Xerox® Product Security Guide

Xerox® B410 Printer
Xerox® C410 Color Printer

Document Version: 2.0 (May 2025)

B410 **C410**

xerox™

Document Version: 2.0 (May 2025).

Contents

1. Introduction

Purpose

The purpose of this document is to disclose information for the Xerox® B410 and Xerox® C410 (referred to as “products” or “the system” in this document) 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

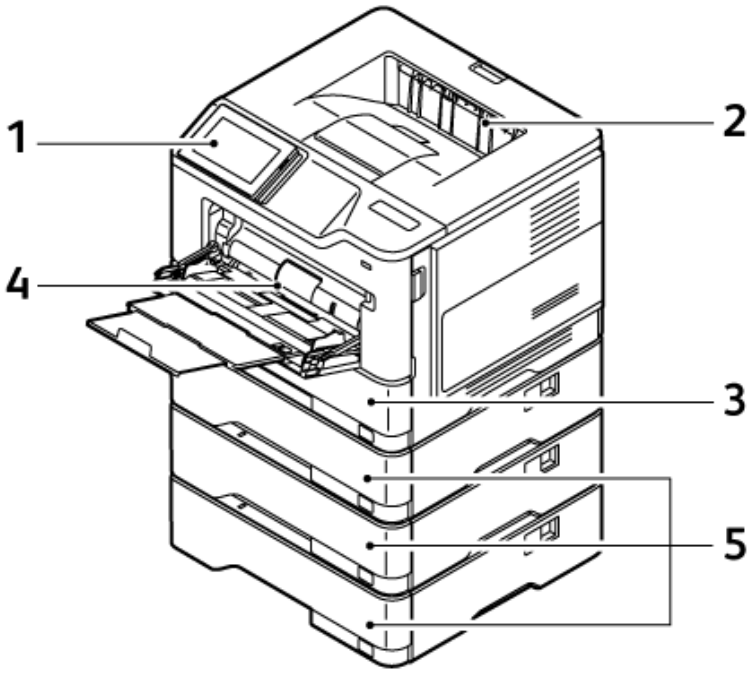
The content of this document is provided for information purposes only. Performance of the products referenced herein is exclusively subject to the applicable Xerox Corporation terms and conditions of sale and/or lease. Nothing stated in this document constitutes the establishment of any additional agreement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

2. Product Description

PHYSICAL COMPONENTS

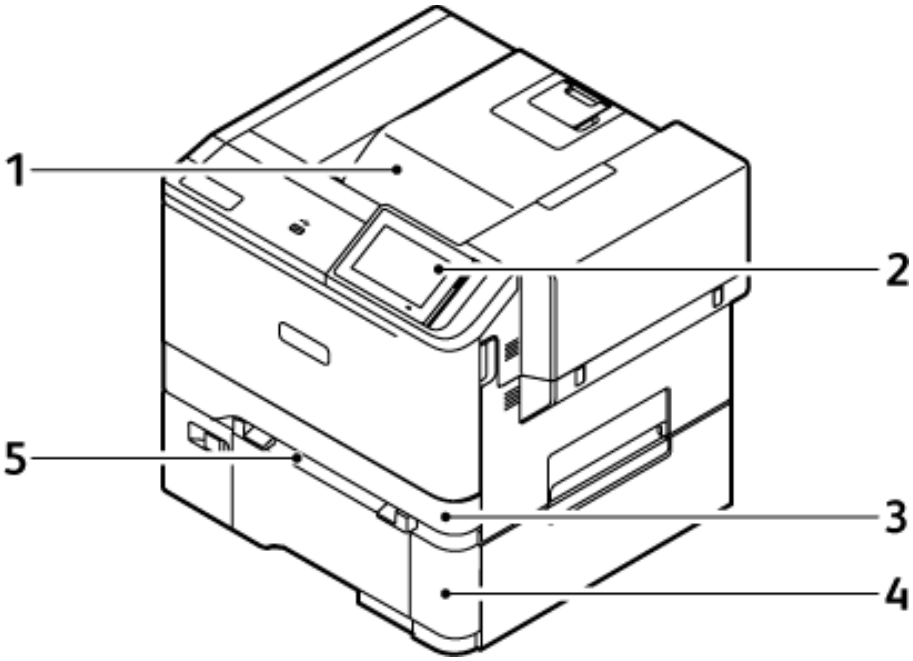
Xerox® B410 and C410 products consist of marking engine, controller, and user interface. A typical configuration is depicted below. Please note that options including paper trays, etc. may vary by configuration, however, they are not relevant to security and are not discussed.

