Version 1.2
May 19, 2015

Secure Installation and Operation of Your WorkCentre™ 5945 / 5955

Secure Installation and Operation of Your WorkCentre™ 5945 / 5955

Purpose and Audience

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 devices are currently undergoing Common Criteria evaluation and are evaluated in a particular configuration, referred to in the rest of this document as the "evaluated configuration". Section 1 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 http://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 Security Target[3]. Upon completion of the evaluation, the Security Target will be available from the Common Criteria Certified Product website (http://www.commoncriteriaportal.org/products.html) list of evaluated products, from the Xerox security website (http://www.xerox.com/information-security/common-criteria-certified/enus.html), or from your Xerox representative.

I. 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 Image Overwrite
- On Demand Image Overwrite
- Data Encryption
- FIPS 140-2 Mode
- IP Filtering
- Audit Log
- Security Certificates, Transport Layer Security (TLS)/Secure Sockets Layer (SSL) and HTTPS
- IPSec
- Local, Remote or Smart Card Authentication
- Local Authorization
- User Permissions
- Personalization
- 802.1x Device Authentication
- Session Inactivity Timeout
- USB Port Security
- Software Verification Self-Test
- SFTP Filing
- Embedded Fax Secure Receive
- Secure Print
- Hold All Jobs
- McAfee® Embedded Control (a ConnectKey feature)

---

[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 Multifunction Device Security Target WorkCentre 5945/5955, Latest Version issued

System Administrator login is required when accessing the security features via the Web User Interface (Web UI) or when implementing the guidelines and recommendations specified in this document. To log in to the Web UI as an authenticated System Administrator, follow the instructions under "Accessing CentreWare Information Services as a System Administrator" under "Accessing Administration and Configuration Settings" in Section 2 of the applicable System Administration Guide (SAG)[4].

To log in to the Local User Interface (denoted hereafter in this document as the Control Panel) as an authenticated System Administrator, follow "Accessing the Control Panel as a System Administrator" under "Accessing Administration and Configuration Settings" in Section 2 of the SAG.

b. Follow the instructions located in Chapter 4, Security, in the SAG to set up the security functions listed in Item a above. Note that whenever the SAG requires that the System Administrator provide an IPv4 address, IPv6 address or port number the values should be those that pertain to the particular device being configured.

In setting up the device to be in the evaluated configuration, perform the following[5]:

1. ***Administrator Password***:

   i. Change the Administrator password upon installation. Reset the Administrator password periodically.

   - Set the Administrator password to a minimum length of eight alphanumeric characters.
   - Change the Administrator password once a month and
   - Ensure that all passwords are strong passwords (e.g., passwords use a combination of alphanumeric and non-alphanumeric characters; passwords don't use common names or phrases, etc.).

   To change the Administrator password from the Web UI, follow the instructions under "Changing the System Administrator Password" in Section 2 of the SAG.

   To change the Administrator password from the Control Panel, follow the instructions under "Changing the System Administrator Password at the Control Panel" in Section 2 of the SAG.

   ii. Disable the Admin Password Reset security feature so it is not used. To disable this feature, perform the following:

   - At the Web UI select the **Properties** tab.
   - Select the following entries from the **Properties** '**Content** menu': **Security → Admin Password → Reset Policy**
   - Select the [**Disable Password Reset**] option and then select the [**Apply**] button to save the option entered.

2. ***Authentication***:

   i. Establish local authentication at the device by following the "Configuring Local Authentication Settings" instructions in Section 4 of the SAG.

   Set up unique user accounts with appropriate privileges on the device for all users who require access to the device by following the "User Database" instructions in Section 4 of the SAG.

   ii. Establish network (remote) authentication access to network accounts by following the "Configuring Network Authentication Settings" instructions in Section 4 of the SAG to set up an Authentication Server.

   In the evaluated configuration the only allowable Authentication Types are **Kerberos (Solaris)**, **Kerberos (Windows)** or **LDAP**.

   When configuring network authentication using LDAP/LDAPS enable SSL by following the instructions in Step 3 for "Configuring LDAP Server Optional Information" under "LDAP" in Section 3 of the SAG, making sure that **Enable SSL (Secure Socket Layer)** under SSL is selected.

   iii. Establish user authentication via a Smart Card by following the "Configuring Smart Card Authentication Settings" instructions in Section 4 of the SAG.

