Xerox®
Security Guide

Entry Production Color Presses

Versant® 2100/3100 Color Digital Press	Versant® 80/180 Color Digital Press	ColorPress® Production Press
Versant 2100 Press, Versant 3100 Press	Versant 80 Press, Versant 180 Press	Color 800/1000 Press Color 800i/1000i Press

Xerox® Security Guide for Entry Production Color Class Products

Document Version: 1.0 (February 2019).

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

Table of Contents

1 Introduction

Purpose

The purpose of this document is to disclose information for the Xerox ® Entry Production Color Presses (hereinafter referred to 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. Furthermore, this document is provided 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 as this information is readily available elsewhere. We assume the reader has a working knowledge of the topics contained within.

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.

Product Description

Physical Components

Versant® products consist of an input document handler and scanner, marking engine, controller, and user interface. ColorPress® products do not have an input document handler or scanner. 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.

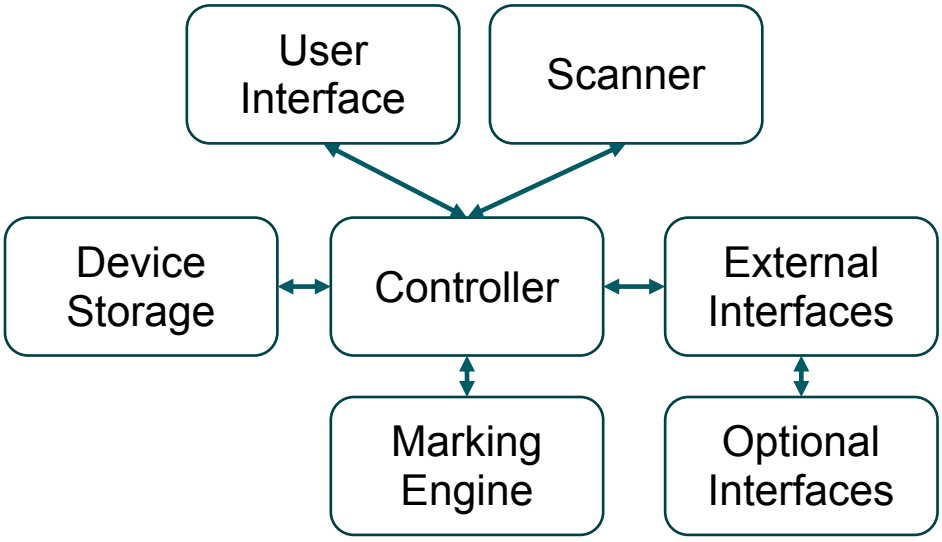
1. HCF.
2. Bypass paper feed tray.
3. Front USB Port(s)*
4. Touch screen user interface.
5. Toner Door Cover.
8. Main Right Front Door.
9. Paper Tray Module
10. Offset Catch Tray

*Denotes a security related component

6. Main Left Front Door.
7. Main Middle Front Door.

Architecture

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



User Interface TRUE FOR VERSANT BUT NOT FOR COLOR PRESS ~~NOTE~~ ~~(~~There is no Scanner on Color Press or Versant 2100/3100)

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 6 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. Versant® and ColorPress® products encrypt user data and include media sanitization (overwrite) options that ensure that erased data cannot be recovered, described further in section 2 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~~(Versant cannot print from USB – not an option. 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 service.

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

Xerox Versant® and ColorPress® products do not offer a wireless connector option.

Near Field Communications (NFC) Reader

The system supports an installable RFID reader for authentication and convenience in certain configurations. Versant® products accept the RFID reader via USB on the front of the product. This communication cannot write or change any settings on the system. The data exchanged is not encrypted and may include information including system network status, IP address and product location. NFC functionality can be disabled using the embedded web server of the product. NFC functionality requires a software plugin that can be obtained from Xerox sales and support. NFC functionality is supported via optional touch screen user interface or optional dedicated NFC USB dongle.

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

SMART CARD – CAC/PIV

All Versant® products support CAC/PIV login by enabling the Versant® Plug-in feature and then enabling the appropriate plug-in. Additional plug-ins can be downloaded from Xerox.com in the Support area online.

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.

2 User Data Protection

Xerox Entry Production Color Presses receive, process, and may optionally store user data from several sources including: local print, scan, ~~fax~~ NO FAX ON VERSANT OR CP1000, 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 on the product is encrypted** by default. Note that encryption may be disabled to enhance performance on both Versant® and ColorPress® products (though this is not recommended in secure environments).