B410



1. Control Panel
2. Standard Output Tray
3. Tray 1, Standard 550-sheet Tray
4. Multipurpose Feeder or Bypass Tray
5. Optional Feed Trays

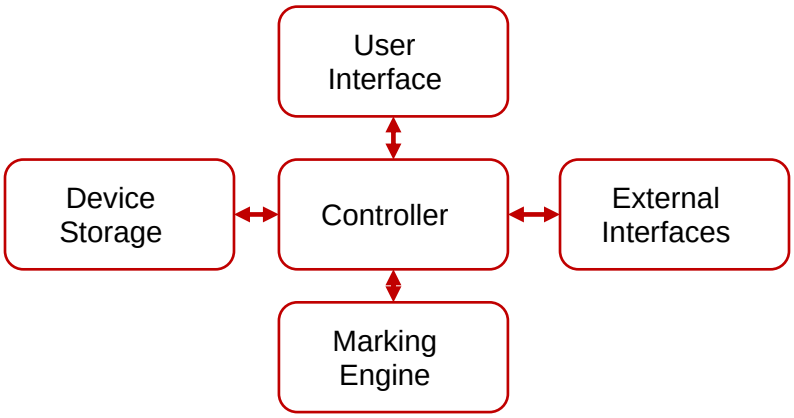
C410



1. Standard Output Tray
2. Control Panel
3. Standard 250-sheet Tray
4. Optional Feeder Tray
5. Manual Feeder

ARCHITECTURE

The 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), to distinguish it from the remote web server interface, also known as Embedded Web Server (EWS).

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

MARKING ENGINE

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

CONTROLLER

The controller manages document processing using proprietary hardware and algorithms to process documents into high-quality electronic and/or printed reproductions. Documents may be temporarily buffered in RAM during processing. An optional hard drive is available on these products. For model specific details please see Appendix A: Product Security Profiles.

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

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

Controller External Interfaces

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

One USB port may be located on the front of the product, near the user interface. Access to the front USB ports may be restricted based on user access. The front USB port can be fully disabled by a system administrator on these products. The front USB port supports the following:

- Walk-up users may insert a USB thumb drive to retrieve documents for printing from a FAT formatted USB device. The controller will only allow reading/printing of a limited set of known document types (such as, PDF, PNG, JPEG, TIFF, etc.). Other file types including binary executables are not supported.
- Connection of optional equipment such as a human interface device (HID).
- Access can be permitted or restricted based on a defined schedule.
- Firmware updates may be submitted through the USB ports. Note that the product can be configured to restrict local firmware updates based on user access control settings.

INTERNAL NETWORK CONNECTIONS

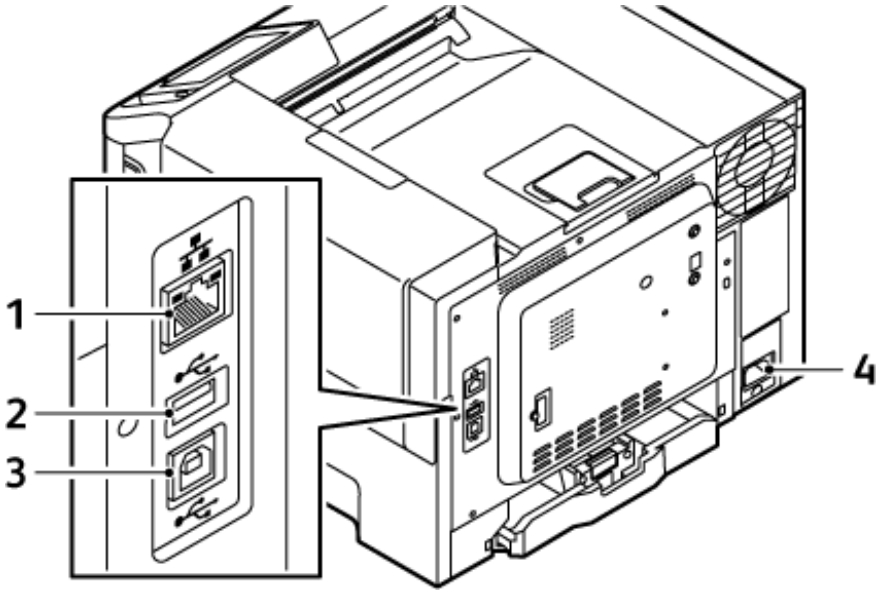
	B410 / C410 Supported
Standard 10/100/1000 Ethernet	Yes
Optional Wireless Adapter Kit 802.11b/g/n/ac	Yes

