Secure Installation and Operations Guide

Xerox® VersaLink® C415/C625/B415/B625 Multifunction Printer

Version 2.0 (February 2025)

Document Version: 1.3 (April 2024).

Contents

1. Introduction

Purpose

This document provides information on the secure installation, setup and operation. All customers, but particularly those concerned with secure installation and operation of these devices, should follow these guidelines.

Overview

This document lists some important customer information and guidelines[1] that will ensure that your device is operated and maintained in a secure manner.

Background

These products are evaluated as part of Common Criteria certification in a particular configuration, referred to in the rest of this document as the "evaluated configuration". The Initial section describes how to install and configure the machine so that it is in the same configuration as it is for evaluation.

Customers are advised that changes to the evaluated configuration may be required to support business goals and for compliance with policies applicable to their environment[2] . After careful review of this document, customers should document settings to be applied to devices in their environment establishing a unique benchmark configuration to support processes such as installation, change management and audit. Xerox Professional Services, which can be contacted via https://www.xerox.com/about-xerox/customer-training/tab1-ab-enus.html, can assist in evaluating and configuring these devices.

The information provided here is consistent with the security functional claims made in the applicable Security Targets[3]. When Common Criteria certification of these products is completed, the Security Targets will be available from the Common Criteria Certified Product website (https://www.commoncriteriaportal.org/products.html) list of evaluated products, from the Xerox security website (https://www.xerox.com/information-security/common-criteria-certified/enus.html), or from your Xerox representative.

It should be noted that throughout the rest of this document the terms "system administrator" or "administrator" are used to refer to the U.ADMIN role specified in the applicable Security Targets and in the Hardcopy Device Protection Profile[4] while the terms "user" or "users" are used to refer to the U.NORMAL role in the Hardcopy Device Protection Profile.

---

[1] All guidelines in this document apply to the System Administrator unless explicitly stated otherwise.

[2] For example, if the customer security policy requires that passwords are reset on a quarterly basis, the Reset Policy for the Admin Password will need to be enabled. Also, many customers choose to manage user credentials centrally, rather than on individual devices through local authorization.

[3] Xerox Multi-Function Device Security Target, Xerox® VersaLink™ C415 / B415 with eMMC version 0.2; Xerox Multi-Function Device Security Target, Xerox® VersaLink™ C415 / B415 with HDD, Xerox Multi-Function Device Security Target, Xerox® VersaLink™ C625 / B625 with eMMC version 0.2; Xerox Multi-Function Device Security Target, Xerox® VersaLink™ C625 / B625 with HDD version 0.2;

[4] Protection Profile for Hardcopy Devices IPA, NIAP, and the MFP Technical Community, Version 1.0, September 10, 2015

2. Evaluation Configuration Description

The TOE is an MFD (Xerox® Versalink™ C415 / B415 / C625 / B625) with eMMC and HDD that consists of a printer, copier, scanner, fax, and associated administrator and user guidance. The Evaluated Configuration comprises the hardware, and all software and firmware within the MFD enclosure. Xerox® Versalink® B415 / B625 are mono MFP or black and white printers; C415/C625 are color MFP or color printers. All models have an ARM Cortex A53 processor and run Yocto Linux 3.1.2. Each model consists of an input document handler and scanner, Xerox embedded Fax accessories, marking engine, controller, Xerox Workflow scanning accessory, and user interface. Differences between models is limited to print speed and options such as finishers, paper trays and document handlers. The differences between the models are not security relevant.

The Xerox MFP's within the scope of the evaluation are shown in the table below.

XEROX MFP's

Model	Firmware Version
Versalink™ C415	119.028.003.11705
Versalink™ B415	119.029.003.11705
VersaLink™ C625	119.024.003.11705

The administrator and user guidance included in the Evaluated Configuration are listed in Table below.

SYSTEM USER AND ADMINISTRATOR GUIDANCE

Title	Version	Date
Xerox® B415 Multifunction Printer User Guide, v1.1, September 2023 (702P09164)	1.1	September 2023
Xerox® C415 Color Multifunction Printer User Guide, v1.1, September 2023 (702P09149)	1.1	September 2023
Xerox® VersaLink® B625 Multifunction Printer User Guide (702P09148)	1.2	September 2023
Xerox® VersaLink® C625 Color Multifunction Printer User Guide (702P09147)	1.1	September 2023
Xerox® VersaLink® C620/B620 Single Function and VersaLink® C625/B625/C415/B415 Multifunction Printers System Administrator Guide (702P09150)	1.2	September 2023
Smart Card Installation and Configuration Guide for Xerox®, AltaLink® / VersaLink® Series Version 1.0 March 25, 2024	1.0	March 2024

3. Secure Installation and Set-up in the Evaluated Configuration

To set up the machines in the evaluated configuration, follow the guidelines below:

A. Set up and configure the following security protocols and functions in the evaluated configuration:
   - Immediate Overwrite and Scheduled
   - Enable FIPS with Common criteria (CC) compliance
   - IP Filtering
   - Audit Log
   - Security Certificates, Transport Layer Security (TLS) and HTTPS
   - IPsec
   - Local, Remote or Smart Card Authentication
   - Local or Remote Authorization
   - User Permissions
   - Personalization
   - 802.1x Device Authentication
   - Session Inactivity Timeout
   - USB Port Security
   - SFTP Filing (only for transfer of the audit log to an audit log server)
   - Embedded Fax Secure Receive
   - Secure Print
   - Hold All Jobs
   - Erase Customer Data

System Administrator authentication is required when accessing the security features and administrative functions of the device or when implementing the guidelines and recommendations specified in this document. To log in as an authenticated System Administrator via the Embedded Web Server (EWS)[5] , follow the instructions under “Accessing the Embedded Web Server” in the Getting Started section of Xerox® VersaLink® C625 and C415 Color Multifunction Printers Xerox® VersaLink® B625 and B415 Multifunction Printers System Administrator Guide (SAG)

To log in as an authenticated System Administrator via the Local User Interface (denoted hereafter in this document as the Control Panel), follow “Accessing the Control Panel as a System Administrator” under “Accessing Administration and Configuration Settings” in the Xerox® VersaLink® C625 and C415 Color Multifunction Printers Xerox® VersaLink® B625 and B415 Multifunction Printers System Administrator Guide.

To log in as an authenticated user who is not the System Administrator ‘admin’ user, follow the instructions for “Accessing the Embedded Web Server” under “Accessing Administration and Configuration Settings” in the Getting Started section of the SAG, except that instead of entering ‘admin’ for the User ID and the system administrator password the user should enter his/her User ID and his/her authentication password.

B. Follow the instructions located in the Security section, in the SAG to set up the security functions listed in Item A above. Note that whenever the SAG requires that the System Administrator

[5] The remote interface is referred to in documentation as the either the Embedded Web Server (EWS) or CentreWare Internet Services (CWIS). In this document it will be referred to as the EWS.

provide an IPv4 address, IPv6 address or port number the values should be those that pertain to the device being configured.

Each section below will explain the setup requirements for the device to be in the evaluated configuration.

AUTHENTICATION PASSWORDS

Authentication passwords for unique user accounts established for all users and System Administrators should be set by the System Administrator to a minimum length of 15 alphanumeric characters unless applicable internal procedures the System Administrator must comply with require a minimum password of a greater length (the minimum length can be set to any value between 1 and 63 alphanumeric characters). Authentication passwords should always be strong passwords by using a combination of upper case and lower case letters, digits, and allowable special characters (“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, and other printable ISO 8859-15 set and Unicode/UTF-8 set characters except “>”), not use common names or phrases, etc.

The ‘maximum length’ can be set to any value between 15 and 63 (alphanumeric) characters consistent with the same internal procedures. Follow the instructions for “Specifying User Password and Account Requirements” under “User Database” under “Configuring Local Authentication Settings” in The Security section of the SAG to set both the minimum and maximum user authentication password lengths from the EWS.be disabled on this family of products.

ADMINISTRATOR PASSWORD

Change the Administrator password upon installation. Reset the Administrator password periodically. Change the Administrator password once a month. To change the Administrator password from the EWS, follow the instructions under “Changing the System Administrator Password” in the Initial Setup section of the SAG.
To change the Administrator password from the Control Panel, follow the instructions under “Changing the Administrator Password at the Control Panel” in the Initial Setup section of the SAG.
Disable the Admin Password Reset security feature so it is not used. To disable this feature from the EWS, follow the instructions under “Disabling the Administrator Password Reset” in The Security section of the SAG.

AUTHENTICATION FAILURE HANDLING

When five successive authentication attempts are made using either the Control Panel or EWS, the device will lockout the user or system administrator for a configurable time-period, the default is 5 minutes. After the configure lockout period has elapsed, the user or system administrator will be able to attempt another authentication attempt.

When the Control Panel or LUI is locked down after 5 unsuccessful authentication attempts, no user will be able to login at the LUI until the configured lockout period has elapses, users other than the user that cause the lockout can login to EWS while the control panel is on lockout.

The number of successive authentication attempts failure before the user is locked out is not configurable in the TOE.

To configure the 5-minute lockout period, in EWS, as a System Administrator, perform the following:

1. Click Properties, Security, Device Account Requirements
2. Set the User Lockout period. The default value is 5 Minutes

ESTABLISHING A REMOTE SESSION

To establish a remote session with the device via EWS, any user (whether a System Administrator or non-admin) must perform the following:

1. Locate your device IP address using the Configuration Report.
   Note: The device prints a Configuration Report at power-up. Otherwise, you can print a Configuration Report by performing the following on the device LUI:
   - Touch Device, then touch Information Pages.
   - Touch Configuration Report, then touch Print.
2. Ensure that TCP/IP and HTTP are enabled. If you disabled either of the protocols, at the Control Panel, re-enable the protocols.
3. At your computer, open a Web browser. In the address field, type the IP address of the device, then press Enter or Return.
   Note: To ensure that untrusted-certificate Web browser errors do not appear, install the Device Root Certificate Authority for the device. See “Installing the Device Root Certificate Authority” under “Security Certificates” in The Security section of the SAG
4. In the top right area of the page, click Login.
5. Type in the user’s User ID and password in the appropriate field.
6. Click Log

AUTHENTICATION

Establish local authentication at the device via either the Control Panel or EWS by following the “Configuring Local Authentication Settings” instructions in the Security section of the SAG.

Set up unique user accounts with appropriate credentials (user names and passwords) on the device for all users who require access to the device via the Control Panel or EWS by following instructions in the Security section of the SAG.