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)

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

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

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

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

User Data in Transit

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

Inbound User Data

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

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

Outbound User Data

Scanning to Network Repository, Email, Fax Server
Versant® digital press products support scanning of hardcopy documents to external network locations including file repositories and email and facsimile services. In addition to supporting network level encryption including IPSec and WPA, Xerox products support the following:

Protocol	Encryption	Description
HTTP	N/A	Unencrypted HTTP protocol
HTTPS (TLS)	TLS	HTTP encrypted by TLS
FTP	N/A	Unencrypted FTP
SFTP (SSH)	SSH	FTP encrypted by SSH
SMBv3	Optional	Encryption may be enabled on a Windows share. Versant® and ColorPress® products 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

Xerox Versant® Color Presses support the Xerox App Gallery® which 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.

		Versant® 80/180 Press **Versant 80 Press, Versant 180 Press**	**Versant® 2100/3100 Press** **Versant 2100 Press, Versant 3100 Press**	**Color 800/100 Press®** **Color 800/1000 Presses, Color 800i/1000i Presses**
Local Data Encryption (HDD, SDD, IC, SD Card)		AES-256	AES-256	AES-256
Federal Information Protection Standard 140-2		Yes	Yes	Yes
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				
	HTTPS (TLS)	1.1/1.2	(Not Applicable)	(Not Applicable)
	SFTP (SSH)	SSH-2	(Not Applicable)	(Not Applicable)
	SMB (unencrypted)	v1, v2, v3	(Not Applicable)	(Not Applicable)
	SMB (with share encryption enabled)	V3	(Not Applicable)	(Not Applicable)
	HTTP (unencrypted)	Supported	(Not Applicable)	(Not Applicable)
	FTP (unencrypted)	Supported	(Not Applicable)	(Not Applicable)
Scan to Fax Server				
	HTTPS (TLS)	1.1/1.2	(Not Applicable)	(Not Applicable)
	SFTP (SSH)	SSH-2	(Not Applicable)	(Not Applicable)
	SMB (unencrypted)	v1, v2, v3	(Not Applicable)	(Not Applicable)
	SMB (with share encryption enabled)	V3	(Not Applicable)	(Not Applicable)
	S/MIME	Supported	(Not Applicable)	(Not Applicable)
	HTTP (unencrypted)	Supported	(Not Applicable)	(Not Applicable)
	FTP (unencrypted)	Supported	(Not Applicable)	(Not Applicable)
	SMTP (unencrypted)	Supported	(Not Applicable)	(Not Applicable)
Scan to Email				
	S/MIME	Supported	(Not Applicable)	(Not Applicable)
	SMTP (unencrypted)	Supported	(Not Applicable)	(Not Applicable)

3 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 & HTTPS (TLS), SFTP (SSH), SMB, CIFS, SMTP & SMTPS, POP3 & POPS, etc. Authentication Services LDAP & LDAPS, SMB, Kerberos. Infrastructure ISAKMP (IPSec), DHCP & DHCPv6, etc. Cloud Services No direct APE to the above.

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
20	TCP	• FTP data (Active) - Client -
21	TCP	• FTP – Client -
25	TCP	• SMTP
53	TCP/UDP	• DNS – Client -
67	UDP	• BOOTP/DHCP – Client
80	TCP	• HTTP(CWIS)
80	TCP	• HTTP(SESAMi Manager)
80	TCP	• HTTP(WebDAV)
88	UDP	• Kerberos – Client -

110	TCP	• POP3 – Client -
123	UDP	• SNTP – Client -
137	UDP	• NETBIOS – Name Service
138	UDP	• NETBIOS – Datagram Service
161	UDP	• SNMP
162	UDP	• SNMP trap
389	TCP	• LDAP – Client -
427	TCP/UDP	• SLP
443	TCP	• HTTP(CWIS)
500	UDP	• ISAKMP
547	UDP	• DHCPv6 – Client
636	TCP	• LDAPS – Client -
995	TCP	• POPS – Client -
1824	TCP	• HTTPS(OffBox Validation) – Client -
1824	TCP	• Xerox Secure Access
1900	UDP	• SSDP
5353	UDP	• Mdns
9100	TCP	• raw IP
15000	TCP	• Loopback port for the control of SMTP server