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 a USB target connector used for printing and connecting a PC.

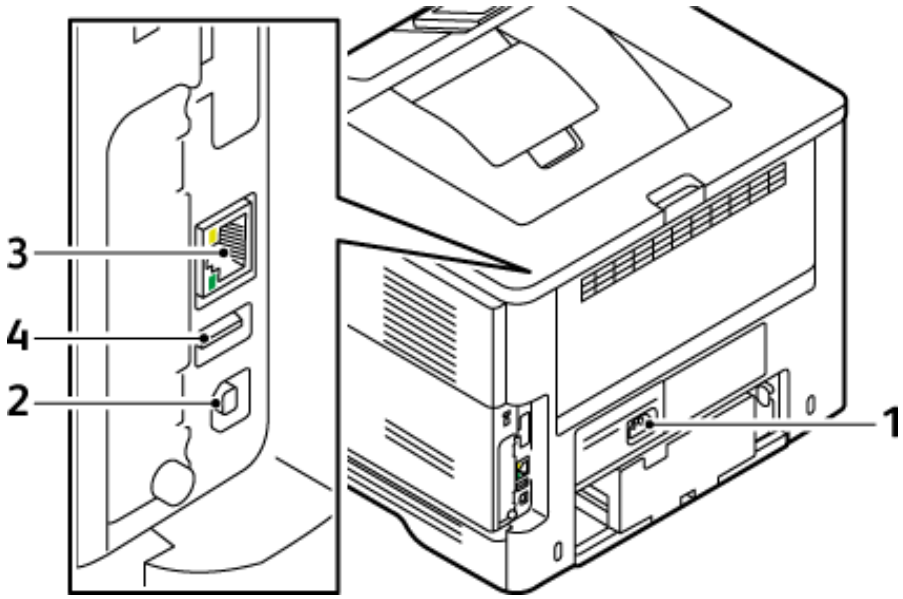
> **Note:** This port is also used for service Diagnostics and cannot be disabled by a system administrator.

B410



1. Ethernet Port
2. USB Port (thumb drive, keyboard, card readers)
3. USB Printer Port (PC connections)
4. Power Cord Socket

C410



1. Power Cord Socket
2. USB Printer Port (PC connections)
3. Ethernet Port
4. USB Port (thumb drive, keyboard, card readers)

3. User Data Protection

Xerox® Printers receive, process, and may optionally store user data from several sources including local print. All user data is temporarily stored in DRAM.

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.

Statement of Volatility

Your printer contains various types of memory that can store device and network settings, and user data.

Type of Memory	Description
Volatile memory	The printer uses standard random-access memory (RAM) to buffer temporarily user data during simple print jobs.
Non-volatile memory	The printer may use two forms of non-volatile memory: EEPROM and NAND (flash memory). Both types store the operating system, printer settings, and network information.
Hard disk storage drive	Some printers may have a hard disk drive installed. The printer hard disk is designed for printer-specific functionality. The hard disk lets the printer retain buffered user data from complex print jobs, form data, and font data.

NON-VOLATILE MEMORY WIPE

A non-volatile memory wipe erases a printer's- memory. volatile memory—EEPROM and NAND. These components store the device operating system, device settings and network information. No user-related print is stored in non-volatile memory.

You can completely clear all printer, network, and shortcut settings on the device. This function is ideal when retiring, recycling, or removing a device from a secure environment.