Configure network (remote) authentication access to network accounts from either the Control Panel or EWS by performing the following:

Configuring Network Authentication Settings

To configure access rights using network authentication:

Set the login method to User Name / Password - Validate on the Network. To set the Login Method for the EWS perform the following:

1. In the Embedded Web Server, click Properties→Login/Permissions/Accounting.
2. Click Login Methods.
3. For Control Panel & Website Login Methods, click Edit.
4. For Website Login, select an option.

   Note: Website Login is only available when the following authentication method is enabled for the control panel:

   • Smart Cards

5. Click Save.

CONFIGURING AUTHENTICATION SERVER SETTINGS FOR LDAP ON THE EWS

The device uses an LDAP server for authentication, authorization, and personalization. The LDAP server appears in the EWS on the LDAP Server page.
Select LDAP as the network authentication method and authorization method. The device will use this server automatically. Then follow the directions under "Configuring Authentication Server Settings for LDAP" under "Configuring Network Authentication Settings" in the Security section of the SAG.
After you click Apply, perform the following:

1. Enable TLS.
2. Follow the directions for "Adding LDAP Server Information" and for "Managing LDAP Servers in the Embedded Web Server" under "LDAP" of the SAG.
3. Follow the directions "To use LDAPS, for Secure LDAP Connection" in Item 6. under "Configuring LDAP Server Optional Information" under "LDAP" of the SAG.
4. To configure a secure LDAP connection, follow the instructions for "Configuring a Secure LDAP Connection" under "LDAP" of the SAG.

   Note: The LDAP Server must have encryption enabled, ensure that a certificate issued from the LDAP server certificate authority is installed on the device.

CONFIGURING SMARTCARD AUTHENTICATION SETTINGS ON THE EWS

Establish user authentication via a Smart Card and smart card reader by following the "Configuring Smart Card Authentication Settings" instructions in the Security section of the SAG. Note that smart card authentication is done at the device and may require inputs at the Control Panel.

Note that there are two other authentication methods available on the device – Xerox Secure Access and Convenience Authentication. Neither of these two authentication methods is allowable as part of the evaluated configuration. Note also that proximity cards are only supported by Xerox Secure Access and Convenience Authentication, so proximity cards are also not part of the evaluated configuration.

AUTHORIZATION

Either local authorization or network authorization using LDAP is allowed in the evaluated configuration.

When new user accounts are created, they are assigned user roles, and when new objects are created, users are granted access based on their roles. If the user role is changed while the user is logged in, the change will take effect at the users next login.

Only a System administrator can manage security attributes with roles and access permissions. System Administrators can set users specific security attributes in relation to the roles that user obtains. Non-administrative users can only change their own password and do not have access to the Properties setting to manage any other user security attributes or any other functions.

LOCAL AUTHORIZATION

- Establish local authorization at the device using the Control Panel by following the "Configuring Local Authorization Settings" instructions under the "Setting the Authorization Method' in the Security section of the SAG. Note that local user accounts on the device should be set up first before user permissions are set up.
- When adding new users, set up user roles and user permissions to access device apps and pathways based on the roles users are assigned to by following the instructions for user permissions in the "Authorization" section in the Security section of the SAG. Follow these same instructions to add/delete

user role, to change the roles users are assigned to or to change what access permissions each role has.

- Set the permission for all Non-Logged In Users Roles via EWS (see “User Roles” in the Security section of the SAG) to be Not Allowed for the following: (1) all print permission categories (by following the “Editing Print Permissions for the Non-Logged In Users Role” under the “User Roles” section under the “User Permissions” section under the “Authorization” section in the Security section of the SAG) and (2) all apps/services and tools (by following the “Editing Apps and Tools Permissions for the Non-Logged In Users Role” under the “User Roles” section under the “User Permissions” section under the “Authorization” section in the Security section of the SAG).

NETWORK AUTHORIZATION

Establish remote authorization via EWS using LDAP by following the “Configuring Network Authorization Settings” and “Configuring Network Authorization Server Settings” instructions in the Security section of the SAG. Make sure to only follow the instructions pertaining to setting up an LDAP Server.

Network Authorization using an SMB server is not part of the evaluated configuration and should not be used.

Ensure that Logged-In Users have access (i.e., permission is Allowed) to the following apps (see “Editing Apps and Tools Permissions for the Non-Logged In Users Role” under “Authorization Settings” in The Security section of the SAG):

- Print From
- Fax
- Workflow Scanning
- Email

PERSONALIZATION

Enable personalization via EWS by following the instructions for “Specifying the Method the Printer Uses to Acquire Email Address of Users” under “Setting Up Authentication for a Smart Card System” in the Security section of the SAG. Configure personalization by following the instructions for “Configuring LDAP User Mappings” under “LDAP” in Network Connectivity section of the SAG.

IMMEDIATE IMAGE OVERWRITE

For devices with the optional HDD kit installed, both Immediate Image Overwrite and On Demand Image Overwrite are enabled by default at the factory when the device is first delivered and cannot be disabled, on the HDD configuration. For the eMMC configuration, Job Data removal is enabled by default at the factory.

SECURITY CERTIFICATES

Install a digital certificate on the device before enabling TLS via EWS by following the appropriate instructions under “Security Certificates” in in The Security section of the SAG for installing any one of the digital certificates (Device Certificate, CA Certificate or Trusted Certificate) the device supports.

Note that a Xerox device certificate signed by the Xerox Generic Root CA is installed by default on the device. If the device uses this certificate, and users attempt to access the device using the Embedded Web Server, an error message could appear in their Web browser. To ensure that error messages do not appear, in the Web browsers of all users, install the Xerox Generic Root CA certificate by following the instructions for “Installing the Device Root Certificate Authority” under “Security Certificates” in The Security section of the SAG.

If a CA certificate is desired, a Certificate Signing Request (CSR) will have to be sent to a Certificate Authority to obtain the CA Certificate before it can be installed on the device; follow the instructions for “Creating a Certificate Signing Request” under “Security Certificates” in in The Security section of the SAG to create the CSR.

The auto-generated Default Xerox Device Certificate will contain a signature algorithm of SHA256/ECDSA of NIST Curve P-384 key size, and an encryption algorithm of ECDSA of NIST Curve P-384 key size.

Note that if a New Xerox Device Certificate is installed on the device, the friendly name automatically assigned by the device for that certificate may not be correct.

TRANSPORT LAYER SECURITY

The following TLS cipher suites are supported in the evaluated configuration:

- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA

Follow the instructions under ‘Enabling DNS Settings the Control Panel’ from the Control Panel or ‘” Configuring DNS” (under “Configuring IP Settings in the Embedded Web Server”) from EWS in The Network Connectivity section of the SAG for entering the host and domain names, to assign the machine a valid, fully qualified machine name and domain (required for TLS to work properly).

If the default device certificate is to be used, download the generic Xerox Root CA certificate from the device by following the instructions using EWS for saving the certificate file under “Viewing, Saving or Deleting a Certificate” in The Security section of the SAG and then installing the saved certificate in the certificate store of the System Administrator's browser.

Enable HTTPS from EWS by following the instructions for “Using TLS for all HTTP Communication (HTTPS)” under “Secure HTTP (TLS)” in The Security section of the SAG. Set the ‘Force Traffic over HTTPS’ option to be Yes.

Note that the device when in FIPS with CC Mode, the device will be configured for TLS 1.2 only.

The device should be configured for SHA-1, SHA-256, and above for the Evaluated Configuration.

To verify, perform the following:

Access the EWS by typing https://{IP Address of the device}.

1. Authenticate as a System Administrator.
2. Select the Properties tab.
3. Select Security > TLS.
4. Observe that the TLS 1.2 only setting is enabled, and that TLS 1.3 is disabled.
5. Ensure that SHA-1, SHA-256 and above is configured.

FIPS 140 MODE

Encryption of transmitted and stored data by the device must meet the FIPS 140-3 Standard. Enable the use of encryption in "FIPS 140 mode" and check for compliance of certificates stored on the device to the FIPS 140-3 Standard via EWS by following the instructions for "Enabling FIPS 140 Mode and Checking for Compliance" in The Security section of the SAG. Make sure to select the 'Enable FIPS with Common Criteria (CC) compliance' option.

Since Kerberos and SFTP are not FIPS compliant secure protocols, make sure when enabling FIPS mode that you set up the proper exceptions for both Kerberos and SFTP. The Evaluated configuration includes the Mocana cryptographic module which it uses to provide cryptographic services. The Security Target document references the certificate numbers for these features. The type of DRBG that is configured by default is AES256 and is not configurable.

DATA ENCRYPTION

Data encryption is enabled by default at the factory and cannot be disabled, the TOE uses AES_CBC_256 by default, no additional cryptographic settings are necessary for data encryption.

IP FILTERING

Enable and configure IP Filtering to create IP Filter rules via EWS by following the instructions under "IP Filtering" in The Security section of the SAG.
Note that IP Filtering will not work if IPv6 is used instead of IPv4.
Note also that a zero ('0') should be used and not an asterisk ('*') if a wildcard is needed for an IP address in an IP Filter rule.

AUDIT LOG

The Audit Log consists of two components – the main audit log and a set of protocol log files (one for each of the four secure protocols – TLS, HTTPS, SSH which SFTP uses and IPsec). Section 7 "Selected Audit Log Entries" in this document shows the selected audit log entries that pertain to the security functions/features discussed in this document.

For each audit log entry in the main audit log a time stamp is included.
The set of multiple protocol log files contain log information pertaining to secure sessions. Specifically, the protocol log files each contain:

- A date/time stamp for each entry
- The remote IP address of the endpoint of the communication session.
- The protocol used for the secure session.
- A status indicating that the secure session was successful or a failure.

- An error indicator (error code or message) indicating the reason for the error - this is the reason for session failure. Note: The specific message or code is an outcome of the various logging technologies used in the system.

The protocol log files are enabled separately by following the instructions for “Enabling Secure Protocol Logs” under “Audit Log” in The Security section of the SAG.

The main audit log is always enabled and cannot be disabled. To download the audit log in a .csv file and then store it in a compressed file on an external IT product using the EWS follow the appropriate instructions for “Saving an Audit Log” under “Audit Log” in The Security section of the SAG.

In downloading or transferring the main Audit Log and log files to a drive or other external trusted IT product, the System Administrator should ensure that Audit Log records are protected after they have been exported to an external trusted IT product and that the exported records are only accessible by authorized individuals.