[4]Xerox® WorkCentre® 5945/5955 Multifunction Printer System Administrator Guide, Version 1.0: September 2013.

[5] The instructions for setting up the device in the Evaluated Configuration assume that the System Administrator has been successfully authenticated as a System Administrator at either the Control Panel or Web UI following the instructions in section I.a of this document..

3. ***Authorization***:

   i. Only local authorization is allowed in the evaluated configuration. Establish local authorization at the device by following the "Configuring Local Authorization Settings" instructions in Section 4 of the SAG. Note that local user accounts on the device should be set up first before user permissions are set up.

   Set up user roles and user permissions to access device services and features based on the roles users are assigned by following the instructions for "User Permissions" under "Configuring Authentication Settings" in Section 4 of the SAG.

   ii. Set the permission for all Non-Logged In Users Roles (see "User Roles" in Section 4 of the SAG) to be **Not Allowed**, **Not Allowed & Hidden** or **Never**, as appropriate, for the following: (1) all print permission categories (by following the "Editing Print Permissions for the Non-Logged In Users Role" under "Configuring Authorization Settings" in Section 4 of the SAG) and (2) all services and tools (by following the "Editing Services and Tools Permissions for the Non-Logged In Users Role" under "Configuring Authorization Settings" in Section 4 of the SAG). Also set the

4. ***Personalization***: Enable personalization by following the instructions for "Specifying the Method the Printer Uses to Acquire Email Address of Users" under "Configuring Smart Card Authentication Settings" under "Configuring Authentication Settings" in Section 4 of the SAG. Configure personalization by following the instructions for "Configuring User Mappings" under "LDAP" in Section 3 of the SAG.

5. ***Immediate Image Overwrite***: Follow the instructions under 'Enabling Immediate Image Overwrite at the Control Panel' or 'Enabling Immediate Image Overwrite' in Section 4 of the SAG to enable Immediate Image Overwrite from the Control Panel or the Web UI, respectively.

   Both Immediate Image Overwrite and On Demand Image Overwrite are enabled by default at the factory when the device is first delivered.

6. ***Security Certificates***: Install a digital certificate on the device before enabling SSL by following the appropriate instructions under "Security Certificates" in in Section 4 of the SAG for installing the any one of the digital certificates (Device Certificate, CA Certificate or Trusted Certificate) the device supports.

   Note that a Xerox self-signed certificate is installed by default on the device. 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 Section 4 of the SAG to create the CSR.

7. ***Transport Layer Security (TLS)/Secure Sockets Layer (SSL)***:

   i. Follow the instructions under 'Enabling DND/DDNS Settings the Control Panel' or '"DNS" (under "Configuring IP Settings in CentreWare Internet Services") in Section 3 of the SAG for entering the host and domain names, to assign the machine a valid, fully qualified machine name and domain from the Control Panel or the Web UI, respectively (required for SSL to work properly).

   ii. If a self-signed certificate is to be used download the generic Xerox root CA certificate from the device by following the instructions for saving the certificate file under "Viewing, Saving or Deleting a Certificate" in Section 4 of the SAG and then installing the saved certificate in the certificate store of the System Administrator's browser.

   iii. Enable HTTPS by following the instructions for "Enabling HTTPS (SSL)" under "Secure HTTP (SSL)" in Section 4 of the SAG. Set the 'Force Traffic over SSL' option to be **Yes (all HTTP requests will be switched to HTTPS)**.

   iv. Disable SSLv3.0 in favor of TLS v1.x to avoid vulnerabilities associated with downgrading from TLS to SSLv3.0.

8. ***FIPS 140-2 Mode***: Encryption of transmitted and stored data by the device must meet the FIPS 140-2 Standard. Enable the use of encryption in "FIPS 140 mode" and check for compliance of certificates stored on the device to the FIPS 140-2 Standard by follow the instructions for "Enabling FIPS 140 Mode and Checking for Compliance" in Section 4 of the SAG.

9. ***Data Encryption***: Enable data encryption by following the instructions under "Enabling Encryption of Stored Data" in Section 4 of the SAG; data encryption is enabled by default at the factory when the device is first delivered. Before enabling disk encryption make sure that the device is not in diagnostics mode and that there are no active or pending scan jobs.