NOTE: After all settings are removed or reset, network connectivity cannot be retained because the device is in the out-of-box shipping state. You are prompted to select either restarting the device with the out-of-box install wizard or leaving the printer in an offline state. There is no network connectivity until the device is restarted to ensure that the original ship configuration is maintained.

User Data in Transit

This section focuses on the protection of user data 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.

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

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. **Management Services** SNMP, Web interface, Web Services, etc. **Infrastructure and Discovery Services** IPsec, , mDNS, Bonjour, etc.	**Authentication Services** LDAP & LDAPS, SMB, Kerberos **Infrastructure** IPsec, DHCP and DHCPv6, SMTP, 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. Some ports can be configured to different value for some features/protocols.

Port	Type	Service Name
80	TCP	HTTP
443	TCP	HTTPS
137	UDP	WINS
161	UDP	SNMP
162	UDP	SNMP TRAP
515	TCP	LPR/LPD
631	TCP	IPP
5353	UDP	mDNS

Port	Type	Service Name
9100	TCP	Raw IP (JetDirect, AppSocket, PDL Datastream)
9300	UDP	Remote Management
9301	UDP	Remote Management
9302	UDP	Remote Management
9400	TCP	Enhanced Print Port
9500	TCP	Remote Management
9501	TCP	Remote Management
3702	UDP	WS-Discovery
65001	TCP	WS-Discovery
65003	TCP	WS-Eventing

Network Encryption

IPSEC

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

	Xerox® B410 and C410 Printers
IPsec	
Supported IP Versions	IPv4, IPv6
Key exchange authentication method	Preshared Key & digital signature authentication (device authentication certificate, server validation certificate)
ESP Encryption Method	3DES, AES
ESP Authentication Methods	SHA1, SHA256, SHA512

WIRELESS 802.11 WI-FI PROTECTED ACCESS (WPA)

Products equipped with WiFi support WPA2, WPA2/WPA, WPA3, and WPA3/WPA2 Personal Modes and WPA+, WPA2, WPA2+ PMF Enterprise 802.1X Wireless Security modes compliant with IEEE 802.11i. The wireless network adapters used in Xerox products are certified by the Wi-Fi Alliance.

	Xerox® B410 and C410 Printers
Wi-Fi (802.11)	

	Xerox® B410 and C410 Printers
No Encryption	Supported
WPA2, WPA3 Personal (PSK)	AES
WPA2, WPA2+PMFEnterprise	EAP-MD5
	EAP-MS-CHAPv2
	LEAP
	PEAP
	EAP-TLS
	EAP-TTLS-CHAP
	EAP-TTLS-MSCHAP
	EAP-TTLS-MSCHAPv2
	EAP-TTLS-PAP

TLS

These products support TLS 1.0, TLS 1.1, TLS 1.2, and TLS1.3.
TLS 1.0, TLS 1.1, and TLS1.2 can be independently disabled via the EWS.
TLS 1.3 is always supported and cannot be disabled.

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

	Xerox® B410 and C410 Printers
TLS	
TLS Versions	TLS 1.3 (default) TLS 1.0, TLS 1.1, and TLS 1.2 TLS 1.1, TLS 1.1, and TLS1.2 can be independently turned off

SNMPV3

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

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

NOTE: SHA1 is deprecated and considered insecure. Xerox recommends using SHA256 and above.

	Xerox® B410 and C410 Printers
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

These products support both CA signed and self-signed device certificates. The products can accept certificates with a bit length of up to 4096 bits.

The device has a self-generated default device certificate by which the device can be uniquely identified. Device generated certificates use SHA256/RSA2048, however the products can accept certificates for lower/higher key/hash lengths.

	Xerox® B410 and C410 Printers
Device Certificates	
Certificate Length	Up to 4096 (for RSA certificates)
Default Device Certificate	SHA256/RSA2048
Supported Hashes	SHA256, SHA512
Product Web Server	Supported
IPPS Printing	Supported
802.1X Client	Supported
IPsec	Supported
SFTP	Not 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.