The actual format of the Audit Log, including time stamps, is indicated in “Interpreting the Audit Log” under “Audit Log” in The Security section of the SAG.

The System Administrator should download and review the main Audit Log and protocol log files on a daily basis.

The main Audit Log can contain up to 15,000 entries. Once the Audit Log is full it will overwrite the oldest event with the new event information, and it will keep logging events this way until the main Audit Log is cleared. The machine will send a warning email when the audit log is filled to 90% (i.e., 13,500) of the 15,000 maximum allowable number of entries and repeated thereafter at 15,000 entries until the Audit Log is downloaded.

The protocol log files can hold up to 10MB worth of data. Just as was the case for the main Audit Log, once a Protocol Log File is full it will overwrite the oldest entries with the new information, and it will keep logging entries this way until the Audit Log is cleared. The machine will send a warning email when a protocol log file is filled to 90% of maximum capacity and will repeat each time it reaches 90% capacity until the Audit Log is downloaded.

The System Administrator should be aware that there is the possibility that on an intermittent basis multiple entries may be included in the audit log for the same event.

The Audit Log can be transferred to an audit log server outside the device by following the directions for “Enabling Automatic Log Transfer” under “Audit Log” in The Security section of the SAG. The only special requirement on the audit log server the Audit Log is to be transferred to is that it must support the SFTP protocol. As was the case for downloading the audit log, when you transfer the audit log you will get both the main audit log and the four protocol log files.

IPSEC

Enable and configure IPsec using the EWS by following the instructions under “IPsec” in The Security section of the SAG. Note that IPsec should be used to secure printing jobs; HTTPS (TLS) should be used to secure scanning jobs. Use the default values for IPsec parameters whenever possible for secure IPsec setup.

To encrypt (PROTECT) a protocol via IPsec, create a security policy[6] as follows:

1. Follow the instructions under “Managing Host Groups” to create a new host group or use a predefined Host Group.
2. Follow the instructions under “Managing Protocol Groups” to create a Protocol Group that includes the protocol(s) that you want to encrypt using IPsec.
3. Follow the instructions under “Managing Actions” to create an IPsec action with the desired parameters.
4. Create a security policy by selecting the Security Policies tab and following the instructions for “Managing Security Policies”. Make sure to select the Host Group and Protocol Group just created and select the action of ‘Encrypt’. Click Add Policy to add this new security policy.
5. Now create a second security policy with the default values for Host Group (‘All’) and Protocol Group (‘All’) and an action of ‘Block’ – that will cause all protocols created to be discarded (blocked), except for in this case the protocols covered by the first rule created that are to be protected and IPsec will encrypt the packets transmitted over the protected protocol.
6. Make sure that the security policy for the protocols (IPsec) for which encryption is desired is the top priority policy (if it is not already) by performing the following:
    a. Under Saved Policies, select the policy you want to move, then click the Promote or Demote buttons.

By default, any packet that does not fit any user defined security policy will pass through unmodified. Therefore, if the second security policy was not created in the above case, for example, any packet that was not for one of the protocols that was to be encrypted would automatically pass through unmodified.

The instructions for “Creating a New Action” under “Managing Actions” under “IPsec” in The Security section of the SAG describe how to set up an IPsec action to use either tunnel or transport mode.

The instructions below for “Configuring Internet Key Exchange Settings” describe how to set the key lifetimes for IKE Phase 1 and Phase 2, the DH Group, the hash algorithm and the encryption algorithm. Note the that maximum key lifetime for both Phase 1 and Phase 2 is 86,400 seconds (24 hours), which is the default value, and the minimum key lifetime is 60 seconds for Phase 1 and 300 seconds for Phase 2.

- In the IKE Phase 1 area, for Key Lifetime, type the length of time until the key expires in Seconds, Minutes, or Hours. When a key reaches this lifetime, the Security Association is renegotiated and the key is regenerated or refreshed.
- In the IKE Phase 2 area, for IPsec Mode, select an option.

    Transport Mode: This option encrypts the IP payload only.

    Tunnel Mode: This option encrypts the IP header and the IP payload.

    Note: Tunnel mode treats the entire IP packet as an Authentication Header (AH) or Encapsulating Security Payload (ESP), which provides protection for the entire packet.
- If you selected Tunnel Mode, for Enable Security End Point Address, select an address type. Options are Disabled, IPv4 Address, or IPv6 Address.
- For IPsec Security, select ESP, AH, or BOTH.
- For Perfect Forward Secrecy (PFS), select an option. Options are Group 20 (EC P-384), Group19 (EC

[6] Note that IPsec security policies are sets of conditions, configuration options, and security settings that enable two systems to agree on how to secure traffic between them. You can have multiple policies active at the same time, however, the scope and policy list order determine the overall policy behavior.

P-256), Group 14 (2048-bit MODP), or None.

- For Hash, select an option. Options are SHA-256, SHA-1, or None.
- If you selected ESP or BOTH for the IPsec Security type, for Encryption, select AES-CBC-128/256 or None.
- For Key Lifetime, type the length of time until the key expires in Seconds, Minutes, or Hours. When a key reaches this lifetime, the Security Association is renegotiated, and the key is regenerated or refreshed.
- Click Save.

The device supports the following for IPsec – IKEv1 protocol with main mode and DH Group 14 (2048-bit MODP), Group 19 (256-bit Random ECP), and Group 20 (384-bit Random ECP)
Pre-shared keys for IPsec are set by following the instructions for "Creating a New Action". Pre-shared keys can be between 1 and 32 alphanumeric characters in length. Pre-shared keys should follow the same general rules as stated for creating strong passwords: 22 characters in length, composed of any combination of upper and lower case letters, numbers, and special characters (that include: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")").

Note that IPsec can be disabled at the Control Panel by following the instructions for "Disabling IPsec at the Control Panel" under "IPsec" in The Security section of the SAG. However, if IPsec is disabled the device will no longer be in the evaluated configuration.

Ensure that an IP Address of 0.0.0.0 is not used to create a new Host Group.

If either ESP or BOTH are selected for the IPsec Security type, AES must be selected as the encryption option.

To configure the device to use AES, use actions to more specifically manage how IPsec controls dependent protocols. Two actions are predefined. You can create custom protocols.
The following actions are predefined:

- **Pass**: This action allows unencrypted traffic.
- **Block**: This action blocks unencrypted traffic.

To create a new action, follow the instructions for "Creating a New Action" under "Managing Actions" under "IPsec" in Chapter 4 of the SAG.
Manual Keying is used when client systems either do not support IKE or are not configured for IKE. To configure manual keying, follow the instructions for "Configuring Manual Keying Settings" under "Managing Actions" under "IPsec" in Chapter 4 of the SAG.
Internet Key Exchange (IKE) is a keying protocol that allows automatic negotiation and authentication, anti-replay services, and CA support. It can also change encryption keys during an IPsec session. IKE is used as part of virtual private networking. To configure IKE follow the instructions for "Configuring Internet Key Exchange Settings" under "Managing Actions" under "IPsec" in Chapter 4 of the SAG.

SESSION INACTIVITY TIMEOUT

Enable the session inactivity timers (termination of an inactive session) from the EWS by following the instructions for "Setting System Timeout Values" or from the Control Panel by following the instructions for "Setting the System Timeout Values at the Control Panel" under System Timeout in The Security section of the SAG.

The default session timeout limits are 60 seconds for the Control Panel and 60 minutes for the EWS. To

avoid unexpected false error messages, make sure the EWS session inactivity timer is less than 25 days.

SECURE PRINT

Set the Secure Print security function to require the User ID for identification purposes to release a secure print job. Access and configure the Secure Print security function using the EWS by following the instructions under “Configuring Secure Print Settings” in the Printing section of the SAG.

Ensure that the ‘Release Policies for Secure Print Jobs Requiring Passcode When the User is Already Logged In’ option is set to Prompt for Passcode Before Releasing Jobs.

For best security, print jobs (other than LANFax jobs) submitted to the device from a client or from the EWS should be submitted as a secure print job. To ensure that print jobs can only be submitted as secure print jobs, for logged in users (since non-logged in users are denied permission to print any job in the evaluated configuration), in the instructions for “Setting Job Type Print Permissions” under “Editing Print Permissions for the Non-Logged In Users Role” under “Authorization Settings” in The Security section of the SAG, on the ‘Job Types’ page select the Only Allow Secure Print option and then select Custom and set the permission to be Allowed for Secure Print and Not Allowed for all other print types.

Once a secure print job has been submitted the authenticated user can either release the job for printing at the Control Panel by following the instructions under ”Secure Print” under “Printing Features” in the Print section of the applicable User Guide or delete the job at the Control Panel by following the directions under “Viewing, Printing or Deleting Jobs” under “Managing Secure and Held Print Jobs” under “Jobs” in the Print section of the applicable User Guide.
Note that only the submitter of a secure print job can release the job, and in the evaluated configuration only the System Administrator can delete any job, except for a secure print job where the job submitter can delete the job by entering the secure print PIN. To ensure that only the System Administrator can delete jobs, perform the following based on the instructions for “Editing a Logged-In User Role” under “Editing Apps and Tools Permissions for the Non-Logged-In Users Role” under “Authorization Settings” in The Security section of the SAG:

- Create a new permission role for Logged-In Users and give it any desired descriptive name.
- For this newly created role, set the method to be All Logged-In Users.
- Under the Apps & Tools tab, choose Custom. When the page is refreshed, go to the selection under ‘Jobs’ for ‘Job Deletion (Active Queue Only)’ and set it to Not Allowed.
- Click Apply to save the changes.

HOLD ALL JOBS

The Hold All Jobs function is used in the evaluated configuration. Set the Enablement option to Hold All Jobs in a Private Queue and the Unidentified Jobs Policies option to Hold Jobs; Only Administrators can Manage Jobs using the EWS by following the instructions for “Configuring the Hold All Jobs Feature” under “Hold All Jobs” in the Print section of the SAG.

Once a held print job has been submitted the authenticated user can release the job for printing at the Control Panel by following the instructions under ”Releasing Held Print Jobs” under “Held Print Jobs” under “Printing Features” in the Print section of the applicable User Guide. To delete a held job at the Control Panel follow the applicable instructions under “Managing Jobs at the Control Panel” under “Managing Jobs” in the Print section of the applicable User Guide.

