Version 1.3
Nov 09, 2015

Supplemental Guide -- Secure Installation and Operation of Your WorkCentre™ 7535/7556

Supplemental Guidance - Secure Installation and Operation of Your WorkCentre® 7535/7556

Purpose and Audience

This supplemental guide provides additional information on the secure installation and operation of a WorkCentre 7535/7556 Multifunction System not contained in the Secure Installation and Operation of Your WorkCentre. 7525/7530/7535/7545/7556 document. All customers, but particularly those concerned with secure installation and operation of the machines, should follow these guidelines.

Overview

This document lists some important customer information and guidelines that will ensure that your WorkCentre 7535/7556 device is operated and maintained in a secure manner.

Background

Customers are advised that changes to the evaluated configuration may be required to support business goals and for 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[1]. 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[2]. 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. Make sure that system software release 061.121.225.14700 and patch 761522v1[3] are installed on the device.

b. Set up and configure the following security protocols and functions in the evaluated configuration:

- Immediate Image Overwrite (IIO)
- On Demand Image Overwrite (ODIO)
- 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 or Remote Authorization
- User Permissions
- Personalization
- 802.1x Device Authentication
- Session Inactivity Timeout
- USB Port Security
- SFTP Filing
- Embedded Fax Secure Receive

---

[1] 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.

[2] Xerox Multi-function Device Security Target WorkCentre 7535/7556, Latest Version issued

[3] The zip file containing system software release 061.121.225.14700 and patch 761522v1, along with the applicable installation instructions, can be obtained from http://www.support.xerox.com/support/workcentre-7545-7556/file-download/enus.html?contentId=132892.

.

- Secure Print
- Hold All Jobs

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" located on page 19 in the 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 the "System Administrator Access at the Control Panel" instructions located on page 17 in the SAG.

II. Follow the instructions located in the SAG in Chapter 4, Security 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. Also note that in the evaluated configuration IPv6 is disabled.

1. ***Administrator Password***:

   Change the Administrator password as soon as possible. Reset the Tools 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 Tools password, follow the "Changing the System Administrator Password" instructions on page 19 in the SAG.

   Disable the Admin Password Reset security feature will be disabled 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.

   Follow the "Specifying Password Requirements" instructions on page 62 in the SAG to set the minimum and maximum user authentication password lengths.

2. ***Authentication***:

   i. Establish local authentication at the device by following the "Setting Up Local Authentication" 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 Information" instructions in Section 4 of the SAG.

   ii. Establish network (remote) authentication access to network accounts by following the "Network Authentication" 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)** or **Kerberos (Windows)**. Network authentication using LDAP is not part of the evaluated configuration and should not be used.

   iii. Establish user authentication via a Smart Card by following either the "Setting UP Authentication for a Smart Card System" instructions in Section 4 of the SAG or follow the instructions in the Smart Card Guide[5].

3. ***Authorization***:

   Only local authorization is allowed in the evaluated configuration.

[4]Xerox® WorkCentre® 7525/7530/7535/7545/7556 System Administrator Guide, Version 1.1: March 2011

[5] Xerox® Smart Card Xerox® WorkCentre® 7525/7530/7535/7545/7556, Version 4.0: September 2011

Local Authorization

i. Establish local authorization at the device by following the "Setting Up Local Authorization" 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 "Editing the Role for Non-Authenticated Users" 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).

Network Authorization

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

4. ***Personalization***: To enable personalization perform the following:
   - On the Login Methods page, next to Acquired Logged-in User's Email Address, click **Edit**.
   - Under Acquire logged-in user's email address from, select an option:
     - **Auto** instructs the printer to attempt to acquire the email address of the user from the Smart Card. If an email address is not associated with the Smart Card, the printer searches the Network Address Book. If an email address is not found, the printer uses the email address specified in the From Field. Edit From Field settings on the Required Settings tab of the Email Setup page.
     - **Only Smart Card** instructs the printer to acquire the email address of the user from the Smart Card.
     - **Only Network Address Book (LDAP)** instructs the printer to search the Network Address Book to acquire the email address of the user.
   - To configure LDAP server settings, under Server Configuration, next to Network Address Book (LDAP), click **Edit**.
   - To enable or disable Personalization, under Feature Enablement, next to Acquire Email from Network Address Book, click **Enable Personalization** or **Disable Personalization**.
   - Click **Save**.

   Configure personalization by following the instructions for "Configuring LDAP User Mappings" under "LDAP" in Section 3 of the SAG.

5. ***Immediate Image Overwrite***: Follow the instructions 'Enabling Immediate Image Overwrite' in Section 4 of the SAG to enable Immediate Image Overwrite from the Web UI. To enable Immediate Image Overwrite from the Control Panel, perform the following:
   - At the printer control panel, press the **Machine Status** button, then touch the **Tools** tab.
   - Touch **Security Settings>Image Overwrite Security**.
   - Touch **Job Overwrite**.
   - Touch **Enable**.
   - Touch **OK**.

   Immediate Image Overwrite is enabled by default at the factory when the device is first delivered.

6. **On Demand Image Overwrite**: Follow the instructions 'Manually Deleting Image Data' under Overwriting Image Data in Section 4 of the SAG to enable a manual On Demand Image Overwrite (i.e., an On Demand Image Overwrite initiated immediately by the System Administrator) from the Web UI; follow the instructions 'Scheduling Routine Deletion of Image Data' under Overwriting Image Data in Section 4 of the SAG to enable a scheduled On Demand Image Overwrite from the Web UI.