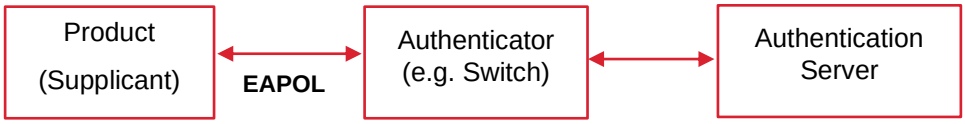
NOTE: SHA1 is deprecated and considered insecure. Xerox recommends using SHA256 and above.

	Xerox® C410 and B410 Printers
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
802.1X Client	Supported
Email Signing	Not Supported
Email Encryption	Not Supported
Email (STARTLS)	Not Supported
OCSP Signing	Not Supported

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® B410 and C410 Printers
Network Access Control	
802.1x	Supported
Authentication Methods	LEAP, PEAP, EAP-MD5, EAP-MSCHAPv2, EAP-TLS, EAP-TTLS (with the following authentication methods: CHAP, MSCHAP, MSCHAPv2, PAP)

CISCO IDENTITY SERVICES ENGINE (ISE)

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

Cisco ISE Profiling Services provides dynamic detection and classification of endpoints connected to the network. ISE collects various attributes for each network endpoint to build an endpoint database. The classification process matches the collected attributes to prebuilt or user-defined conditions, which are then correlated to an extensive library of product profiles. These profiles include a wide range of product types, including tablets, smartphones, cameras, desktop operating systems (for example, Windows®, Mac OS® X, Linux® and others), and workgroup systems such as Xerox printers and 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® B410 and C410 Printers
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 these 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

The products leverage a FIPS 140-2 (Level 1) compliant cryptographic module used for user space cryptographic functions including key management, hashing, symmetric and asymmetric cryptography.

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.

These devices can be configured to allow TCP/IP connections only from a specified list of TCP/IP addresses. This blocks all TCP connections from other addresses, protecting the device against unauthorized printing and configuration. These devices support TCP connection filtering with the Restricted Server List field. By using this option, the device can accept only previously specified TCP/IP connections and rejects all others.

The restricted server list allows up to 50 IP addresses or subnets to be specified. The device responds normally to any address in the list and rejects TCP connections to any address that is not on the list. The products can be further configured to restrict the allowed IP Addresses to Block All Ports, Block Printing Only, or Block Printing and HTTP Only.

The restricted server list does not affect UDP traffic, and so connectionless interactions, such as ping, are allowed from any address.

PERSONAL IDENTIFIABLE INFORMATION (PII)

Personal Identifiable Information (PII) can be entered or stored into the device through several means: address book, bookmarks, device description, display device information, and engineering logs. The PII is stored in Non-Volatile memory, and it is not readable outside of the operation of the device.

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

These 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 these products cannot be accessed by users. Unlike devices such as desktop and laptop computers that have BIOS that can be accessed via a keystroke on startup, the BIOS of these 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, these 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 using 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 securely.

Boot Process Security

TRUSTED BOOT

The chain-of-trust process on these products to check the operating system during startup, normal operation and execution of an internal application is defined in the following list. If any of the following tests fail, the device halts operation of all processes and reports an error.

- The device's physical hardware is used to verify the signature on the kernel.
- The kernel is then used to verify the signatures on each firmware flash partition before it is mounted by the device.
- Internal device drivers and executable code are designed to be operated on trusted read-only flash partitions.
- Each time a block is paged from the trusted flash memory to RAM, its hash value is verified by the kernel, which provides continuous verification and tamper detection.

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. These products include 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.

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.
- **TPM Firmware Updates:**
  The firmware can be updated for the TPM chip.

For additional information on Firmware updates and various upgrade methods supported, please see the System Administrator Guide.

Event Monitoring and Logging

AUDIT LOG

These products support Audit Logging.

Operational Security

IMPORT/EXPORT CONFIGURATION

Certain system settings can be captured in a configuration file. Configuration files are not encrypted and have the potential to contain sensitive information depending on which product feature setting is selected. Access to both creating (exporting) and applying (importing) a configuration file can be restricted using user access controls. Configuration files can only be created and applied through the Embedded Web Server.