As is the case for a secure print job, only the submitter of a held print job can release the job. Only the submitter of a held print job, and the System Administrator, can delete the print job.

802.1x DEVICE AUTHENTICATION

Enable and configure 802.1x device authentication from the Control Panel by following the instructions for "Enabling and Configuring 802.1x at the Control Panel" or from the EWS by following the instructions for "Enabling and Configuring 802.1x in the Embedded Web Server", both under 802.1x in the Security section of the SAG. Ensure that the 802.1x username and password are not blank when configuring 802.1x device authentication from the Control Panel.

Note: To be in the evaluated configuration EAP-TLS should be selected as the 802.1x authentication method.

USB PORT SECURITY

In the evaluated configuration USB ports should generally all be disabled.
If a USB port needs to be used to perform a function like diagnostics, installing a software upgrade, or using the smart card reader, the applicable host or target USB port should be temporarily enabled while the applicable function is being performed, and then when the function is competed it should be immediately disabled again.

Enable or disable the USB Ports using the EWS by following the instructions for enabling and disabling USB Ports under "USB Port Management" in The Security section of the SAG. To enable or disable the USB Ports using the Control Panel follow the instructions for "USB Port Management at the Control Panel" under "USB Port Management" in The Security section of the SAG.

SFTP FILING

SFTP Filing is used in the evaluated configuration only for transfer of the Audit Log to an external audit log server. Specify the use of Secure FTP for transferring the Audit Log to an external audit log server using the EWS by following the instructions for "Configuring FTP and SFTP Client Settings" under "FTP/SFTP Client" in The Network Connectivity section of the SAG.

Note that SFTP uses SSH. All cryptographic parameters for SSH are configured on the printer by default and cannot be modified in the TOE.

ERASE CUSTOMER DATA

Initiate the feature to erase all customer date from the device at the Control Panel and restore the device to factory-installed values by following the instructions for "Erase Customer Data" in The Logs section of the SAG.

Note: Initiate the "Erase Customer Data" function before the device is decommissioned, returned, sold or disposed of.

4. EVALUATED CONFIGURATION

The following protocols, services and functions are considered part of the evaluated configuration and should be enabled:

- TCP/IP
- Date and Time
- Copy
- Embedded Fax
- Fax Forwarding on Receive (for received Embedded Faxes)
- Scan to E-mail, including email encryption and signing
- Workflow Scanning
- Scan to Mailbox
- Print from Mailbox
- NTP

When setting up the device to be in the evaluated configuration, perform the following special setup for the above services (otherwise follow the appropriate instructions in the appropriate section of the SAG to set up and/or configure the protocol/service/function):

TCP/IP

- Enable IPv4 from the Control Panel by following the instructions for “Enabling TCP/IP” under “IP” in The Network Connectivity section of the SAG. Configure IPv4 by following the instructions for “Configuring the Network Address Manually at the Control Panel” and “Configuring DNS Settings at the Control Panel” under “IP” in The Network Connectivity section of the SAG.
- Set up and configure IPv4 from the EWS by following the instructions for “Configuring IPv4”, under “Configuring IP Settings in the Embedded Web Server” under “IP” in The Network Connectivity section of the SAG.

Note that IPv6 is not part of the Evaluated Configuration.

LISTENING SERVICES (INBOUND PORTS)

- Network Encryption

DATE AND TIME

- Ensure that the date and time on the device is correct and is set for the correct time zone where the device is located. Set the date and time from the Control Panel by following the instructions in “Setting the Date and Time at the Control Panel” under “Initial Setup at the Control Panel” in Chapter 2 of the SAG.
- Set the date and time from the EWS by following the instructions in “Setting the Date and Time in the Embedded Web Server” under “Initial Setup in the Embedded Web Server” in Chapter 2 of the SAG.
- The ‘Date and Time Setup’ option can be set to either Manual (NTP Disabled) or Automatic Using NTP.

EMBEDDED FAX

- Ensure that Embedded Fax is properly installed. The procedure for sending an Embedded Fax at the Control Panel and the features and settings available to a user for configuring/sending an Embedded Fax at the Control Panel are described under “Fax Workflows” under Fax in the Print section (Xerox Apps) of the User Guide.

- Set Embedded Fax parameters and options on the device at the Control Panel by following the instructions for “Configuring Required Fax Settings at the Control Panel“ under “Fax” in the Faxing section of the SAG.
- Set the minimum length of the (Embedded Fax) secure receive passcode from either the Control Panel or EWS by following the instructions in “Configuring Fax Passcode Length” under “Fax Security” in the Faxing section of the SAG.
- Enable and set (Embedded Fax) Secure Receive passcode from the Control Panel by following the instructions for “Enabling or Disabling the Secure Fax Feature” under “Setting Incoming Fax Defaults” under “Setting Fax Defaults” under “Fax” in the Faxing section of the SAG. To prevent unauthenticated users from being able to enable or disable the Secure Receive function, do not touch the Allow User to Manage option.
- Enable Fax Forwarding to email only on Receive and establish up to five fax forward rules using the EWS by following the instructions for “Fax Forwarding” under “Fax” in the Faxing section of the SAG. Only add E-mail addresses to the fax forward rules established by following the instructions for “Adding Email Addresses to the Rule”.
- Fax forwarding to a file location via SMB is not part of the Evaluated Configuration.
- Printing of Embedded Fax confirmation reports is not included in the Evaluated Configuration. The Embedded Fax cover sheets should not be printed with an Embedded Fax job.
- Be aware that if the Embedded Fax secure receive passcode length is changed via the Control Panel, the changed secure receive passcode length may not be reflected on the Control Panel after the system has saved the change. After the system has saved the change the changed secure receive passcode length will be reflected on the EWS and will be in effect when attempting to enter a new Embedded Fax secure receive passcode.

SCAN TO MAILBOX

- Enable and configure the Scan to Mailbox feature from the EWS by following the instructions under 'Enabling or Disabling Scan to Mailbox' under "Scanning to a Folder on the Device" in The Scanning section of the SAG.
- Establish a unique Scan-to-Mailbox mailbox for each authenticated user.
- Establish unique names for each Scan-to-Mailbox mailbox.
- Be aware that if Scan-to-Mailbox folders are cloned any existing mailboxes on the target device that have the same name as a mailbox in the clone file and will have their passwords reset to the password in the clone file.
- Sometimes an existing Scan-to-Mailbox mailbox passcode may have to be entered twice to access the applicable mailbox.
- In configuring the Scan to Mailbox feature, set the feature so that scanned documents are only stored in private folders and that public folders are not allowed by setting the proper scan policies. To set the scan policies for the Scan to Mailbox feature using the EWS follow the instructions under "Setting Scan Policies" under "Scanning to a Folder on the Device" in The Scanning section of the SAG. In the evaluated configuration set the scan policies as follows:
    1. Deselect Allow scanning to Default Public Folder
    2. Deselect Require per job password to public folders
    3. Select Allow additional folders to be created
    4. Select Require password when creating additional folders
    5. Select Prompt for password when scanning to private folder
    6. Deselect Allow access to job log data file

SCAN TO EMAIL

- Enable and configure the Scan to Mailbox feature from the EWS by following the instructions under "Scanning to an Email Address" in The Scanning section of the SAG.
- Set the domain filtering to limit the domains to which Scan to E-mail jobs can be sent. Enable the domain filtering option using the EWS by following the instructions under "Editing Domain and Email Filter Settings" under "Configuring Email Security Settings" under "Scanning to an Email Address" in The Scanning section of the SAG.
- Configure encryption and signing of Scan to Email jobs using the EWS by following the instructions for "Configuring Email Encryption Settings" and "Configuring Email Signing Settings", respectively, under "Configuring Email Security Settings" under "Scanning to an Email Address" in The Scanning section of the SAG. Set the 'Email Encryption Enablement' option to Always On; Not Editable by user.
- Configure encryption of Scan to Email jobs sent from the device over SMTP using the EWS by following the instructions for "Configuring SMTP Connection Encryption Settings" under "SMTP Server" in The Network Connectivity section of the SAG. Set the SMTP encryption method option to SMTPS.
- Configure authentication of SMTP to send Scan to Email jobs or to forward received Embedded Faxes via email using the EWS by following the instructions for "Configuring SMTP Authentication Settings" under "SMTP Server" in The Network Connectivity section of the SAG.

WORKFLOW SCANNING

- When configuring workflow scanning file repositories using the EWS (see “Configuring File Repository Settings” under “Workflow Scanning’ in The Scanning section of the SAG) or workflow pool repositories (see “Configuring Workflow Pool Repository Settings” under “Workflow Scanning’ in The Scanning section of the SAG) set the transfer protocol in the evaluated configuration to be HTTPS only; SFTP should be used only for audit log transfer.

NTP

- If it is desired to use an NTP server to synchronize and set the internal system time used by the device, using the EWS follow the instructions for enabling and configuring NTP under “NTP” in The Network Connectivity section of the SAG.

5. Excluded Features From Evaluated Configuration

The following features and protocols are not included in the evaluated configuration:

- Reprint from Saved Job
- Remote Services
- Custom Services (Extensible Interface Platform or EIP)
- Network Accounting and Auxiliary Access
- Use of Embedded Fax mailboxes
- Wi-Fi
- Wi-Fi Direct Printing
- Web Services
- InBox Apps
- Remote Control Panel
- SFTP when used for scanning
- SNMPv3
- Scan to USB
- Print from USB
- SMB Filing

Customer software upgrades via the network are not allowed as part of the evaluated configuration. System software upgrades are disabled by default to prevent unauthorized replacement of the system software. Administrators should only enable software upgrades when performing an upgrade, and software upgrades should be disabled when complete.

Software upgrades can be disabled by setting the Security Installation Policy for Software Upgrades to not allow software upgrades as follows:

1. In the Embedded Web Server, click Properties→Security→Installation Policies.
2. Make sure that the Allow Software Upgrades checkbox is not checked.
3. Click Apply.

If Software upgrades need to be enabled, check the Allow Software Upgrades checkbox.

6. Secure Acceptance

Secure acceptance, once device delivery and installation are completed, should be done by:

- Printing out a Configuration Report from the EWS by following the instruction for “Printing a Configuration Report from the Embedded Web Server” or from the Control Panel by following the instructions for “Printing a Configuration Report from the Control Panel” instructions, both under “Configuration Page” in Chapter 2 of the SAG. The Configuration Report will show the updated version of software/firmware on the device.
- Comparing the software/firmware versions listed on the Configuration Report with the Evaluated Software/Firmware versions listed in Table 1 of the applicable Security Target, latest version issued and ensure that they are the same in all cases.
- Following internal customer policies and procedures required to evaluate and install devices in your environment.