Network Encryption

IPSec

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

		Versant® 80/180 Press	**Versant® 2100/3100 Press**	**Color 800/100 Press®**
		Versant 80 Press, Versant 180 Press	**Versant 2100 Press, Versant 3100 Press**	**Color 800/1000 Presses, Color 800i/1000i Presses**
IPSec				
	Supported IP Versions	IPv4, IPv6	IPv4, IPv6	IPv4, IPv6
	Key exchange authentication method	Preshared Key & digital signature, device authentication certificate, server validation certificate	Preshared Key & digital signature	Preshared Key & digital signature
	Transport Mode	Transport & Tunnel mode	Transport mode only	Transport mode only
	Security Protocol	ESP & AH	ESP only	ESP only
	ESP Encryption Method	AES, 3DES, Null	AES, 3DES, DES	AES, 3DES, DES
	ESP Authentication Methods	SHA1, SHA256, None	SHA1, SHA256, None	SHA1, SHA256, None

Wireless 802.11 Wi-Fi Protected Access (WPA)

Xerox Versant® and ColorPress® products do not offer a wireless network connector option.

TLS

Versant® and ColorPress® products support the latest version, TLS 1.2.

		Versant® 80/180 Press	Versant® 2100/3100 Press	Color 800/100 Press®
		Versant 80 Press, Versant 180 Press	Versant 2100 Press, Versant 3100 Press	Color 800/1000 Presses, Color 800i/1000i Presses
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
	Remote control	1.2	1.2	1.2

Public Key Encryption (PKI)

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

A digital certificate includes the following data:

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

There are four types of certificates:

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

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

Device Certificates

Versant® and ColorPress® 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.

		Versant® 80/180 Press	**Versant® 2100/3100 Press**	**Color 800/100 Press®**
		Versant 80 Press, Versant 180 Press	**Versant 2100 Press, Versant 3100 Press**	**Color 800/1000 Presses, Color 800i/1000i Presses**
Device Certificates				
	Certificate Length	1024, 2048	1024, 2048	1024, 2048
	Supported Hashes	SHA1, SHA256	SHA256, SHA384, SHA512	SHA256, SHA384, SHA512
	Product Web Server	Supported	Supported	Supported
	IPPS (TLS) Printing	Supported	Supported	Supported
	802.1X Client	Supported	Supported	Supported
	Email Signing	Supported	(Not Applicable)	(Not Applicable)
	Email Encryption	Supported	(Not Applicable)	(Not Applicable)
	OCSP Signing	Supported	Supported	Supported
	IPSec	Supported	Supported	Supported

	SFTP	Supported	(Not Applicable)	(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:

• Trusted Root CA Certificate -Certificates 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.

• Intermediate CA Certificate - Certificates that link a certificate to a Trusted Root CA Certificate in certain network environments.

• Other Certificates- 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 containing 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.

		Versant® 80/180 Press	**Versant® 2100/3100 Press**	**Color 800/100 Press®**
		Versant 80 Press, Versant 180 Press	**Versant 2100 Press, Versant 3100 Press**	**Color 800/1000 Presses, Color 800i/1000i Presses**
Trusted Certificates				
	Minimum Length Restriction Options	None, 1024, 2048	1024, 2048	1024, 2048
	Maximum Length	4096	4096	4096
	Supported Hashes	SHA1/224/256/384/512	SHA1/224/256/384/512	SHA1/224/256/384/512
	Supported Formats	.cer, .crt, .der, .pem, PKCS#7 (.p7b), PKCS#12 (.pfx, .p12)	.cer, .der, PKCS#7, PKCS#12 (.pfx, .p12)	.cer, .der, PKCS#7, PKCS#12 (.pfx, .p12)
	IPSec	Supported	Supported	Supported
	LDAP	Supported	Supported	Supported
	Scanning (HTTPS/TLS)	Supported	(Not Applicable)	(Not Applicable)
	Scanning (SFTP/SSH)	Used for audit log transfer	(Not Applicable)	(Not Applicable)
	802.1X Client	Supported	Supported	Supported
	Email Signing	Supported	(Not Applicable)	(Not Applicable)
	Email Encryption	Supported	(Not Applicable)	(Not Applicable)
	OCSP Signing	Supported	Supported	Supported

Certificate Validation
ColorPress® and Versant® 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.