RESTORE FACTORY DEFAULTS

The system can be restored to factory default configuration.

CONFIDENTIAL PRINT

Hold and print jobs securely with a unique PIN.

6. Configuration and Security Policy Management Solutions

Xerox Device Manager and Xerox® CentreWare® Web (available as a free download) centrally manage Xerox Devices. For details, please visit Xerox.com or speak with a Xerox representative.

7. Identification, Authentication, and Authorization

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

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

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

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

PASSWORD POLICY

The following password attributes can be configured:

Password Policy	
Minimum Length	1
Maximum Length	32

All newly sold devices are shipped without an Admin account. The product Install Wizard requests that the user create an Admin account and assign a password as a part of the installation process. This step can be skipped.

NETWORK AUTHENTICATION

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

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

SMART CARD AUTHENTICATION

Smart Card authentication is supported for these products.

Smart Cards	
Common Access Card (CAC)	Supported
PIV/ PIV II	Supported
Gemalto MD	Supported

Authorization (Role-Based Access Controls)

These products offer granular control of user permissions. Users can be assigned to a pre-defined Admin role, or customers may design highly flexible custom permissions (groups).

Permissions are broken into three main categories: Functional Access, Administrative Menus, and Device Management. Security access controls can be disabled in the Administrative Menu category.

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.

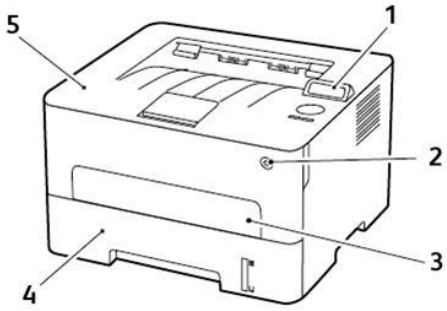
Security Resource	URL
Frequently Asked Security Questions	https://www.xerox.com/en-us/information-security/frequently-asked-questions
Common Criteria Certified Products	https://security.business.xerox.com/en-us/documents/common-criteria/
Current Software Release Quick Lookup Table	https://www.xerox.com/security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

9. Appendix A: Product Security Profiles

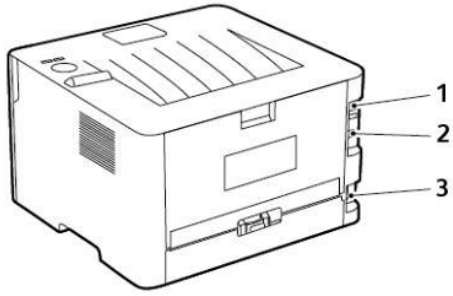
This appendix describes specific details of product.

Xerox® B410 Printer

PHYSICAL OVERVIEW



1. Control Panel
2. Power button
3. Manual Feeder
4. 250–sheet Tray
5. Standard Bin



1. Ethernet port
2. USB printer port
3. Power cord socket

SECURITY RELATED INTERFACES

Security Related Interfaces	
Ethernet	10/100/1000 Base TX Ethernet interface.
Rear USB 3.0 (Type B)	USB target connector used for printing from a PC. Note: This port is used for service Diagnostics and cannot be disabled by a system administrator.
Front USB2.0 (Type A) port(s)	USB target connector used for printing, logs and import configuration settings. Note: Some features that leverage USB ports can be disabled independently based on services in device settings under USB.

CONTROLLER NON-VOLATILE STORAGE

	IC	HDD*	SSD	SD Card
Contains User Data (e.g., Print)	No	Yes	N/A	N/A
Encryption Support (AES-256)	Yes	Yes	Yes	Yes
NIST 800-171 Overwrite Support	N/A	Up to 7 pass erase	eMMC	N/A
Contains Configuration Settings	Yes	Yes	Yes	N/A
Customer Erasable	Erase Printer Memory	Up to 7 pass erase	eMMC	N/A

IC- Integrated Circuit, soldered to circuit board
HDD*- Optional Magnetic Hard Disk Drive
SSD- Solid State Disk
SD Card- Secure Digital Card

CONTROLLER VOLATILE MEMORY

Model	Size	Type	Use	User Data	How to Clear
B410	1 GB	DDR3 DRAM	Executable code, Printer control data, temporary storage of job data	Yes	Power off system