7. Secure Operation of Device Services/Functions Part of the Evaluated Configuration

PASSCODES

Change the following passcodes on a regular basis, choose passcodes to be as random as possible and set them to the indicated minimum lengths:

- Smart Card or CAC passcode – 8 characters (alphanumeric)
- Secure Print passcode – 6 digits
- (Embedded Fax) Secure Receive passcode – 6 digits
- Scan to Mailbox password – 8 characters (alphanumeric).
- IPsec IKE Pre-Shared Key Passphrase – 22 characters (alphanumeric)

Passcodes for Scan-to-Mailbox mailboxes should be selected to be as random as possible, should be changed on a regular basis consistent with applicable internal policies and procedures and should not contain any blank spaces.

Ensure that local usernames established on the device match domain names and that both map to the same individual.

OPERATION OF IIO AND ODIO (DEVICES WITH OPTIONAL HARD DISK DRIVED ONLY)

1. If a manual ODIO is to be run set up and initiate a manual ODIO as follows:
   - From the EWS follow the “Manually Deleting Image Data” instructions under “Overwriting Image Data” in The Security section of the SAG.
   - From the Control Panel follow the “Manually Deleting Image Data at the Control Panel” instructions under “Overwriting Image Data” in The Security section of the SAG.
2. If a scheduled ODIO is to be run set up and initiate a scheduled ODIO as follows:
   - From the EWS follow the “Scheduling Routine Deletion of Image Data” instructions under “Overwriting Image Data” in The Security section of the SAG.
   - From the Control Panel follow the “Scheduling Routine Deletion of Image Data at the Control Panel” instructions under “Overwriting Image Data” in The Security section of the SAG.
3. Set the ‘Confirmation Report’ setting to “On” when setting up a manual or scheduled ODIO from the Control Panel or EWS so that a Confirmation Report will always be printed upon completion of an ODIO.
4. A Standard ODIO will overwrite all image data except data stored by the Reprint Save Job feature and data stored in Embedded Fax dial directories and mailboxes; a Full ODIO will overwrite all image data including data stored by the Reprint Save Job feature and data stored in Embedded Fax dial directories and mailboxes.
5. IIO of a delayed or secure print job will not occur until after the machine has printed the job.
6. If an IIO fails, an error message will appear at the top of the screen indicating that there is an Immediate Image Overwrite error and that an On-Demand Image Overwrite should be run. This error message will persist until a manual ODIO is initiated by the System Administrator. In the case that the copy controller is reset at the same time a copy job is being processed by the device, this same error message may also appear when the copy controller has completed its reset.
7. If there is a power failure or system crash while a network scan job is being processed, an IIO of the residual data will occur upon job recovery. However, the network scan job may not appear in the

Completed Job Log.

8. If there is a power failure or system crash of the network controller while processing a print job, residual data might still reside on the hard disk drive(s). Immediately initiate a full ODIO once the machine has been restored.
9. Once a manual or scheduled ODIO has been initiated it cannot be aborted.
10. Before invoking an ODIO verify that:
    - There are no active or pending print or scan jobs.
    - There are no new or unaccounted for Dynamic Loadable Modules (DLMs), clone files or other software running on the machine.
    - There are no active processes that access the hard disk drive(s).
    - No user is logged into a session via network accounting, Xerox Standard Accounting, or the internal auditron, or into a session accessing a directory on the hard disk drive(s).
    - After a power on of the machine all subsystems must be properly synced and, if printing of Configuration Reports is enabled on the device, the Configuration Report must have printed.
    - For any previously initiated ODIO request the confirmation sheet must have printed.
11. When invoked from the EWS the status of the completed ODIO may not appear on the EWS but can be ascertained from the Confirmation Report that is printed after the Network Controller reboots.
12. If an ODIO fails to complete because of an error or system crash, a system reboot or software reset should be initiated from either the Control Panel or the EWS and be allowed to complete; otherwise, the Control Panel may become unavailable. If the Control Panel does become unavailable the machine will have to be powered off and then powered on again to allow the system to properly resynchronize. Once the system reboots or software reset has completed immediately perform another ODIO.
13. If Embedded Fax is enabled and then subsequently disabled before there is a power failure or system crash and Embedded Fax is then re-enabled after the device is restored to operational mode, the first ODIO that is subsequently initiated may fail. If that situation occurs reinitiate the ODIO.

    Note: When an ODIO fails under this scenario no Fax ODIO report may be printed, the EWS may indicate that the ODIO was successful, the Confirmation Report may indicate that the ODIO was 'Not Completed' because the device lost power and the Audit Log may indicate that the ODIO was 'Cancelled'.
14. If there is a failure in the hard disk drive(s) a message recommending that an On-Demand Image Overwrite be run will appear on the Control Panel screen. An Immediate Image Overwrite Error Sheet will also be printed or may contain incomplete status information. Immediately perform the requested On Demand Image Overwrite.
15. The time shown on the On Demand Overwrite progress screen displayed on the Control Panel may not reflect Daylight Savings Time. The message shown on the On Demand Overwrite progress screen displayed on the Control Panel may be slightly different for different products, reflecting the expected time the ODIO will take to complete for that product.
16. If an ODIO is successfully completed, the completion (finish) time shown on the printed On Demand Overwrite Confirmation Report will be the time that the system shuts down.
17. Perform a Full ODIO immediately before the device is decommissioned, returned, sold or disposed of.

OPERATION OF JOB DATA REMOVAL (DEVICES WITHOUT OPTIONAL HARD DISK DRIVES ONLY)

- Under EWS under Properties>Security>Job Data Removal:
  a. There are 2 selections, Remove Now, or Scheduled (See The Security section in SAG "Job Data Removal for Solid State Storage Devices" for full directions for each.
- Under Advanced Settings, there are 2 selections for Removal mode:
  a. Standard: Removes all User data stored in memory except for
     - Jobs and folders stored in the print from saved jobs feature

- Jobs stored in the scan to folder
- Fax mailbox contents (if a fax card is installed)

b. Full: Removes all stored user data from device memory

Note that the Job Data removal, Remove now feature, once selected, will take the device offline, and will reboot, and cannot be cancelled.

WHEN UTILIZING TLS FOR SCANNING

- TLS should be enabled and used for secure transmission of scan jobs.
- When storing scanned images to a remote repository using an https: connection, a Trusted Certificate Authority certificate should be uploaded to the device so the device can verify the certificate provided by the remote repository.
- When a certificate for a remote TLS repository fails its validation checks the associated scan job will be deleted and not transferred to the remote TLS repository. In this case the job status reported in the Completed Job Log for this job will read: "Job could not be sent as a connection to the server could not be established".
- The HTTPS protocol should be used to send scan jobs to a remote IT product.

AUDIT LOG NOTES

Some text in the main Audit Log may contain strings that are not written in US-ASCII.

In viewing the main Audit Log the System Administrator should note the following:

- User names in Audit Log entries can sometimes include extraneous characters.
- Deletion of a file from Reprint Saved Job folders or deletion of a Reprint Saved Job folder itself is recorded in the Audit Log (Event 21, Delete File/Dir).
- Deletion of a print or scan job or deletion of a scan-to-mailbox job from its scan-to-mailbox folder may not be recorded in the Audit Log.
- Deletion of a held job may display an incorrect status in the corresponding entry in the Audit Log (Event 21, Delete File/Dir).
- Extraneous process termination events (Event 50, Process Terminated) may be recorded in the Audit Log when the device is rebooted or upon a Power Down / Power Up. Extraneous security certificate completion status (Created/Uploaded/Downloaded) events (Event 38, X509 certificate) may also be recorded.
- Duplicate audit log entries may appear in the Audit Log for some events such as when the system timeout values are changed or when adding/deleting a Domain Controller for smart card authentication.
- When a configuration page in printed, the corresponding audit log entry may have "system user" as the user name rather than the actual user who printed the configuration page.
- Download and review the Audit Log on a daily basis. In downloading the Audit Log the System Administrator should ensure that Audit Log records are protected after they have been exported to an external trusted IT product and that the exported records are only accessible by authorized individuals.
- If a system interruption such as power loss occurs a job in process may not be fully written to the hard disk drive(s). In that case any temporary data created will be overwritten during job recovery but a corresponding record for the job may not be recorded in the completed job log or audit log.
- Once Embedded Device Security is enabled on the device, any attempts to read from read-protected files and directories or to change write protected files and directories will result in a Security Alert being recorded in the Audit Log. If configured, an email alert will also be sent.
- The device will provide an email alert to the System Administrator when the main Audit Log reaches 13,500 entries (90% "full"), when the main Audit Log reaches 28,500 events, (15K +13.5K), and every 15,000 event intervals thereafter (e.g., 43,500 events, 61,500 events, etc.). To enable the System Administrator to get any email alert, follow the instructions for "Email Alerts" under "Configuring Alerts" in The Logs section of the SAG.
- Set the e-mail address to notify when the audit log reaches 13,500 audit events or when it is full. To set the alert follow the instructions for "Configuring Alerts" in The Logs section of the SAG.
- The audit log can also be saved in Common Event Format and transferred via the syslog protocol to a Software Information and Event Management (SIEM) system on an external server. The instructions for doing this are as follows:

1. Log into the EWS as an administrator
2. Click Properties Security Logs SIEM
3. Configure up to 3 destinations to send the audit log via the Syslog protocol
4. Select the View Events button to view the latest audit log events; select the Download Events button to download the audit log in the Common Event Format for transfer.
5. Select the Send Sample Event button to send the audit log to the configured destination(s).