		Versant® 80/180 Press	Versant® 2100/3100 Press	Color 800/100 Press®
		Versant 80 Press, Versant 180 Press	Versant 2100 Press, Versant 3100 Press	Color 800/1000 Presses, Color 800i/1000i Presses
Email S/MIME				
	Versions	v3	(Not Applicable)	(Not Applicable)
	Digest	SHA1, SHA256, SHA384, SHA512	(Not Applicable)	(Not Applicable)
	Encryption	3DES, AES128, AES192, AES256	(Not Applicable)	(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

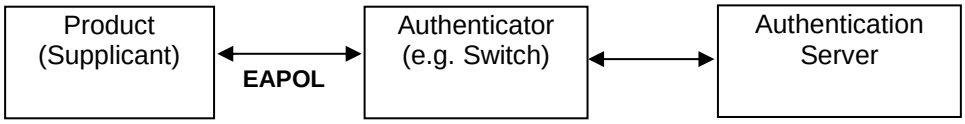
• Encryption of packets to prevent unauthorized access

		Versant® 80/180 Press	Versant® 2100/3100 Press	Color 800/100 Press®
		Versant 80 Press, Versant 180 Press	Versant 2100 Press, Versant 3100 Press	Color 800/1000 Presses, Color 800i/1000i Presses
SNMPv3				
	Digest	(Not Supported)	(Not Supported)	(Not Supported)
	Encryption	(Not Supported)	(Not Supported)	(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.



		Versant® 80/180 Press	Versant® 2100/3100 Press	Color 800/100 Press®
		Versant 80 Press, Versant 180 Press	Versant 2100 Press, Versant 3100 Press	Color 800/1000 Presses, Color 800i/1000i Presses
Network Access Control				
	802.1x	Supported	Supported	Supported
	Authentication Methods	PSK, AES (CCMP)/TKIP, PEAPv0/MS-CHAPv2, EAP-TLS, EAP-TTLS/PAP, EAP-TTLS/MS-CHAPv2, EAP-TTLS/EAP-TLS	MD5, MS-CHAPv2, PEAP/MS-CHAPv2, EAP-TLS	MD5, MS-CHAPv2, PEAP/MS-CHAPv2, EAP-TLS

Cisco Identity Services Engine (ISE)

Cisco ISE is an intelligent security policy enforcement platform that mitigates security risks by providing a complete view of which users and what products are being connected across the entire network infrastructure. It also provides control over what users can access on 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 Versant®, 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. For instance, 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

		Versant® 80/180 Press	**Versant® 2100/3100 Press**	**Color 800/100 Press®**
		Versant 80 Press, Versant 180 Press	**Versant 2100 Press, Versant 3100 Press**	**Color 800/1000 Presses, Color 800i/1000i Presses**
Network Access Control				
	Cisco ISE	Supported	Supported	(Not 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 Versant® and ColorPress® 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.

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

Versant® products use encryption algorithms for Kerberos, SMB, and PDF Direct Print Service that are not approved by FIPS140-2. They can however operate in FIPS140-2 approved Mode in order to maintain compatibility with conventional products after an exception is approved by a system administrator. They do not use FIPS compliant algorithms when in this configuration.

Additional Network Security Controls

Additional network security controls are discussed in the following sections.

Endpoint Firewall Options

		Versant® 80/180 Press	**Versant® 2100/3100 Press**	**Color 800/100 Press®**
		Versant 80 Press, Versant 180 Press	**Versant 2100 Press, Versant 3100 Press**	**Color 800/1000 Presses, Color 800i/1000i Presses**
Firewall		Stateful Packet Filter	IP Whitelisting	IP Whitelisting
	Stateful Firewall	Supported	Supported	Supported

	IP Whitelist	Supported	Supported	Supported

IP Whitelisting (IP Address Filtering)
Versant® products support IP Whitelisting only.

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

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

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

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

Pre-Boot BIOS Protection

BIOS

- The BIOS is inaccessible and cannot be cleared or reset.
- The BIOS can only be modified by a firmware update, which is digitally signed.
- BIOS will fail secure, locking the system if integrity is compromised.

Embedded Encryption

- Configuration Settings (including security settings) and User Data are encrypted by AES.
- Each device is encrypted using its own unique key.

Boot Process Integrity

Firmware Integrity & Verification

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

Event Monitoring & Logging

- The Audit Log feature records security-related events.

Continuous Operational Security

Firmware and Diagnostic Security Controls

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

Fail Secure Vs Fail Safe

Versant® and ColorPress® products are designed to fail secure.

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

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

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

Pre-Boot Security

BIOS

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

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

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

Embedded Encryption

AES encryption is used to protect the system, user data, and configuration (including security settings) from being retrieved or modified. Each device uses its own unique key that is securely generated. Encryption is enabled by default. Media encryption and sanitization are discussed in Section 2 User Data Protection.