10. ***IP Filtering***: Enable and configure IP Filtering to create IP Filter rules by following the instructions under "IP Filtering" in Section 4 of the SAG.

    Note that IP Filtering is not available for either the AppleTalk protocol or the Novell protocol with the 'IPX' filing transport. Also, IP Filtering will not work if IPv6 is used instead of IPv4.

11. ***Audit Log***: Enable the audit log, download the audit log .csv file and then store it in a compressed file on an external IT product using the Web UI by following the appropriate instructions for "Enabling Audit Log" and "Saving an Audit Log", respectively, under "Audit Log" in Section 4 of the SAG.

    Save audit log entries on a USB drive attached to the device via one of the Host USB ports using the Control Panel by following the appropriate instructions for "Saving an Audit Log to a USB Drive" under "Audit Log" in Section 4 of the SAG. 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.

    The System Administrator should download and review the Audit Log on a daily basis. 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.

12. ***IPSec***: Enable and configure IPSec by following the instructions under "IPsec" in Section 4 of the SAG. Note that IPSec should be used to secure printing jobs; HTTPS (SSL) should be used to secure scanning jobs. Use the default values for IPSec parameters whenever possible for secure IPSec setup.

    Note that IPSec can be disabled at the Control Panel by following the instructions for "Disabling IPSec at the Control Panel" under "IPSec" in Section 4 of the SAG. However, if IPSec is disabled the device will no longer be in the evaluated configuration.

13. ***Session Inactivity Timeout***: Enable the session inactivity timers (termination of an inactive session) from the Web UI 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" in Section 4 of the SAG.

14. ***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 by following the instructions under "Configuring Secure Print Settings" in Section 5 of the SAG.

    Make sure 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 Web UI 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) follow the instructions for "Setting Job Type Print Permissions under "Editing Print Permissions for the Non-Logged In Users Role" under "Configuring Authorization Settings" in Section 4 of the SAG, select **Custom** and then 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 "Releasing a Secure Print" or delete the job at the Control Panel by following the directions under "Deleting a Secure Print", both under "Printing Special Job Types" under "Printing Features" in Section 5 of the applicable User Guide[6].

    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, including a secure print job. To ensure that only the System Administrator can delete jobs, from the WebUI follow the instructions for "Editing Services and Tools Permissions for the Non-Logged In Users Role" under "Configuring Authorization Settings" in Section 4 of the SAG and set the entry for 'Delete Jobs' under 'Job Status Pathway' to **Not Allowed** for all defined logged in user roles except the System Administrator and Accounting Administrator roles, which are set to **Allowed** for this entry (non-logged in users should be denied permission to access any device services or features as discussed in I.b.3.ii above).

    Set job deletion to 'System Administrator Only' at the Control Panel by following the instructions for "Setting Job Deletion Options at the Control Panel" in Section 10 of the SAG.

15. ***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** by following the instructions for "Configuring the Hold All Jobs Feature" under "Hold All Jobs" in Section 5 of the SAG.

    Once a held print job has been submitted the authenticated user can either 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 Section 5 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 Section 5 of the applicable User Guide.

[6]Xerox® WorkCentre® 5945/5955 User Guide, Version 1.0: March 2014.

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

16. ***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 Web UI by following the instructions for "Enabling and Configuring 802.1x in CentreWare Internet Services" in Section 4 of the SAG.

17. ***USB Port Security***: Enable or disable the USB Ports using the Web UI by following the instructions for "Enabling and Disabling USB Ports" under "USB Port Security" in Section 4 of the SAG. To enable or disable the USB Ports using the Control Panel follow the instructions for "Enabling or Disabling All USB Ports at the Control Panel" under "USB Port Security" in Section 4 of the SAG

18. ***SFTP Filing***: ***SFTP Filing*** is used in the evaluated configuration. Specify the use of Secure FTP for sending scan or backup job files over the network by following the instructions for "Configuring FTP and SFTP Filing Settings" under "FTP/SFTP Filing" in Section 3 of the SAG.

19. **McAfee Embedded Control**: If use of the Embedded Device Security is desired, from the Web UI check that Embedded Device Security is enabled by following the instructions under "McAfee Embedded Control" in Section 4 of the SAG. If the default Enhanced Security is desired, select the **Enhanced Security** for the 'Security Level'; if the 'Integrity Control' option is desired, select **Integrity Control** for the 'Security Level'. Do not select the **Disable McAfee Secure Device** 'Security Level' option.