SPECIAL CONFIGURATION NOTES

1. Be careful not to create an IP Filtering rule that rejects incoming TCP traffic from all addresses with source port set to 80; this will disable the EWS. Also, configure IP filtering so that traffic to open ports from external users (specified by subnet mask) is dropped and so that the following ports for web services are closed: tcp ports 53202, 53303, 53404 and tcp/udp port 3702. Also ensure that entire access to the device is not blocked by defining, for example, a rule for IP Address 0.0.0.0 with a reject/drop action kept in Position 1 in the list of IP Filters.
2. Ensure the user permission roles names do not contain single quotes (‘) or double quotes (“).
3. Ensure there are no jobs being held by the device when data encryption is enabled/disabled.
4. If the hash algorithm is selected to be SHA-256 (for those cases (e.g., IPsec IKE Settings) where a hash algorithm can be selected) the Administrator may not be able to change the hash selection to be SHA-1. See The Security section of the SAG for the place where the hash size can be set – IPsec “Creating a New Action”; otherwise the device will automatically set the hash size without intervention required.
5. Users should be aware that correct remote repository document pathnames for the receipt of workflow scanning jobs should start with one ‘\’ as opposed to the two ‘\’s shown in the SAG (e.g., page 140).
6. Users should be provided with appropriate training on how to use the device in a secure manner before being assigned user accounts to access the device.
7. Before upgrading software on the device via the Manual/Automatic Customer Software Upgrade, please check for the latest certified software versions. Otherwise, the machine may not remain in its evaluated configuration.
8. Users experiencing problems logging in to the device using the EWS only on a particular web browser are advised to switch to a different web browser.
9. The device should be installed in a standard office environment. Office personnel should be made aware of authorized service calls (for example through appropriate signage) in order to discourage unauthorized physical attacks such as attempts to remove the internal hard disk drive(s). Ensure that office personnel are made aware to pick up the outputs of print and copy jobs in a timely manner.
10. Caution: The device allows an authenticated System Administrator to disable some functions like FIPS mode that are necessary for secure operation. Periodically review the configuration of all installed machines in your environment to verify that the proper evaluated configuration is maintained.
11. System Administrators should avoid opening emails and attachments from unknown sources unless the emails and attachments have been properly scanned for viruses, malware, etc.
12. The device has an automatic lockout that will disable the ability of anyone who enters five successive incorrect authentication credentials via either the Control Panel or the EWS from logging into the device for 5 minutes. After the 5-minute lockout period, login attempts will automatically be allowed again.
13. System Administrators and users should:
    - Whenever possible use a browser to access the EWS whose only purpose is to access the EWS.
    - Always logoff the browser immediately after completing any tasks associated with accessing the EWS.
    - Not allow the browser to either save their username/password or “remember” their login.
    - Follow secure measures, only use browsers with TLS 1.1 and above and not open any malicious links or documents with their browser.
14. If software upgrades are required, restrict upgrades to System Administrators only by following the instructions for “Updating the Device Software” in The Logs section of the SAG. The best way to determine the current software version is to print out a Configuration Report by following the instructions below:
    - Touch the Device LUI, then touch Information Pages

- Touch Configuration Report, then touch Print

15. The latest general software release available from https://www,xerox.com can be found by accessing the following in the order stated:
    - Go to https://www,xerox.com
    - Select the Customer Support > All Support and Drivers links
    - In the text box enter the model number of your device. A menu list of all Xerox devices with that model number will appear; select the one that corresponds to the product you have.
    - Select the link that includes the 'Print Drivers & Downloads'
    - Scroll down the resultant page; under 'Firmware' will be the latest general release. Click on the release link and a page will be displayed that allows you to download the release onto a desired location.
16. All passwords entered on the Control Panel for authentication purposes will be obfuscated by '*'s. All passwords entered on the EWS for authentication purposes will also be obfuscated, but the character that does the obfuscation will depend on the web browser used. This applies to all the models covered by these guidelines.
17. The System Administrator does not have to configure or perform any actions to utilize the random number generation needed for key generation and for the encryption algorithms.
18. The following errors could result from power-on self-tests:
    - In the case of a health failure check for entropy sources, the letter 'J' is displayed on POST code display on the back of the MFD and the device is rebooted. The POST code remains for several seconds until the controller resets. After three (3) sequential reboots as a result of continuous entropy health check failures, the device will be halted with 'J' being displayed. At this point the System Administrator should initiate a service call to fix the device.
    - At any point in the first three (3) reboots the entropy health check passes, it resets the reboot count to 0 and clears the 'J' display.
    - Any errors associated with failure of any of the encryption modules are indicated on the console connected to the backchannel; there will be no error messages displayed on the Control Panel. This console is only be accessible from a Xerox service technician. The only action required by the System Administrator is to contact Xerox Technical Support to have a Xerox service technician check this console when the device is being serviced.
19. Unauthenticated User should not be able to delete another user's print job if the admin sets the Job Deletion for Non-Logged in Users (Unauthenticated) to Not Allowed.
20. Unauthenticated user permission for scan to not allowed.
21. Should a connection between the device and another IT product using one of the security protocols in the evaluated configuration be unintentionally broken or terminated, in general the user does not have to take any action; the connection will automatically be reestablished. The only exception is that if the user is in the middle of an EWS session and the HTTPS connection is broken, HTTPS itself will automatically reconnect but the user will have to reestablish the EWS session between the browser being used and the EWS to access the device again.
22. When five successive authentication attempts are made using either the Control Panel or EWS, the device will lockout the user or system administrator for 5 minutes. After the 5-minute lockout period the user or system administrator will be able to attempt another authentication attempt.
23. There are no situations where key destruction may be delayed at the physical layer.

8. Secure operation of Device Services/Functions Not Part of the Evaluated Configuration

Evaluated Configuration
Change the SNMPv1/v2c public/private community strings from their default string names to random un-guessable string names of at least 8 characters in length.
SNMPv3:

- SNMPv3 cannot be enabled until TLS and HTTPS (TLS) are enabled on the machine. To enable SNMPv3 using the EWS follow the instructions for "Configuring SNMPv3" under "SNMP" in The Network Connectivity section of the SAG.

  Be aware that in configuring SNMPv3 there is the option of resetting both the Privacy and Authentication passwords back to their default values. This option should only be used if necessary, since if the default passwords are not known no one will be able to access the SNMP administrator account[7].

  Make sure that the "Authentication/Encryption" selection in the evaluated configuration is 'SHA-1/AES-128'.
- Customers should sign up for the RSS[8] subscription service available via the Xerox Security Web Site (Security@Xerox) at https://www,xerox.com/security that permits customers to view the latest Xerox Product Security Information and receive timely reporting of security information about Xerox products, including the latest security patches.
- Customers who encounter or suspect software problems should immediately contact the Xerox Customer Support Center to report the suspected problem and initiate the SPAR (Software Problem Action Request)[9] process for addressing problems found by Xerox customers.
- Depending upon the configuration of the device, two IPv4 addresses, a primary IPv4 address and a secondary IPv4 address, may be utilized. Select whether the primary IPv4 address will be obtained statically or dynamically via DHCP from the IP (Internet Protocol) page on the EWS[10]. The second IPv4 address is assigned via APIPA when the System Administrator enables the 'Self Assigned Address' option from the IP (Internet Protocol) page on the EWS[11]. If the 'Self Assigned Address' option is enabled (which is the default case), this secondary IPv4 address will not be visible to the SA . The 'Self Assigned Address' option from the EWS IP (Internet Protocol) page should be disabled unless either APIPA is used or Apple

[7] The SNMP administrator account is strictly for the purposes of accessing and modifying the MIB objects via SNMP; it is separate from the System Administrator "admin" user account or user accounts given SA privileges by the System Administrator "admin" user. The administrator account cannot perform any System Administrator functions.
[8] Really Simple Syndication – A lightweight XML format for distributing news headlines and other content on the Web. Details for signing up for this RSS Service are provided in the **Security@Xerox RSS Subscription Service guide** posted on the Security@Xerox site at https://www,xerox.com/**go/xrx/template/009.jsp?view=Feature&ed_name=RSS_Security_at_Xerox&Xcntry=USA&Xlang=en_US**.
[9] A SPAR is the software problem report form used internally within Xerox to document customer-reported software problems found in products in the field.
[10] The primary IPv4 address can also be assigned dynamically via DHCP from the Dynamic Addressing screen on the Control Panel.
[11] The primary IPv4 address will always be displayed on the Configuration Report that can be printed for the device.

Rendezvous/Bonjour support is required.

- If IPv6 is disabled and then a software upgrade is performed by a Xerox Service Technician using an AltBoot, IPv6 will be disabled even though both the Control Panel and EWS show that IPv6 is enabled. IPv6 can be enabled again via the EWS by first disabling and then re-enabling it.
- Software Verification Test: Initiate the software verification test feature using the EWS by following the instructions for “Verifying the Software” in The Security section of the SAG.
- The device does provide a Remote Control Panel that allows a user to access the control panel of the printer from a Web browser. Although this feature is not part of the evaluated configuration, if this capability is desired follow the instructions for “Remote Control Panel” in The Logs section of the SAG. Make sure that the Block device control panel option is selected to restrict other users from accessing the control panel when someone is connected via the Remote Control Panel.
- Users are able to print, fax, scan and copy according to the User permission Access Rights that can be set on the device based on administrator configured policies. See Chapter 4, ‘Security’ in the SAG.
- The following windows are available to any authentication and authorized user from the Control Panel. These windows provide standard machine services or job management capability:
    - Embedded Fax Batch Send Confirmation – Allows a user to either send an Embedded Fax job to a remote destination immediately or include the job as part of a “batch” of Embedded Fax jobs sent to the same destination. Is accessible by selecting the following screens/buttons in order: [Services Home] hard button [Fax] feature button [Start] hard button when a user is submitting an Embedded Fax Send job to the same destination as a previously submitted “delayed send“ Embedded Fax job.
    - Pausing an active job being processed by the device – Allows the user to pause an active copy, print, workflow scanning, scan to email, Internet Fax or Embedded Fax job while it is being processed. Is accessible by selecting the [Stop] machine hard button while a job is being processed by the device. Depending on the type of jobs being processed by the device when the [Stop] button is selected, one of the following Pause windows will be displayed as appropriate to allow the user to determine whether to delete or continue processing of the job: Scanning Pause window, Printing Pause window, Copy Only (Scanning and Printing) Pause window, Scanning/Printing (Simultaneous Jobs) Pause window, Scanning Build Job Segment (No Printing) Pause window, Printing Build Job Segment (No Scanning) Pause window or Scanning Build Job Segment/Printing Another Job Pause window.
    - Overwrite Security Failure – Automatically provides an error message to the user is case an Immediate Image Overwrite of a copy, print, workflow scanning, scan to email, LAN Fax or Embedded Fax job fails. The error message informs the user to notify the System Administrator that an On Demand Overwrite should be run and persists on the Control Panel screen until either a manual or a scheduled On Demand Overwrite is initiated.
- The EWS provides a set of on-line help pages that provide guidance on most of the EWS pages. These on-line help pages can be accessed from the EWS by selecting the [Help] button on the upper right hand corner of every EWS page; the on-line help page corresponding to the EWS page being viewed will be displayed. There is also a ‘TOC’ contents list of all EWS help pages to the left of each help page; scrolling through the content list and

selecting the desired page will also cause the applicable on-line help page to be displayed.