Boot Process Security

Firmware Integrity

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

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

ColorPress® and Versant® 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.

Event Monitoring & Logging

Audit Log

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

Field	Description
Index	A unique value that identifies the event.
Date	The date that the event happened in mm/dd/yy format.

Time	The time that the event happened in hh:mm:ss format.
ID	The type of event. The number corresponds to a unique description.
Description	An abbreviated description of the type of event.
Additional Details	Columns 6–10 list other information about the event, such as: 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.

A maximum of 15,000 events can be stored on the device. When the number of events exceeds 15,000, audit log events will be deleted in order of timestamp, and then new events will be recorded. The audit log be exported at any time by a user with administrative privileges. Note that as a security precaution, audit log settings and data can only be accessed via HTTPS.

Operational Security

Firmware Restrictions

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

- Local Firmware Upgrade via USB port:

Xerox service technicians can update product firmware using a USB port on the PC UI. This ability is restricted to CSE installation only.

Additional Service Details

Xerox products are serviced by a tool referred to as the Portable 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.

Backup & Restore (Cloning)

Certain system settings can be captured in a ‘clone’ file that may be applied to other systems of the same model. Clone files are encoded but not encrypted and have the potential to contain sensitive information depending on which product feature setting is selected. Access to both create and apply a clone file can be restricted using role-based access controls. Clone files can only be created and applied through the Embedded Web Server.

EIP Applications

Xerox products can offer additional functionality through the Xerox Extensible Interface Platform (EIP). Third party vendors can create Apps that extend the functionality of a product. Xerox signs EIP applications that are developed by Xerox or Xerox partners. Products can be configured to prevent installation of unauthorized EIP applications. The Versant® supports EIP applications. ColorPress® does not support EIP.

5 Configuration & 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.

6 Identification, Authentication, and Authorization

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

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

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

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

Authentication

ColorPress® and Versant® devices support the following authentication modes:

- Local Authentication
- Network Authentication
- Smart Card Authentication (CAC, PIV, SIPR, .Net)
- Convenience Authentication

Local Authentication

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

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

Password Policy
The following password attributes can be configured:

		Versant® 80/180 Press	**Versant® 2100/3100 Press**	**Color 800/100 Press®**
		Versant 80 Press, Versant 180 Press	**Versant 2100 Press, Versant 3100 Press**	**Color 800/1000 Presses, Color 800i/1000i Presses**
Password Policy				
	Minimum Length	1	1	1
	Maximum Length	63	63	63
	Password cannot contain User Name	Supported	Supported	Supported
	Password complexity options (in addition to alphabetic characters)	Require a number	Require a number	Require a number

Network Authentication

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

		Versant® 80/180 Press	Versant® 2100/3100 Press	Color 800/100 Press®
		Versant 80 Press, Versant 180 Press	Versant 2100 Press, Versant 3100 Press	Color 800/1000 Presses, Color 800i/1000i Presses
Network Authentication Providers				
	Kerberos (Microsoft Active Directory)	Supported	Supported	Supported
	Kerberos (MIT)	Supported	Supported	Supported
	SMB NTLM Versions Supported	NTLMv2	NTLMv2	NTLMv2
	LDAP Versions Supported	Version 3 (including TLS 1.2)	Version 3 (including TLS 1.2)	Version 3 (including TLS 1.2)

Smart Card Authentication

Two-factor security - Smart Card plus User Name/Password combination, requires optional card reader hardware and software plugin. Authentication is handled by a remote server. Supported remote authentication methods include Kerberos, SMB and LDAP.

Smart Card authentication is considered very secure due to the nature of the Smart Card architecture and potential levels of encryption of data on the card itself.

Support for the SIPR network is provided using the XCP Plug-in architecture and a Smart Card authentication solution created by 90meter under contract for Xerox.

Details regarding 90meter can be found online here: http://www.90meter.com/

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

		Versant® 80/180 Press	Versant® 2100/3100 Press	Color 800/100 Press®
		Versant 80 Press, Versant 180 Press	Versant 2100 Press, Versant 3100 Press	Color 800/1000 Presses, Color 800i/1000i Presses
Smart Cards				
	Common Access Card (CAC)	Supported	Supported	Supported
	PIV / PIV II	Supported	Supported	Supported
	Net (Gemalto .Net v1, Gemalto .Net v2)	Supported	Supported	Supported
	Gemalto MD	(Not Currently Supported)	(Not Currently Supported)	(Not Currently Supported)

Convenience Authentication

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

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

Some examples of third party convenience authentication providers include:

- Pharos print management solutions: https://pharos.com/
- YSoft SafeQ: https://www.ysoft.com/en

Contact your Xerox sales representative for details and other options.