    Since Integrity Control is a purchasable option, before the Security Level can be set to **Integrity Control** this option must first be installed on the device; enter the installation key for the Integrity Control option provided by Xerox when the option is purchased in the appropriate step in the instructions under "McAfee Embedded Control" in Section 4 of the SAG.

    To install Integrity Control from the Control Panel perform the following:

    - Press the **Machine Status** button and then the **Tools** tab.
    - Touch **Device Settings** > **General**.
    - Touch **Feature Installation**.
    - Enter the installation key for the Integrity Control option provided by Xerox when the option is purchased in the 'Enter Feature Installation Key' text box.
    - Touch **OK**.

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

- TCP/IP
- Date and Time
- Copy
- Embedded Fax
- Fax Forwarding on Receive (for received Embedded Faxes)
- Scan to E-mail
- Workflow Scanning
- Scan to Mailbox
- Scan to USB
- Print from USB
- 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):

1. ***TCP/IP***:

    - Enable IPv4 and IPv6 from the Control Panel by following either the instructions in "Quick Setup Home" for using the IP Address Settings wizard under Initial Setup at the Control Panel in Section 2 of the SAG or the instructions for "Enabling TCP/IP" under "IP" in Section 3 of the SAG. Configure IPv4 or IPv6 by following the instructions for "Configuring TCP/IP Settings at the Control Panel" under "IP" in Section 3 of the SAG

    - Set up and configure IPv4 and IPv6 from the WebUI by following the instructions for "Configuring IPv4" and "Configuring Settings for IPv6", respectively, under "Configuring IP Settings in CentreWare Internet Services" under "IP" in Section 3 of the SAG.

2. ***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".

     Set the date and time from the Web UI by following the instructions in "Setting the Date and Time in CenterWare Internet Services", both under "Setting the Date and Time " in Section 10 of the SAG. Make sure to set the 'Date and Time Setup' option to be **Manual (NTP Disabled)**.

3. ***Embedded Fax***:

   - Ensure that Embedded Fax is properly installed.
   - Set Embedded Fax parameters and options via the Local User Interface on the machine by following the instructions for "Embedded Fax" in Section 8 of the SAG.
   - Set the minimum length of the (Embedded Fax) secure receive passcode from the Control Panel by performing the following:

     ✓ Press the **Machine Status** button and then the **Tools** tab.
     ✓ Touch **Service Settings** > **Embedded Fax Settings**.
     ✓ Touch **Fax Passcode Length**.
     ✓ Enter the desired minimum secure receive passcode length in the indicated 'Length' text box between 4 and 10 digits.
     ✓ Touch **OK**.

     Set the minimum length of the (Embedded Fax) secure receive passcode from the Web UI by following the instructions for "Configuring Fax Passcode Length" under "Fax Security" under "Embedded Fax" in Section 8 of the SAG.

   - Enable and set (Embedded Fax) Secure Receive passcode from the Control Panel by performing the instructions for "Enabling or Disabling the Secure Fax Feature" under "Fax Security" under "Embedded Fax" in Section 8 of the SAG. Set 'Guest Access' to **Disabled** to prevent unauthenticated users from being able to enable or disable Secure Receive.
   - Enable Fax Forwarding on Receive and establish up to five fax forward rules from the Web UI by following the instructions for "Fax Forwarding" under "Embedded Fax" in Section 8 of the SAG. Only add E-mail addresses to the fax forward rules established by following the instructions for "Adding an Email Address to a Fax Forward Rule".
   - The Mailbox and Polling Policy should be set to delete received faxes when they are printed. Set the Mailbox and Polling Policy by following the instructions under "Defining Mailbox and Polling Policies" under "Embedded Fax" in Section 8 of the SAG. Makes sure the **Delete on Print** option is selected for Received Documents.
   - The Local Polling option and embedded fax mailboxes should not be set up or used at any time.
   - Remote Polling should only be used by the System Administrator.
   - Printing of Embedded Fax confirmation reports is not included in the evaluation. The Embedded Fax cover sheets should not be printed with an Embedded Fax job.