- The following pages are available from the Web User Interface with no user login and authentication required:
    - Print – User can submit print jobs through the Web User Interface by choosing Submit job button, without being authenticated.
    - Home Screen – users can view the home screen of the device that contains information on paper Trays, and all active notifications at the device.
    - Jobs – Users can view the active job queue.
- Customers who required specialized changes to support unique workflows in their environment may request specific changes to normal behavior. Xerox will supply these SPAR releases to the specific customers requesting the change. Please note that in general enabling a specialized customer-specific feature will take the system out of the evaluated configuration.

9. SELECTED AUDIT LOG ENTRIES

The following table lists the security-related events that are recorded in the audit log and/or protocol log:

Event ID	Event description	Entry Data
1	System startup	Device name Device serial number
2	System shutdown	Device name Device serial number
3	Manual ODIO Standard started	Device name Device serial number
3	Standard Disk Overwrite started	User name Device name Device serial number
3	ODIO Standard started	Device name Device serial number
4	Manual ODIO Standard complete	Device name Device serial number Overwrite Status
4	ODIO Standard complete	Device name Device serial number Completion Status (“Success” | “Failed”)
4	Standard Disk Overwrite complete	Device name Device serial number Completion Status (“Success” | “Failed”)
5	Print job	Job name User Name Completion Status IIO status Accounting User ID Accounting Account ID
6	Network scan job	Job name User Name Completion Status IIO status Accounting User ID Accounting Account ID total-number-net-destination net-destination.
7	Server fax job	Job name User Name Completion Status IIO status Accounting User ID Accounting Account ID Total-fax-recipient-phone-numbers fax-recipient-phone-numbers net-destination.
9	Email job	Job name User Name Completion Status IIO status Accounting User ID Accounting Account ID total-number-of-smtp-recipients smtp-recipients

Event ID	Event description	Entry Data
12	Copy Job	Job name User Name Completion Status IIO status Accounting User ID Accounting Account ID Total-fax-recipient-phone-numbers fax-recipient-phone-numbers
13	Embedded Fax Job	Job name User Name Completion Status IIO status Accounting User ID Accounting Account ID Total-fax-recipient-phone-numbers fax-recipient-phone-numbers
14	Lan Fax Job	Job name User Name Completion Status IIO status Accounting User ID Accounting Account ID Total-fax-recipient-phone-numbers fax-recipient-phone-numbers
16	Full Disk Overwrite started	User name Device name Device serial number
17	Full Disk Overwrite complete	Device name Device serial number Completion Status (“Success” | “Failed”)
20	Scan to Mailbox job	Job name or Dir name User Name Completion Status IIO status
21	Delete File/Dir	Job name or Dir name User Name Completion Status IIO status
29	Network User Login	UsereName Device name Device serial number Completion Status (Success, Failed)
30	SA login	UsereName Device name Device serial number Completion Status (Success or Failed)
31	User Login	UserName Device name Device serial number Completion Status (Success or Failed)
33	Audit log download	UserName Device name Device Serial Number Completion status (Success or Failed).
34	IIO feature status	UserName Device name Device serial number IIO Status (enabled or disabled)
35	SA pin changed	UserName Device name Device serial number Completion status

Event ID	Event description	Entry Data
36	Audit log Saved	UserName Device name Device serial number Completion status
37	Force Traffic over Secure Connection (HTTPS)	UserName Device name Device serial number Completion Status (Enabled/Disabled/Terminated)
38	X509 certificate	UserName Device name Device serial number Completion Status (Created/uploaded/Downloaded).
39	IP sec Enable/Disable/Configure	UserName Device name Device serial number Completion Status (Configured/enabled/disabled/Terminated)
40	SNMPv3	UserName Device name Device serial number Completion Status (Configured/enabled/disabled).
41	IP Filtering Rules	UserName Device name Device serial number Completion Status (Configured/enabled/disabled).
42	Network Authentication Enable/Disable/Configure	UserName Device name Device serial number Completion Status (Enabled/Disabled)
43	Device clock	UserName Device name Device serial number Completion Status (time changed/date changed)
44	SW upgrade	Device name Device serial number Completion Status (Success, Failed)
49	Smartcard (CAC/PIV) access	UserName (if valid Card and Password are entered) Device name Device serial number Process Name
50	Process terminated	Device name Device serial number Process name
51	Scheduled Disk Overwrite scheduled	Device name Device serial number ODIO type (Full or Standard) Scheduled time ODIO status (Started/Completed/canceled) Completion Status (Success/Failed/Canceled)
`51	Scheduled ODIO Feature	User name Device name Device serial number Status (“Enabled” | ”Disabled” | ”Configured”)
55	SA Tools Access Admin	Device serial number Completion Status (Locked/Unlocked)
57	Session Timer Logout	Device Name Device Serial Number Interface (Web, LUI) User Name (who was logged out) Session IP (if available)

Event ID	Event description	Entry Data
58	Session Timer Interval Change	Device Name Device Serial Number Interface (Web, LUI)(Timer affected by change) User Name (who made this change) Session IP (if available) Completion Status
59	Feature Access Control Enable/Disable/Configure	User Name Device Name Device Serial Number Completion Status (Enabled/Disabled/Configured) Interface (Web, Local, CAC, SNMP) Session IP address (if available)
60	Device Clock NTP Enable/Disable	Device Name Device serial number Enable/Disable NTP NTP Server IP Address Completion Status (Success/Failed)
61	Device Administrator Role Permission	Device Name Device Serial Number User Name (of target user) Completion Status (Grant/Revoke)
62	Smartcard Configuration	UserName Device Name Device Serial Number Card Type Completion Status (Success/Failed)
64	802.1x Configuration	UserName Device Name Device Serial Number Completion Status (Enabled/Configured/Wired/Disabled)
65	Abnormal System Termination	Device Name Device Serial Number
66	Local Authentication	UserName Device Name Device Serial Number Completion Status (Enabled/Disabled)
67	Web User Interface Authentication (Enable Network or Local)	UserName Device Name Device Serial Number Authentication Method Enabled (Network/Local)
68	FIPS Mode Enable/Disable/Configure[12]	UserName Device name Device Serial Number Enable/Disable/Configure
71	USB Port Enable/Disable	User Name Device Name Device Serial Number USB Port ID Completion Status (Enabled/Disabled/Configured)
73	System Log Download	Username IP of requesting device (if available) File names downloaded Destination (IP address) Completion status (Success/failed)

[12] For the new FIPS w/CC mode, there are audit log events triggered by these sequences: FIPS mode disabled->FIPS w/CC mode enabled: FIPS Mode Enable event, followed by FIPS Mode Configure event; FIPS w/CC mode enabled-> FIPS w/CC mode disabled: FIPS Mode Config event followed by FIPS Mode Disable event; FIPS mode enabled -> FIPS w/CC mode enabled: FIPS Mode Config event; FIPS w/CC mode enabled -> FIPS mode enabled: FIPS Mode Config Event

Event ID	Event description	Entry Data
80	SMTP Connection Encryption	UserName Device name Device serial number Completion Status (Enabled for STARTLS / Enabled for STARTLS if Avail / Enabled for SSL/TLS / Disabled / Configured)
81	Email Domain Filtering Rule	User name Device Name Device Serial Number Completion Status (Feature Enabled/Feature Disabled, Rule Added / Rule Deleted)
82	Software Self Test Started	Device Name Device Serial Number
83	Software Self Test Complete	Device Name Device Serial Number Completion Status(Success/Failed/Cancelled)
88	Digital Certificate Import Failure	Device name Device serial number Requester email address Failure Reason (Invalid Address/Invalid Certificate/Invalid Signature)
89	Device User Account Management	User Name Device Name Device serial number User name added or deleted Completion Status (Created/Deleted)
90	User Account Password Change	User Name Device Name Device serial number User name affected Completion Status (Password Modified)
91	EFax Job Secure Print Passcode	UserName (managing passcodes) Device name Device serial number Completion Status (Passcode Created/Changed)
92	Scan2Mailbox Folder Password Change	UserName (managing passwords) Device name Device serial number Folder Name Completion Status (Password was Changed)
93	EFax Mailbox Passcode	UserName (managing passcodes) Device name Device serial number Completion Status (Passcode Created/Changed)
94	FTP/SFTP Filing Passive Mode	User Name Device Name Device Serial Number Completion Status (Enabled / Disabled)
95	EFax Forwarding Rule	User Name Device Name Device Serial Number Fax Line 1 or 2 (if applicable) Completion Status (Rule Edit / Rule Enabled / Rule Disabled)
99	Network Connectivity Enable / Disable	UserName Device name Device serial number Completion Status (Enable Wireless / Disable Wireless (Enable Wired /Disable Wired)

Event ID	Event description	Entry Data
102	SW upgrade enable / disable	UserName Device name Device serial number Completion Status (Enable Installation / Disable Installation)
105	IPv4 Enable/Disable/Configure	UserName Device name Device serial number Completion Status (Enabled Wireless/Disabled Wireless/ Configured Wireless) (Enabled Wired/Disabled Wired/ Configured Wired)
106	SA PIN Reset	Device serial number Completion Status (Success/Failed)
109	Efax Passcode Length	UserName (managing passcodes) Device name Device serial number Completion Status (Passcode Length Changed)
116	EWS Access/Configure	UserName Device name Device serial number Completion Status (Standard Access, Open Access, Restricted)
117	System log push to Xerox	Username if authenticated Server destination URL Log identifier string (filename) Completion Status (Success / Failed)
124	Invalid Login Attempt Lockout	Device name Device serial number Interface (EWS, Local UI) Session IP Address if available
125	Protocol audit Log enable/Disable	UserName Device Name Device serial number Completion Status Enable / Disable
127	Successful Login after Lockout Expires	Device name Device serial number Interface (EWS) Session IP Address if available Count of invalid attempts: “attempts xx” where xx = the number of attempts.
128	Erase Customer Data	Erase Customer Data Device serial number Success / Failed
129	Audit log SFTP scheduled Configure	UserName Device Name Device serial number Completion status (Enable/Disable/Configured)
130	Audit Log SFTP Transfer	UserName Device Name Device serial number Destination server Completion Status (File Transmitted)
131	Remote Software Download Enable Disable	UserName Device name Device serial number Completion Status (Enable/Disable)

