/B210/B215 products support the latest version, TLS 1.2.

		Xerox® Multifunction B215	Xerox® Multifunction B205	Xerox® Printer B210
TLS Versions Supported				
	Product Web Interface	1.2, 1.1, 1.0	1.2, 1.1, 1.0	1.2, 1.1, 1.0
	Product Web Services	1.2, 1.1, 1.0	1.2, 1.1, 1.0	1.2, 1.1, 1.0
	Product IPPS printing	1.2, 1.1, 1.0	1.2, 1.1, 1.0	1.2, 1.1, 1.0

Public Key Encryption (PKI)

A digital certificate is a file that contains data used to verify the identity of the client or server in a network transaction. A certificate also contains a public key used to create and verify digital signatures. To prove identity to another product, a product presents a certificate trusted by the other product. The product can also present a certificate signed by a trusted third party and a digital signature proving that it owns the certificate.

A digital certificate includes the following data:

- Information about the owner of the certificate
- The certificate serial number and expiration date
- The name and digital signature of the certificate authority (CA) that issued the certificate
- A public key
- A purpose defining how the certificate and public key can be used

There are four types of certificates:

- A Product Certificate is a certificate for which the printer has a private key. The purpose specified in the certificate allows it to be used to prove identity.
- A CA Certificate is a certificate with authority to sign other certificates.
- A Trusted Certificate is a self-signed certificate from another product that you want to trust.
- A domain controller certificate is a self-signed certificate for a domain controller in your network. Domain controller certificates are used to verify the identity of a user when the user logs in to the product using a Smart Card.

For protocols such as HTTPS, the printer is the server, and must prove its identity to the client Web browser. For protocols such as 802.1X, the printer is the client, and must prove its identity to the authentication server, typically a RADIUS server.

Device Certificates

B205/B210/B215 products support both CA signed and self-signed certificates. Product certificates support a bit length of up to 2048 bits.

A CA signed certificate can be created by generating a Certificate Signing Request (CSR), and sending it to a CA or a local server functioning as a CA to sign the CSR. An example of a server functioning as a certificate authority is Windows Server 2008 running Certificate Services. When the CA returns the signed certificate, install it on the printer.

Alternatively, a self-signed certificate may be created. When you create a Product Certificate, the product generates a certificate, signs it, and creates a public key used in SSL/TLS encryption.

		Xerox® Multifunction B215	Xerox® Multifunction B205	Xerox® Printer B210
Device Certificates				
	Certificate Length	1024, 2048	1024, 2048	1024, 2048
	Supported Hashes	SHA1, SHA256	SHA256, SHA512	SHA256, SHA512
	Product Web Server	Supported	Supported	Supported
	IPPS (TLS) Printing	Supported	Supported	Supported
	802.1X Client	Supported	Supported	Supported
	Email Signing	(Not currently supported)	(Not currently supported)	(Not Applicable)
	Email Encryption	Supported	(Not currently supported)	(Not Applicable)
	OCSP Signing	(Not currently supported)	(Not currently supported)	(Not currently supported)
	IPSec	Supported	Supported	Supported
	SFTP	(Not currently supported)	(Not currently supported)	(Not Applicable)

Trusted Certificates
Public certificates may be imported to the product's certificate store for validation of trusted external products. The following categories are supported:

• A Trusted Root CA Certificate is a certificate with authority to sign other certificates. These certificates usually are self-signed certificates that come from another product or service that you want to trust.

• An Intermediate CA Certificate is a certificate that links a certificate to a Trusted Root CA Certificate in certain network environments.

• Other Certificates are certificates that are installed on the printer for solution-specific uses.

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

		Xerox® Multifunction B215	Xerox® Multifunction B205	Xerox® Printer B210
Trusted Certificates				
	Minimum Length Restriction Options	None, 1024, 2048	1024, 2048	1024, 2048
	Maximum Length	4096	4096	4096
	Supported Hashes	SHA1/224/256/384/512	SHA1/224/256/384/512	SHA1/224/256/384/512
	Supported Formats	.cer, .crt, .der, .pem, PKCS#7 (.p7b), PKCS#12 (.pfx, .p12)	.cer, .der, PKCS#7, PKCS#12 (.pfx, .p12)	.cer, .der, PKCS#7, PKCS#12 (.pfx, .p12)
	IPSec	Supported	Supported	Supported
	LDAP	Supported	Supported	(Not currently supported)
	Scanning (HTTPS/TLS)	(Not currently supported)	(Not currently supported)	(Not Applicable)
	Scanning (SFTP/SSH)	(Not currently supported)	(Not currently supported)	(Not Applicable)
	802.1X Client	Supported	Supported	Supported
	Email Signing	(Not currently supported)	(Not currently supported)	(Not Applicable)
	Email Encryption	Supported	(Not currently supported)	(Not Applicable)
	OCSP Signing	(Not currently supported)	(Not currently supported)	(Not currently supported)

Certificate Validation
B205/B210/B215 devices support certificate validation with configurable checks for OSCP and CRL. Validation checks include:

- Validation of certificate path
- Certificate expiration
- Validation of trusted CA
- Signature validation