Simple Authentication (non-secure)

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

Authorization (Role Based Access Controls)

ColorPress® and Versant® products offer granular control of user permissions. Users can be assigned to pre-defined roles or customers may design highly flexible custom permissions. A user must be authenticated before being authorized to use the services of the product. Authorization ACLs (Access Control Lists) are stored in the local user database. Authorization privileges (referred to as permissions) can be assigned on a per user or group basis.

Please note that Xerox products are designed to be customizable and support various workflows as well as security needs. User permissions include security-related permissions and non-security related workflow permissions (e.g. walkup user options, copy, scan, paper selection, etc.). Only security-related permissions are discussed here.

Remote Access

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

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

Local Access

Without RBAC permissions defined basic information such as Model, Serial number, Software Version, IP address, and Host Name can be viewed without authentication. This can be disabled by disallowing access to device settings for unauthenticated users or in the absence of authentication.

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.

7 Additional Information & Resources

Security @ Xerox®

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

Responses to Known Vulnerabilities

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

Additional Resources

Below are additional resources.

Security Resource	URL
Frequently Asked Security Questions	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	http://www.xerox.com/security
Bulletins, Advisories, and Security Updates	http://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 of each Versant® and ColorPress® product.

Versant® 80/180

Physical Overview

1. Bypass Tray
2. User Interface
3. Duplex Automatic Document Feeder
4. Offset Catch Tray
5. Dry Ink/Toner Waste Bottle Door
6. Trays 1-3
7. Front Door
8. Dry Ink/Toner Cover

Security Related Interfaces

Ethernet	10/100/1000 MB Ethernet interface.
Rear USB 2.0 (Type A)	USB target connector used for printing.~~xxxx~~Not possible on Versant or CP1000 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	Required	N/A	N/A
Contains User Data (E.g. Print, Scan, Fax)		Yes		
Encryption Support		Configurable		
NIST 800-171 Overwrite Support		Yes		
Contains Configuration Settings		Yes		
Encryption Support		Configurable		
Customer Erasable		On Demand		

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 Non-Volatile Memory

Size	Type	Use	User Modifiable	How to Clear	Volatile
64MB	SDRAM (MCU PWBA)	Temporary storage of variables	N	SRAM is erased when machine is powered off.	Yes
4Gbit	DRAM (SYSTEM MEMORY DIMM)	Temporary storage of program and work area	N	SDRAM is erased when machine is powered off.	Yes
64MB	SDRAM (ESS PWBA)	Temporary storage of program and work area	N	SDRAM is erased when machine is powered off.	Yes
1Gbit	SDRAM (page memory)	Temporary storage of variables	N	SRAM is erased when machine is powered off.	Yes

512MB 1Gbit (64M x 16 bit) x4	SDRAM (page memory) DIMM: IPS PWBA	Temporary storage of variables for IISS	N	SRAM is erased when machine is powered off.	Yes
Additional Information: All memory listed above contains code for execution and configuration information. No user or job data is stored in these locations.					

Controller Volatile Memory

Size	Type	Use	User Modifiable	How to Clear	Volatile
64MB	SDRAM (MCU PWBA)	Temporary storage of variables	N	SRAM is erased when machine is powered off.	Yes
4Gbit	DRAM (SYSTEM MEMORY DIMM)	Temporary storage of program and work area	N	SDRAM is erased when machine is powered off.	Yes
64MB	SDRAM (ESS PWBA)	Temporary storage of program and work area	N	SDRAM is erased when machine is powered off.	Yes
1Gbit	SDRAM (page memory)	Temporary storage of variables	N	SRAM is erased when machine is powered off.	Yes
512MB 1Gbit (64M x 16 bit) x4	SDRAM (page memory) DIMM: IPS PWBA	Temporary storage of variables for IISS	N	SRAM is erased when machine is powered off.	Yes
Additional Information: Additional Information: All memory listed above contains code for execution and configuration information. No user or job data is stored in these locations.					

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.