Event ID	Event description	Entry Data
144	User or Group Role Assignment	User name Device name Device serial number User or group name (assigned) Role name Action (added/removed)
145	User Permission Role	User name Device name Device serial number Role name Completion status (Created / Deleted / Configured)
146	Admin Password Policy Configure	User name Device name Device serial number
147	Local user account password policy	User name Device name Device serial number
148	Restricted admin login	User name Device name Device serial number Completion status: “Success” or “Failed”
149	Grant / revoke restricted admin rights	User name (of user making the change) Device name Device serial number User name (of target user) Action: “Grant” or “Revoke”
150	Manual session logout	Device Name Device Serial Number Interface (Web, LUI, CAC) User Name (who was logged out) Session IP (if available)
151	IPP Enable/Disable/Configure	User name Device name Device serial number Completion status: (“Enabled” / “Disabled” / “Configured”)
152	HTTP Proxy Server Enable/Disable/Configure	User name Device name Device serial number Completion status: (“Enabled” / “Disabled” / “Configured”)
154	Restricted Admin Permission Role	User name Device name Device serial number Restricted admin role name Completion status (Created / Deleted / Configured)
156	Lockdown and Remediate Security	User name Device Name Device Serial number Completion status: (“Enabled” / “Disabled”)
157	Lockdown Security Check Complete	User name (if available. “SYSTEM”, if executed as a scheduled event) Device name Device serial number Completion status (“Success” / “Failed”)
158	Lockdown Remediation Complete	User name (if available. “SYSTEM”, if executed as a scheduled event) Device name Device serial number Completion status (“Success” / “Failed”)
159	Send Engineering Logs on Data Push	User name (if available) Device name Device serial number Current setting (“Enabled” / “Disabled”)

Event ID	Event description	Entry Data
160	Allow the Print Submission of Clone Files	User Name (if available) Device Name Device serial number Completion status: (“Enabled” / “Disabled”)
161	Network Troubleshooting Start, Stop	User Name Device Name Device Serial Number Completion Status (“Started”, “Stopped”)
162	Network Troubleshooting Data Download	User Name File Name (of downloaded file) Device Name Device Serial Number Destination (IP address) Completion Status (“Success” / “Failed”)
163	dns-sd text file download	User Name File Name (of downloaded file) Device Name Device Serial Number Destination (IP address) Completion Status (“Success” / “Failed”)
164	One-Touch App Management	User Name Device Name Device serial number Onetouch application Display Name Action (“Install” / “Un-install”) Completion: (“Success” / “Failed”)
165	SMB Browse	User Name Device Name Device serial number Completion status: (“Enabled” / “Disabled” / “Configured”)
166	Job Data Removal Standard started	Device Name Device serial number
167	Job Data Removal Standard complete	Device Name Device serial number Completion Status (“Success” / “Failed”)
168	Job Data Removal Full started	Device Name Device serial number
169	Job Data Removal Full complete	Device Name Device serial number Completion Status (“Success” / “Failed”)
170	Scheduled Job Data Removal Configure	User Name Device Name Device serial number Status (“Enable”/”Disable”/”Configured”)
171	Cross-Origin-Resource-Sharing (CORS)	User Name Device Name Device serial number Status (“Enable”/”Disable”)
172	One-Touch App Export	User Name Device Name Device serial number Completion Status: (“Success” | “Failed”)

Event ID	Event description	Entry Data
173	Device File Distribution Trust Operations	User Name Device Name Device serial number Member Name Member serial number TC Lead Device Name TC Lead Serial Number Trust operation: (“Grant” | “Revoke”) Completion status: (“Success” | “Failed”)
174	Device File Distribution Feature	User Name Device Name Device serial number Trust operation: (“Enable” | ”Disable” | “Configure”) Completion status: (“Success” | “Failed”)
175	Device File Distribution - Store File for Distribution	User Name Device Name Device serial number File type: (“SWUP” | “Clone” | “Add-On”) File Name
176	Xerox Configuration Watchdog	User Name Device Name Device Serial number Completion status: (“Enabled” | “Disabled”)
177	Xerox Configuration Watchdog Check Complete	User Name (if available. “SYSTEM”, if executed as a scheduled event) Device Name Device serial number Completion status (“Success” | “Failed”)
178	Xerox Configuration Watchdog Remediation Complete	User Name (if available. “SYSTEM”, if executed as a scheduled event) Device Name Device serial number Completion status (“Success” | “Failed”)
179	ThinPrint Feature	User Name Device Name Device serial number Completion Status: (“Enabled” | “Disabled” | “Configured”)
180	Beaconing for “iBeacon for AirPrint Discovery”	User Name Device Name Device Serial Number Completion Status (Enabled | Disabled)
181	Network Troubleshooting Install, Uninstall	User Name Device Name Device serial number Completion Status: (“Installed” | “Uninstalled”)
182	POP3 Connection Encryption (TLS)	User Name Device Name Device serial number Completion Status: (“Enabled” | “Disabled” | “Configured”)
183	FTP Browse	User Name Device Name Device Serial Number Completion Status (Configured | Enabled | Disabled)
184	SFTP Browse	User Name Device Name Device Serial Number Completion Status (Configured | Enabled | Disabled)

Event ID	Event description	Entry Data
189	Smart Proximity Sensor “Sleep on Departure”	User Name Device Name Device Serial Number Completion Status (Enabled | Disabled)
190	Cloud Service	User Name Device Name Device Serial Number Completion Status (Enabled | Disabled)
192	Scan to Cloud Job	Job Name User Name Cloud Service Completion Status IIO Status Accounting User ID-Name Accounting Account ID-Name
193	Xerox Workplace Cloud	User Name Device Name Device Serial Number Completion Status (Enabled | Disabled)
194	Scan to Save FTP and SFTP Credentials Policy	User Name Device Name Device Serial Number Completion Status (Never | Always| Prompt)
195	Card Reader	Device Name Device Serial Number Status: (Connected | Disconnected)
196	EIP Apps	User Name Device Name Device Serial Number App Name Action (Install | Delete) Completion Status (Success | Failed)
197	EIP Apps	User Name Device Name Device Serial Number App Name Action (Install | Delete) Completion Status (Enabled | Disabled)
201	Cannot Establish a Connection to the OCSP Responder	Device Name Device Serial Number Responder Address
202	OSCP Responder Returns a ‘revoked’ Status	Device Name Device Serial Number Responder Address
204	Syslog Server	User Name Device Name Device Serial Number Server IPv4 Address (If Available) Server IPv6 Address (If Available) Completion Status (Configured | Enabled | Disabled)
8947	ERR_IKE_NOTIFY_PAYLOAD	Protocol log error message, indicates the client rejected a proposal or an SA expired.
8949	ERR_IKE_TIMEOUT	Protocol log error message, indicates the client did not respond to a message
8967	ERR_IKE_MISMATCH_HASH_ALGO	Protocol log error message, indicates an algorithm mismatch between server and client.

Auditable Events

Auditable Events	Relevant SFR	Additional Information	Applicable Audit Log Events
Job completion	FDP_ACF.1	Type of job	5 – Print Job 6 – Network Scan Job 9 – Email Job 12 – Copy 13 – Efax 14 – Lan Fax Job 20 – Scan to Mailbox Job
Unsuccessful User authentication	FIA_UAU.1	None	29 – Network User Login 30 – SA Login 31 – User Login
Unsuccessful User identification	FIA_UID.1	None	29 – Network User Login 30 – SA Login 31 – User Login
Use of management functions	FMT_SMF.1	None	5 – Manual ODIO Standard started 10 – Audit Log Disabled 11 – Audit Log Enabled 15 – Data Encryption enabled 16 – Manual ODIO Full started 18 – Data Encryption disabled 33 – Audit Log download 34 – IIO Feature Status 36 – Audit log Saved 37 - Force Traffic over Secure Connection (HTTPS) 38 – X509 certificate 39 – IP sec 41 – IP Filtering Rules 42 – Network Authentication 51 – ODIO scheduled 58 – Session Timer Interval Change 60 – Device Clock NTP 61 – Grant/Revoke Admin 62 – Smartcard (CAC/PIV)

Auditable Events	Relevant SFR	Additional Information	Applicable Audit Log Events
			64 – 802.1x 80 – SMTP Connection Encryption 89 – User Name Add/Delete 90 – User Name Password Change 94 – FTP/SFTP Filing Passive Mode 95 – EFax Forwarding Rule 109 – EFax Passcode Length 128 – Erase Customer Data 129 – Audit log SFTP scheduled 130 – Audit Log SFTP Transfer 144 – User or Group Role Assignment 145 – User Permission Role 146 – Admin Password Policy Configure 147 – Local user account password policy
Modification to the group of Users that are part of a role	FMT_SMR.1	None	144 – User or Group Role Assignment 145 – User Permission Role
Changes to the time	FPT_STM.1	None	43 – Device Clock 60 – Device Clock NTP
Failure to establish session	FTP_ITC.1, FTP_TRP.1(a), FTP_TRP.1(b)	Reason for failure	Protocol Log

Standard Ports

Port	Type	Service Name
80 or 443	TCP	HTTP including: Web User Interface Web Services for Products (WSD) WebDAV
68	UDP	DHC ACK Response to DHCP
88	UDP	Kerberos
110	TCP	POP3
139	TCP	NETBIOS
161	TCP	SNMP
162	TCP	SNMP Trap
137	UDP	NETBIOS (Name Service)
138	UDP	NETBIOS (Datagram Service)
161	UDP	SNMP
427	TCP/UDP	SLP
443	TCP	HTTPS – HTTP over TLS, IPPS
445	TCP	SMB
500 & 4500	TCP/UDP	IPSec
515	TCP	LPR
631	TCP	IPP
3702	TCP/UDP	WSD (Discovery)
4000	TCP	ThinPrint
5353	TCP/UDP	mDNS
5354	TCP	mDNS Responder IPC
9100	TCP	Raw IP (also known as JetDirect, AppSocket or PDL-datastream)
5909-5999	TCP	Remote Access to local display panel. Port is randomly selected and communications encrypted with TLS 1.2.
51333	TCP	Device File Distribution downloads
53202	TCP	WSD Transfer
53303	TCP	WSD Print
53404	TCP	WSD Scan

10. 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/