Email Signing and Encryption using S/MIME

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

		Xerox® Multifunction B215	Xerox® Multifunction B205	Xerox® Printer B210
Email S/MIME				
	Versions	v3	(Not currently supported)	(Not Applicable)
	Digest	SHA1, SHA256, SHA384, SHA512	(Not currently supported)	(Not Applicable)
	Encryption	3DES, AES256	(Not currently supported)	(Not Applicable)

SNMPv3

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

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

• Authentication to verify that the message is from a valid source

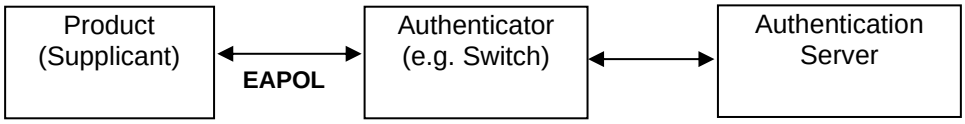
• Encryption of packets to prevent unauthorized access

		Xerox® Multifunction B215	Xerox® Multifunction B205	Xerox® Printer B210
SNMPv3				
	Digest	SHA1, MD5	SHA1, MD5	SHA1, MD5
	Encryption	DES, AES128	DES, AES128	DES, AES128

Network Access Control

802.1x

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



		Xerox® Multifunction B105	Xerox® Multifunction B205	Xerox® Printer B210
Network Access Control				
	802.1x	Supported	Supported	Supported
	Authentication Methods	EAP-MD5 PEAP EAP-MSCHAPV2 EAP-TLS	EAP-MD5 PEAP EAP-MSCHAPV2 EAP-TLS	EAP-MD5 PEAP 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 B205/B210/B215 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

		Xerox® Multifunction B215	Xerox® Multifunction B205	Xerox® Printer B210
Network Access Control				
	Cisco ISE	(Not supported currently)	(Not supported currently)	(Not supported currently)

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 B205/B210/B215 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

B205/B210/B215 products do not support FIPS 140-2.

Additional Network Security Controls

Additional network security controls are discussed in the following sections.

Endpoint Firewall Options

		Xerox® Multifunction B215	Xerox® Multifunction B205	Xerox® Printer B210
Firewall		IP Whitelisting	IP Whitelisting	IP Whitelisting
	Stateful Firewall	(Not currently supported)	(Not currently supported)	(Not currently supported)
	IP Whitelist	Supported	Supported	Supported

IP Whitelisting (IP Address Filtering)
B205/B210/B215 products support IP Whitelisting only.

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

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

B205/B210/B215 products have robust security features that are designed to protect the system from a wide range of threats. Below is a summary of some of the key security controls.

Pre-Boot BIOS Protection

BIOS

- The BIOS is inaccessible and cannot be cleared or reset.
- The BIOS can only be modified by a firmware update, which is digitally signed.

Embedded Encryption

- Configuration Settings (including security settings) and User Data are encrypted by AES.

Boot Process Integrity

Firmware Integrity & Verification

- Firmware is digitally signed.

Runtime Intrusion Prevention & Detection

Runtime Executable Control

- Not supported for Personal Class products.
  Xerox Office Class AltaLink® and VersaLink® support enhanced security controls.

Runtime Intrusion Detection – Memory Control

- Not supported for Personal Class products.
  Xerox Office Class AltaLink® and VersaLink® support enhanced security controls.

Event Monitoring & Logging

- Not supported for Personal Class products.
  Xerox Office Class AltaLink® and VersaLink® support enhanced security controls.

Continuous Operational Security

Firmware and Diagnostic Security Controls

- Not supported for Personal Class products.
  Xerox Office Class AltaLink® and VersaLink® support enhanced security controls.

Fail Secure Vs Fail Safe

B205/B210/B215 products are designed to fail secure.

When a security control is compromised, the control is no longer trustworthy, and a system is at risk of further compromise. In such a scenario, security products may either fail safe [open] or fail secure [closed].

An example from physical security is a door. If power is lost the door may either:

- Unlock and 'fail safe' to an open state (likely for safety reasons such as in a public building).
- Lock and 'fail secure' for security reasons (such as a bank vault).

Boot Process Security

Firmware Integrity

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

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

Firmware Restrictions

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

- Local Firmware Upgrade via USB port:
Xerox service technicians can update product firmware using a USB port and specially configured USB thumb drive. This ability can be restricted by enabling the Customer Service Engineer Restriction feature which will require entry of a unique, customer designated password in order to accept the update.

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

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

Additional Service Details

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

Backup & Restore (Cloning)

The B205/B210/B215 system does not support Cloning.

EIP Applications

The B205/B210/B215 system does not support Xerox Extensible Interface Platform (EIP).

XCP (eXtensible Customizable Platform)

The B205/B210/B215 system does not support the eXtensible Customizable Platform (XCP) plug-in interface.

6 Configuration & Security Policy Management Solutions

Xerox Device Manager and Xerox CentreWare® Web (available as a free download) centrally manage Xerox Devices. Additionally, B205/B210/B215 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

The B205/B210/B215 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.