Versant® 2100/3100

Physical Overview

1. Oversized High Capacity Feeder
2. Bypass Tray
3. Print Engine
4. Control Panel and Touch Screen
5. Dry Ink/Toner Cover
6. Left Front Door
7. Center Front Door
8. Right Front Door
9. Paper Trays 1, 2, and 3
10. Offset Catch Tray

Security Related Interfaces

Ethernet	10/100/1000 MB Ethernet interface.
Optional Wi-Fi Dongle	Supports optional 802.11 Dongle.
Rear USB 2.0 (Type A)	USB target connector used for printing.-Xxxx Not possible on Versant or CP1000 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	Required	N/A	N/A
Contains User Data (E.g. Print, Scan, Fax)		Yes		
Encryption Support		Configurable		
NIST 800-171 Overwrite Support		Yes		
Contains Configuration Settings		Yes		
Encryption Support		Configurable		
Customer Erasable		On Demand		

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 Non-Volatile Memory

Size	Type	Use	User Modifiable	How to Clear	Volatile
8MB	Flash (MCU PWBA)	Permanent storage of program. User image data not stored.	N	Not Customer Clearable	No
2MB	Flash (ESS PWBA)	Permanent storage of program/font data. User image data not stored.	N	Not Customer Clearable	No
16KB	EEPROM (BP PWBA)	Permanent storage of machine setting data. User image data not stored.	N	Not Customer Clearable	No
8MB	Flash (ESS PWBA)	Permanent storage of program. User image data not stored.	N	Not Customer Clearable	No
2GB	SD Card	Billing meters and critical settings	N	Not Customer Clearable	No
1MB	Battery-backed SRAM (NVM PWBA)	Permanent storage of machine setting data/job log data.	N	SRAM is not erased when a main switch is turned off. Not	No

		User image data not stored.		customer alterable.	
512KB	Battery-backed SRAM (ESS PWBA)	Configuration and control set points. User image data not stored.	N	SRAM is not erased when a main switch is turned off. Not customer alterable.	No
512KB	EEPROM	Permanent storage of machine setting data. User image data not stored.	N	Not customer alterable.	No
Additional Information: All memory listed above contains code for execution and configuration information. No user or job data is stored in these locations.					

Controller Volatile Memory

Size	Type	Use	User Modifiable	How to Clear	Volatile
64MB	SDRAM (MCU PWBA)	Temporary storage of variables	N	SRAM is erased when machine is powered off.	Yes
4Gbit	DRAM (SYSTEM MEMORY DIMM)	Temporary storage of program and work area	N	SDRAM is erased when machine is powered off.	Yes
64MB	SDRAM (ESS PWBA)	Temporary storage of program and work area	N	SDRAM is erased when machine is powered off.	Yes
1Gbit	SDRAM (page memory)	Temporary storage of variables	N	SRAM is erased when machine is powered off.	Yes
512MB 1Gbit (64M x 16 bit) x4	SDRAM (page memory) DIMM: IPS PWBA	Temporary storage of variables for IISS	N	SRAM is erased when machine is powered off.	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.					

Size	Type	Use	User Modifiable	How to Clear	Volatile
64MB	SDRAM (MCU PWBA)	Temporary storage of variables	N	SRAM is erased when machine is powered off.	Yes
4Gbit	DRAM (SYSTEM MEMORY DIMM)	Temporary storage of program and work area	N	SDRAM is erased when machine is powered off.	Yes
64MB	SDRAM (ESS PWBA)	Temporary storage of program and work area	N	SDRAM is erased when machine is powered off.	Yes
1Gbit	SDRAM (page memory)	Temporary storage of variables	N	SRAM is erased when machine is powered off.	Yes
Additional Information: All memory listed above contains code for execution and configuration information. No user or job data is stored in these locations.					

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.

ColorPress® 800/1000/800i/1000I

Physical Overview

1. Print Engine Left Side
    a. Upper Left Door
    b. Upper Right Door
    c. Left Front Door
    d. Right Front Door
    e. Trays 1 and 2
2. Print Engine Right Side
    a. Left Front Door
    b. Right Front Door
3. User Interface
4. Optional Offset Catch Tray

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.~~XXXX~~ Cannot print on those printer from USB 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	N/A
Contains User Data (E.g. Print, Scan, Fax)		Yes		
Encryption Support		Configurable		
NIST 800-171 Overwrite Support		Yes		
Contains Configuration Settings		Yes		
Customer Erasable		On Demand		

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
2MB	SDRAM	Contains no user or job specific data. Contains machine specific data (hardware ID, system settings, realtime control parameters, print job control state, performance log information, usage counters)	No	Content can be initialized to factory default values.	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.					