4. ***Scan To Mailbox***:

   a. Enable and configure the Scan to Mailbox feature from the Web UI by following the instructions under 'Enabling or Disabling Scan to Mailbox' in Section 7 of the SAG.

      Establish a unique Scan-to-Mailbox mailbox for each authenticated user.

      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 follow the instructions under "Setting Scan Policies" in Section 7 of the SAG. in the evaluated configuration. Set the scan policies as follows:

      ✓ Deselect **Allow Scanning to Default Public Folder**
      ✓ Deselect **Require per Job password to public folders**
      ✓ Select **Allow additional folders to be created**
      ✓ Select **Require password when creating additional folders**
      ✓ Select **Prompt for password when scanning to private folder**

✓ Deselect **Allow access to job log data**

5. ***Scan to Email***:

- Set the domain filtering to limit the domains to which Scan to E-mail jobs can be sent. Enable the domain filtering option by following the instructions under "Editing Domain and Email Filter Settings" under "Configuring Email Security Settings" under "Scanning to an Email Address" in Section 7 of the SAG.
- Configure encryption and signing of Scan to Email jobs 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 Section 7 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 by following the instructions for "Configuring SMTP Connection Encryption Settings" under "SMTP" in Section 3 of the SAG. Set the 'Email Signing Enablement' option to **Always On; Not Editable by user**.
- Configure authentication of SMTP to send Scan to Email jobs or to forward received Embedded Faxes via email by following the instructions for "Configuring SMTP Authentication Settings" under "SMTP" in Section 3 of the SAG.

6. ***Workflow Scanning***:

- When configuring workflow scanning file repositories (see "Configuring File Repository Settings" under "Workflow Scanning' in Section 7 of the SAG) or template pool repositories (see "Configuring Template Pool Repository Settings" under "Workflow Scanning' in Section 7 of the SAG) set the transfer protocol to be either HTTPS or SFTP.

7. **NTP**:

- If it is desired to use an NTP server to synchronize and set the internal system time used by the device follow the instructions under "NTP" in Section 3 of the SAG.

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

- Reprint from Saved Job
- SMart eSolutions
- Custom Services (Extensible Interface Platform or EIP)
- Network Accounting and Auxiliary Access
- Internet Fax
- Use of Embedded Fax mailboxes
- USB Direct Printing
- AppleTalk and Novell IPX protocols
- Web Services
- Remote Control Panel (a ConnectKey feature)
- SNMPv3

e. 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 disable when complete. Software upgrades can be enabled/disabled by following the instructions for 'Enabling Upgrades' under 'Updating the Printer Software' in Section 10 of the SAG.

II. Secure Acceptance:

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

- Printing out a Configuration Report from the Web UI by following the "Printing the Configuration Report" instructions under "Initial Setup in CentreWare Internet Services" in Section 2 of the SAG, or from the Control Panel by following the "Configuration Report" instructions under "Configuration Page" in Section 3 of the SAG.
- Comparing the software/firmware versions listed on the Configuration Report with the Evaluated Software/Firmware versions listed in Table 2 of the Xerox Multifunction Device Security Target WorkCentre 5945/5955, latest version issued and make sure that they are the same in all cases.
- Following internal customer policies and procedures required to evaluate and install devices in your environment.

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

a. Change the following passcodes on a regular basis, chosen 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)

Passcodes for Scan-to-Mailbox mailboxes should be selected to be as random as possible and should be changed on a regular basis, consistent with applicable internal policies and procedures.

b. Authentication passwords for unique user accounts established for users should be set to a minimum length of 8 (alphanumeric) characters unless applicable internal procedures the System Administrator must comply with require a minimum password of a greater length. The 'Maximum Length' can be set to any value between 8 and 63 (alphanumeric) characters consistent with the same internal procedures. Follow the instructions for "Specifying Password Requirements" under "User Database" under "Configuring Authentication Settings" in Section 4 of the SAG to set the minimum and maximum user authentication password lengths.