Authentication

The B205/B210/B215 devices support the following authentication mode:

- Local Authentication
- Network Authentication

Local Authentication

The local user database stores user credential information. The printer uses this information for local authentication and authorization. When you configure local authentication, the printer checks the credentials that a user provides against the information in the user database. When you configure local authorization, the printer checks the user database to determine which features the user is allowed access.

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

Password Policy
The following password attributes can be configured:

		Xerox® Multifunction B215	Xerox® Multifunction B205	Xerox® Printer B210
Password Policy				
	Minimum Length	1	1	1
	Maximum Length	63	63	63
	Password cannot contain User Name	(Not currently supported)	(Not currently supported)	(Not currently supported)
	Password complexity options	(Not currently supported)	(Not currently supported)	(Not currently supported)

Network Authentication

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

		Xerox® Multifunction B215	Xerox® Multifunction B205	Xerox® Printer B210
Network Authentication Providers				
	Kerberos (Microsoft Active Directory)	Supported	(Not currently supported)	(Not currently supported)
	Kerberos (MIT)	Supported	(Not currently supported)	(Not currently supported)

	SMB NTLM Versions Supported	NTLMv2	(Not currently supported)	(Not currently supported)
	LDAP Versions Supported	Version 3 (including TLS 1.2)	(Not currently supported)	(Not currently supported)

Smart Card Authentication

B205/B210/B215 Products do not support Smart Card Authentication.

Convenience Authentication

B205/B210/B215 Products do not support Convenience Authentication.

Simple Authentication (non-secure)

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

Authorization (Role Based Access Controls)

B205/B210/B215 products do not support Role Based Access Controls.

.

8 Additional Information & Resources

Security @ Xerox®

Xerox maintains an evergreen public web page that contains the latest security information pertaining to its products. Please see 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.

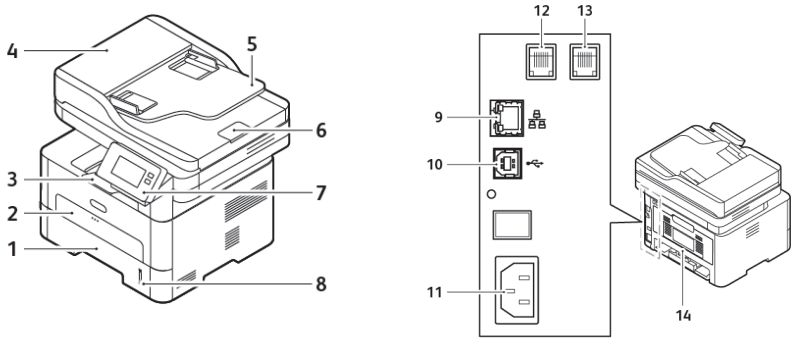
Security Resource	URL
Frequently Asked Security Questions	https://www.xerox.com/en-us/information-security/frequently-asked-questions
Common Criteria Certified Products	https://security.business.xerox.com/en-us/documents/common-criteria/
Current Software Release Quick Lookup Table	https://www.xerox.com/security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

Appendix A: Product Security Profiles

This appendix describes specific details the B205/B210/B215 product family.

Xerox® B205/B210/B15

Physical Overview



1. Paper Tray 1
2. Manual Feeder Slot
3. Output Tray
4. Document Feeder Cover
5. Document Feeder Input Tray
6. Document feeder Output Support
7. Touchscreen User Interface
8. Paper Level Indicator
9. RJ45 Ethernet connection*
10. Rear USB port
11. AC Power
12. Telephone Line Socket (Line)
13. Extension Telephone Socket (EXT)
14. Rear Cover

*Denotes a security related component

Security Related Interfaces

Ethernet	10/100/1000 MB Ethernet interface.
Optional Wi-Fi Dongle	Supports optional 802.11 Dongle.
Rear USB 3.0 (Type B)	USB target connector used for printing. Note: This port can be disabled completely by a system administrator.
Front Panel Optional USB2.0 (Type A) port(s)	Users may insert a USB thumb drive to print from or store scanned files to. (Physical security of this information is the responsibility of the user or operator.) Note that features that leverage USB ports (such as Scan To USB) can be disabled independently or restricted using role based access controls. Firmware upgrades may be applied using this port. Connection of optional equipment such as NFC or CAC readers. Note: This port can be disabled completely by a system administrator.

Encryption and Overwrite

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

Controller Non-Volatile Storage

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

Note: Configuration settings may be erased by the reset to factory defaults feature.
IC- Integrated Circuit, soldered to circuit board
HDD- Magnetic Hard Disk Drive
SSD- Solid State Disk
SD Card- Secure Digital Card

Controller Volatile Memory

Size	Type	Use	User Data	How to Clear	Volatile
4GB	DDR3 SDRAM	Executable code, Printer control data, temporary storage of job data	Yes	Power off system	Yes
Additional Information: The controller operating system memory manager allocates memory dynamically between OS, running processes, and temporary data which includes jobs in process. When a job is complete, the memory pages in use are freed and reallocated as required by the OS.					

Marking Engine Non-Volatile Storage

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

Marking Engine Volatile Memory

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