Controller Non-Volatile Memory

Size	Type	Use	User Data	How to Clear	Volatile
4MB	Flash	OS, Boot code, Application code, Program constant data. Contains no user or job specifi512KBc data	No	Content is erased and reloaded when system software is upgraded or reinstalled.	No
512KB	ROM embedded in CPU IC	OS, Boot code, Application code, Program constant data. Contains no user or job specific data	No	Content is erased and reloaded when system	No

				software is upgraded or reinstalled.	
512KB	Flash	OS, Boot code, Application code, Program constant data. Contains no user or job specific data	No	Content cannot be modified in the field.	No
2MB	Battery RAM	Contains no user or job specific data. Contains machine specific data (hardware ID, system settings, realtime control parameters, print job control state, performance log information, usage counters)	No	Content can be initialized to factory default values.	No
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.					

PCUI Non-Volatile Storage

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

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

PCUI Non-Volatile Memory

Size	Type	Use	User Data	How to Clear	Volatile
128K	EPROM	System BIOS	No	Diagnostics	No
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.					

PCUI Volatile Memory

Size	Type	Use	User Data	How to Clear	Volatile
1GB	SDRAM	OS, Boot code, Application code, Program constant data. Contains no user or job specific data. Contains machine specific data (hardware ID, system settings, real-time control parameters, print job control state, performance log information, usage counters). Contains machine specific data (System Admin password, user preferences). May temporarily contain non-image job specific (job name, size, etc)	No	Content can be initialized to factory default values.	Yes
Additional Information: The controller operating system memory manager allocates memory dynamically between OS, running processes, and temporary data which includes jobs in process. When a job is complete, the memory pages in use are freed and reallocated as required by the OS.					

Marking Engine Non-Volatile Storage

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

Marking Engine Volatile Memory

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

Appendix B: Security Events

Xerox Versant® 80/180 Security Events

ID	Event	Description
0x0101	Change of Device Status	Normal cold-booting Normal warm-booting Booting due to forced LOG initialization Booting due to forced HDD initialization Shutdown User operation status Starting/finishing of Image Overwrite operation Result of self test
0x0201	Login/Logout	Login Logout Access denial due to KO authentication failures Detection of unauthorized access
0x0301	Change of Audit Policy	Enabling of audit-log management function Disabling of audit-log management function
0x0401	Job Completion	Print Copy Scan Fax Mailbox Report Flow Service Jobs other than the above
0x0501	Change/view of Device Setting	Change of date & time setting (local time) User registration Change of registered user information Deletion of registered user information Mailbox creation Mailbox deletion Authentication Mode Change Security Setting Change Security Setting View Contract Type Change Geographic Region Change Activation Code Input Job-Related Change Billing Impression Mode Change

0x0601	Access to Data Stored in Device	Certificate registration Certificate deletion Address addition Address deletion Address change Uploading from remote client (Whole address book) Downloading to remote client (Whole address book) Deletion of all addresses Downloading to remote client (Whole address book)
0x0701	Change/Restoration of Device Configuration	Replacement of important parts Detection of HDD replacement Change of ROM version
0x0801	Communication Result	Reliability Communication Error

Xerox Versant® 2100/3100 Security Events

ID	Event	Description
0x0101	Change of Device Status	Normal cold-booting Normal warm-booting Booting due to forced LOG initialization Booting due to forced HDD initialization Shutdown User operation status Starting/finishing of Image Overwrite operation Result of self test
0x0201	Login/Logout	Login Logout Access denial due to KO authentication failures Detection of unauthorized access
0x0301	Change of Audit Policy	Enabling of audit-log management function Disabling of audit-log management function
0x0401	Job Completion	Print Copy Scan Fax Mailbox Report Flow Service Jobs other than the above
0x0501	Change/view of Device Setting	Change of date & time setting (local time) User registration Change of registered user information Deletion of registered user information Mailbox creation Mailbox deletion Authentication Mode Change Security Setting Change Security Setting View Contract Type Change Geographic Region Change Activation Code Input Job-Related Change Billing Impression Mode Change
0x0601	Access to Data Stored in Device	Certificate registration Certificate deletion Address addition Address deletion Address change Uploading from remote client (Whole address book) Downloading to remote client (Whole address book) Deletion of all addresses Downloading to remote client (Whole address book)

0x0701	Change/Restoration of Device Configuration	Replacement of important parts Detection of HDD replacement Change of ROM version
0x0801	Communication Result	Reliability Communication Error

ColorPress® Security Events

ColorPress utilizes Windows Event Logging which is outside the scope of this document.