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

d. Operation of IIO and ODIO:

1. If a manual ODIO is to be run set up and initiate a manual ODIO as follows:
    - From the Web UI follow the "Manually Deleting Image Data" instructions under "Overwriting Image Data" in Section 4 of the SAG.
    - From the Control Panel follow the "Manually Deleting Image Data at the Control Panel" instructions under "Overwriting Image Data" in Section 4 of the SAG.
2. If a scheduled ODIO is to be run set up and initiate a scheduled ODIO as follows:
    - From the Web UI follow the "Scheduling Routine Deletion of Image Data" instructions under "Overwriting Image Data" in Section 4 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 Section 4 of the SAG.
3. Set the 'Confirmation Report' setting to "On" when setting up a manual or scheduled ODIO from the Control Panel or Web UI so that a Confirmation Report will always be printed upon completion of an ODIO.
4. A Standard ODIO that 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 that 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 an On Demand Image overwrite 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) 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 Web UI the status of the completed ODIO may not appear on the Web UI 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 Web UI 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 WebUI 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.
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.

e. The device supports the use of SSLv2.0, SSLv3.0, RC4 and MD5. However, customers are advised to set the crypto policy of their clients to request TLSv1.x (SSLv3 should be disabled) and to disallow the use of RC4 and MD5. The cryptographic module supports additional ciphers that may be called by other unevaluated functions.

   Using the device in FIPS mode will automatically restrict the device to using SSLv3/TLSv1.x only.

f. When utilizing SSL for secure scanning:
   - ✓ SSL 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 an SSL certificate for a remote SSL repository fails its validation checks the associated scan job will be deleted and not transferred to the remote SSL 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.

g. Audit Log Notes:

   - In viewing the Audit Log the System Administrator should note the following:
     - ✓ Deletion of a file from Reprint Saved Job folders or deletion of a Reprint Saved Job folder itself is recorded in the Audit Log.
     - ✓ 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.
     - ✓ Extraneous process termination events (Event 50) 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) may also be recorded.
   - 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.

h. 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 Web UI. Also, configure IP filtering so that traffic to open ports from external users (specified by subnet

mask) is dropped and so that following ports for web services are closed: tcp ports 53202, 53303, 53404 and tcp/udp port 3702.

i. Initiate the software verification test feature by following the instructions for "Verifying the Software" in Section 4 of the SAG.

j. 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).

k. 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.

l. 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.

m. Users experiencing problems logging in to the device using the Web UI only on a particular web browser are advised to switch to a different web browser.

n. 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.

o. Caution: The device allows an authenticated System Administrator to disable functions like Image Overwrite Security 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.

p. System Administrators should avoid opening emails and attachments from unknown sources unless the emails and attachments have been properly scanned for viruses, malware, etc.

q. System Administrators and users should logoff immediately after using the Web UI. They should also not allow their browser to either save their username/password or "remember" their login. They should also follow secure measures, only use browsers with TLS 1.0 and above and not open any malicious links or documents with their browsers.

IV. Secure Operation of Device Services/Functions Not Part of the Evaluated Configuration

a. 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.

b. SNMPv3 cannot be enabled until SSL and HTTPS (SSL) are enabled on the machine. To enable SNMPv3 follow the instructions for "Configuring SNMPv3" under "SNMP" in Section 3 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].

c. Customers should sign up for the RSS[8] subscription service available via the Xerox Security Web Site (Security@Xerox) at 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.

d. 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.

e. 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 Web UI[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 Web UI. If the 'Self Assigned Address' option is enabled (which is the default case), this secondary IPv4 address will not be visible to the SA[11].

---

[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 http://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.

The 'Self Assigned Address' option from the Web UI ***IP (Internet Protocol)*** page should be disabled unless either APIPA is used or Apple Rendezvous/Bonjour support is required.

f. 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 Web UI show that IPv6 is enabled. IPv6 can be enabled again via the Web UI by first disabling and then re-enabling it.

V. The following windows are available to any authenticated and authorized user from the Local User Interface. 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.

VI. The Web UI provides a set of on-line help pages that provide guidance on most of the Web UI pages. These on-line help pages can be accessed from the Web UI by selecting the [**Help**] button on the upper right hand corner of every Web UI page; the on-line help page corresponding to the Web UI page being viewed will be displayed. There is also a 'TOC' contents list of all Web UI 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 UI with System Administrator login and authentication but are not documented in the SAG, User's Guides or the on-line help:

- **Application Domain/Content Query -** Allows the configuration of the system to perform an LDAP query for the logged-in user's authentication domain prior to authenticating the server. Is accessible by typing **http://{IP Address}**[12]**/diagnostics/index.dhtml** and then selecting '**Authentication Domain/Context Query**' from the **Diagnostics** Content Menu or by typing **http://{IP Address}/diagnostics/authenticationQuery.php**.
- **Scanning Lock Files -** Allows bypassing the filename locking feature. Is accessible by typing **http://{IP Address}/diagnostics/index.dhtml** and then selecting '**Scanning Lock Files**' from the **Diagnostics** Content Menu or by typing **http://{IP Address}/diagnostics/lockFiles.php**.
- **Gray Other Queues Button -** Allows the System Administrator to grey out the 'Other Queue' button on the Control Panel. Is accessible by typing **http://{IP Address}/diagnostics/index.dhtml** and then selecting '**Grey Other Queues Button**' from the **Diagnostics** Content Menu or by typing **http://{IP Address}/diagnostics/hideotherqueuesbutton.php**.
- **Secure Attribute Editor -** Allows the user to change some system attributes related to PDLs (e.g., memory usage, copies per page, etc.). Is accessible by typing **http://{IP Address}/diagnostics/secureattr.dhtml**.
- **Job Log File Format -** Allows the System Administrator to set the XML job log file format. Is accessible by typing **http://{IP Address}/diagnostics/jobLog.dhtml**.
- **File Extension Case -** Allows the System Administrator to select all file extensions to be created in either lower or upper case. Is accessible by typing **http://{IP Address}/diagnostics/fileExtensionCase.dhtml**.
- **Email Security -** Allows the System Administrator to secure the device's email service. Is accessible by typing **http://{IP Address}/diagnostics/emailSecurity.php**.
- **Binary Printing Support -** Allows the device to accept printing jobs that are identified as binary files. Is accessible by typing **http://{IP Address}/diagnostics/binaryAllow.php.**

[12] {IP Address} is the IPv4 address of the machine

- **Postscript Filter PDL Guessing Policy -** Allows the System Administrator to select whether the Postscript Filter guess algorithm will use a strict or loose interpretation. Is accessible by typing **http://{IP Address}/diagnostics/postScriptTokens.php**.
- **Web Services IP Lockout Reset -** Allows the System Administrator to clear the Web Services IP Address Lockout cache. Is accessible by typing **http://{IP Address}/diagnostics/ipLockout.php**.
- **Service Registry Reset -** Allows the System Administrator to reset the device's Service Registry to its default values. Is accessible by typing **http://{IP Address}/diagnostics/registryReset.php**.
- **Job Queue Limit -** Allows the System Administrator to set the maximum number of jobs that can be listed in the device's job queues. Is accessible by typing **http://{IP Address}/diagnostics/jobLimit.php**.
- **Barcode Space Character Interpretation -** Allows the System Administrator to choose how the device renders space characters within barcode fonts. Is accessible by typing **http://{IP Address}/diagnostics/barcodeSpaceToggle.php**.
- **DHCP v6 -** Allows the System Administrator to choose which compliance option will be followed when DHCP v6 is used. Is accessible by typing **http://{IP Address}/diagnostics/ dhcpv6Options.php**.
- **View Service Registry Contents -** Allows the System Administrator to view the contents of the device's Service Registry. Is accessible by typing **http://{IP Address}/diagnostics/viewRegistry.php**.
- **Diagnostics Tree -** Allows the System Administrator to view the selectable list of diagnostics Special Purpose Pages. Is accessible by typing **http://{IP Address}/diagnostics/tree.php**.
- **PCL Advanced Configuration -** Allows the System Administrator to enter the desired PCL advanced configuration paper size code. Is accessible by typing **http://{IP Address}/diagnostics/pclSetup.php**.
- **Control Kerberos Settings –** Allows the System Administrator to control how the device performs Kerberos authentication with a domain controller, LDAP server and other kerberized services as they are developed. Is accessible by typing **http://{IP Address}/diagnostics/kerberosSettings.php**.
- **Download DLM PCL Forms -** Allows the System Administrator to download the DLM PCL forms into the device. Is accessible by typing **http://{IP Address}/diagnostics/dl_pcl.php**.
- **Multiple Pages per JBIG2 Dictionary -** Allows the System Administrator to enable the multiple pages per JBIG2 dictionary feature (for PDF and PDF/A only). Is accessible by typing **http://{IP Address}/diagnostics/disableMultiplePages.php**.
- **Show Web UI Configuration Page -** Allows the System Administrator to enable users who are not authenticated administrators to view the Web UI Configuration Page. Is accessible by typing **http://{IP Address}/diagnostics/ShowConfigSheet.php**.
- **NTLM v2 Response -** Allows the System Administrator to enable the device to send only the NT Lan Manager (NTLM) Version 2 protocol (and refuse the LM & NTLM versions). Is accessible by typing **http://{IP Address}/diagnostics/NTLMSecurity.php**.
- **Custom Size Allowed -** Allows the System Administrator to allow custom size paper to be used for print jobs. Is accessible by typing **http://{IP Address}/diagnostics/customSizeAllowed.php**.
- **Copies Per Page Print Setting -** Allows the System Administrator to permit the use of the copies per page setting for print jobs. Is accessible by typing **http://{IP Address}/diagnostics/copiesPerPage.php**.
- **HTTP SSL Cipher Encryption Strength -** Allows the System Administrator to control the set of supported ciphers when using SSL (e.g., to enforce 128 bit or higher encryption keys). Is accessible by typing **http://{IP Address}/diagnostics/SSLCiphers.php**.
- **Port 9100 Print Stream Filtering -** Allows the System Administrator to enable/disable the filtering of the RAW IP print stream for the occurrence of the PostScript control-T character. Is accessible by typing **http://{IP Address}/diagnostics/Port9100PrintStreamFiltering.php**.
- **Install Software (View Scan Templates Created by WIA Driver) -** Allows the System Administrator to install the #00022121 Network Controller version to view templates created by the Microsoft Windows Image Acquisition (WIA) driver. Is accessible by typing **http://{IP Address}/diagnostics/00022121.dhtml**. The System Administrator should be aware that installing this Network Controller version will result in the device no longer being in the evaluated configuration.
- **Cost Control Enablement and Receipt Printing Setup -** Allows the System Administrator to enable the Cost Control feature when Secure Access and network accounting are enabled. Is accessible by typing **http://{IP Address}/diagnostics/CostControl.php**.