MARKING ENGINE NON-VOLATILE STORAGE

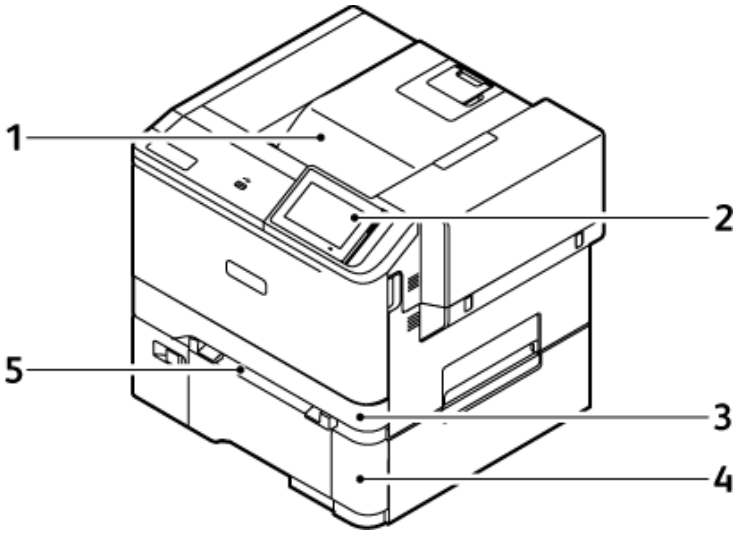
The marking engine does not contain any non-volatile storage.

MARKING ENGINE VOLATILE MEMORY

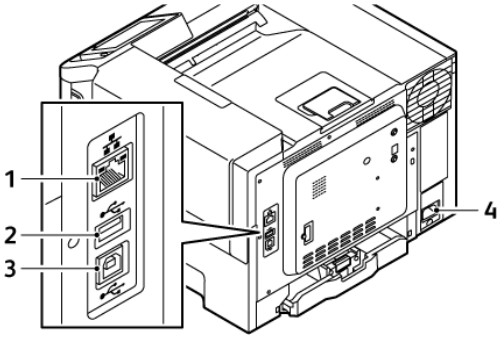
The marking engine volatile memory does not store or process user data.

Xerox® C410 Printer

PHYSICAL OVERVIEW



1. Standard Output Tray
2. Control Panel
3. Standard 250-sheet Tray
4. Optional 550+100-sheet Tray
5. Manual Feeder
6. Optional 650-sheet duo tray
7. Optional 550-sheet tray



1. Ethernet Port
2. USB Port (keyboard, options)
3. USB Printer Port (PC connections)
4. Power Cord Socket

SECURITY RELATED INTERFACES

Security Related Interfaces	
Ethernet	10/100/100 Base TX Ethernet interface.
Rear USB 3.0 (Type B)	USB target connector used for printing. Note: This port is used for service Diagnostics and cannot be disabled by a system administrator.
Front USB2.0 (Type A) port(s)	Users may insert a USB thumb drive to print from files. (Physical security of this information is the responsibility of the user or operator.) Note: Some features that leverage USB ports can be disabled independently based on services in device settings under USB. Firmware upgrades may be applied using this port.

CONTROLLER NON-VOLATILE STORAGE

	IC	HDD*	SSD	SD Card
Contains User Data (e.g., Print)	No	Yes	N/A	N/A
Encryption Support (AES-256)	Yes	Yes	Yes	Yes
NIST 800-171 Overwrite Support	N/A	Up to 7 pass erase	eMMC	N/A
Contains Configuration Settings	Yes	Yes	Yes	N/A
Customer Erasable	Erase Printer Memory	Up to 7 pass erase	eMMC	N/A

IC- Integrated Circuit, soldered to circuit board
HDD*- Optional Magnetic Hard Disk Drive
SSD- Solid State Disk
SD Card- Secure Digital Card

CONTROLLER VOLATILE MEMORY

Model	Size	Type	Use	User Data	How to Clear
C410	1 GB	DDR3 DRAM	Executable code, Printer control data, temporary storage of job data	Yes	Power off system

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.