  Note: This page will only be accessible if network accounting is enabled, so it will not be displayed for a device in the evaluated configuration.

- **Scan Image Compression -** Allows the System Administrator to manage the asymmetric sub sampling options of scan image processing. Is accessible by typing **http://{IP Address}/diagnostics/asymmetricSubSample.php**.
- **Enable Scanning Multithread Processing -** Allows the System Administrator to manage the enablement for multithread scan image processing. Is accessible by typing **http://{IP Address}/diagnostics/multiThreadingEnableDisable.php**.
- **TIFF Rotation for Scan to Email -** Allows the System Administrator to enable a special TIFF rotation when processing Scan to Email jobs that saves time and processing power. Is accessible by typing **http://{IP Address}/diagnostics/enableTIFFRotation.php**.
- **Port 9100 Parse PDF Format -** Allows the System Administrator to enable the printing of PDF files over Port 9100 that have added data to the beginning or the end of the file. Is accessible by typing **http://{IP Address}/diagnostics/Port9100ParsePDF.php**.
- **Enable/Disable Selective Spooling -** Allows the System Administrator to enable or disable Selective Spooling that sends incoming print jobs directly to the PDL interpreter and bypassing the spooling to disk step. Is accessible by typing **http://{IP Address}/diagnostics/SelectiveSpooling.php**.
- **Certificate Signing Request -** Allows the System Administrator to configure the Certificate Signing Request (CSR) feature on the device to not include the device's IPv4 address as the Common Name (CN) entry in the 'Subject' field so the CSR has only a single CN entry. Is accessible by typing **http://{IP Address}/diagnostics/singleCN.php**.

VII. The following pages are available from the Web User Interface with no user login and authentication required:

- **Site Map** - Provides the user with hyperlink pointers to each Web User Interface screen organized by Web UI tab. Is accessible by selecting the [**Site Map**] button in the upper right hand corner of every Web User Interface page.
- **Exit from Sleep Mode** – Automatically informs the user, when the Network Controller is in 'Sleep Mode' at the time the user attempts to make a change to current settings on a Web User Interface web page, that the Network Controller needs to be taken out of 'Sleep Mode' before the requested changes can be made.

VII. 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.

Contact

For additional information or clarification on any of the product information given here, contact Xerox support.

Disclaimer