   To enable a manual On Demand Image Overwrite from the Control Panel, perform the following:

- At the printer control panel, press the **Machine Status** button, then touch the **Tools** tab.
- Touch **Security Settings>Image Overwrite Security**.
- Touch **Disk Overwrite Now**.
- To change the overwrite mode, touch **Overwrite Mode**, then touch an option.
- To set the printer to print a confirmation report after it overwrites data, touch **Confirmation Report**, then select an option.
- Touch **Overwrite Now**.

Note: Depending on how many files are being deleted, the printer can be offline for up to 60 minutes during the deletion process.

- To acknowledge the message and start the process, touch **Overwrite Now**.

Manual On Demand Image Overwrite is also enabled by default at the factory when the device is first delivered.

7. ***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.

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

   i. Follow the instructions under 'Configuring 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 TLS/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.

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

9. ***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 following the instructions for "Enabling FIPS 140 Mode and Checking for Compliance" in Section 4 of the SAG.

10. ***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 WorkCentre 7535/7556 is not in diagnostics mode and that there are no active or pending scan jobs.

11. ***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.

    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.

12. ***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.

    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 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.

13. ***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 performing the following:
    - At the printer control panel, press the **Machine Status** button, then touch the **Tools** tab.
    - Touch **Security Settings>IPsec**.
    - Touch **Disable IPsec**.

    However, if IPSec is disabled the device will no longer be in the evaluated configuration.

    IPsec can be enabled in the CentreWare Internet Services only.

14. ***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 performing the following:
    - At the printer control panel, press the **Machine Status** button, then touch the **Tools** tab.
    - Touch **Device Settings>Timers>System Timeout**.
    - Specify the time the printer waits to log out an inactive user at the control panel. Next to Timeout (Mins), and Timeout (Secs), touch the arrows.
    - To instruct the printer to display a warning message before it logs a user out of the touch screen, under Warning Screen, touch **Enabled**.
    - Touch **Save**.

15. ***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 performing the following:
    Configuring Secure Print Device Policies
    - To access the Secure Print page, click **Properties>Services>Printing>Secure Print**, or click **Security>Secure Print**.
    - Click the **Device Policies** tab.
    - To reveal or hide the characters in job names with asterisks, on the Device Policies tab, under Conceal Job names, select the desired option.

      Note: When a Secure Print job is sent to the printer, by default, the job name appears in the list of jobs on the control panel touch screen. The characters in the job name are shown as asterisks to hide the title of the document that is being printed.
    - Under Release Policies for Secure Print Jobs Requiring Passcode When the User is Already Logged In, select an option:
      - **Release Jobs Without Prompting for Passcode** allows users who are logged in to release a Secure Print job without typing a password.
      - **Prompt for Passcode Before Releasing Jobs** requires users who are logged in to type a password to release the job.
    - Click **Apply**.

    Configuring Secure Print Driver Defaults
    - On the Secure Print page, click the **Print Driver Defaults** tab.
    - On the Print Driver Defaults tab, under Method, select a method for releasing a Secure Print job.
      - **User ID** requires users to log in at the control panel to release their Secure Print jobs.
      - **Passcode** requires users to type a passcode to release a Secure Print job at the control panel.
    - Type a number from 4 through10 to specify the length of the Secure Print password.
    - Click **Apply**.

    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 the Role for the Non-Logged In Users" under "User

Permissions" 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" under "Printing Special Job Types" under "Printing Features" in Section 5 of the User Guide[6].

To delete a secure print job at the Control Panel perform the following:

- At the control panel, press the **Job Status** button.
- Touch the **Secure Print Jobs** or **My Secure Jobs** tab.
- Touch the folder that holds the secure print job.
- Enter the passcode number that you assigned to the print job using the keypad.
- Touch the corresponding print job in the list, then touch **Delete**.

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 perform the following:

- In CentreWare Internet Services, click **Properties>Security>Authentication**.
- Click **Tools & Feature Access**.
- Under Presets, select an option.
- If you selected Custom Access, under Role State, for each service or tool in the list, select **Unlocked** or **Locked**.
- To hide a service icon on the printer touch screen, select **Hidden**.
- Click **Apply**.

Select "Custom Access" under Presets and then set the entry for 'Job Deletion (Active Queue Only)' under 'Job Status Pathway' to "Administrator Only'.

Set job deletion to 'System Administrator Only' at the Control Panel by performing the following:

- At the printer control panel, press the **Machine Status** button, then touch the **Tools** tab.
- Touch **Security Settings>Job Deletion**.
- Set Job Deletion to **System Administrator Only**.
- Touch **Save**.

16. ***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 release the job for printing at the Control Panel by performing following:

    - At the control panel, press the **Job Status** button.
    - Touch **Active Jobs**.
    - To determine why the job was held, touch the job, then touch **Details**.
    - Do one of the following:
        - To release a held job, touch the job, then touch **Release**.
        - To release all held jobs, touch **Release All Jobs**.

    To delete a held job at the Control Panel:

    - At the control panel, press the **Job Status** button.
    - Touch **Active Jobs**.
    - touch the job, then touch **Delete**.

    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.

17. ***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.

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

[6]Xerox® WorkCentre® 7500 Series User Guide, Version 1.1: March 2011.

18. **USB Port Security**: Enable or disable the USB Ports using the Web UI by following the instructions for "Enabling or Disabling USB Ports" under "USB Port Security" in Section 4 of the SAG.

19. ***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:
    - In CentreWare Internet Services, click **Properties>Connectivity>Setup**.
    - Under Protocol, next to FTP/SFTP Filing, click **Edit**.
    - To configure FTP or SFTP filing settings for each service listed under Within Services, click the link.
    - Under Mode, select an option:
      - **Passive** mode transfers data over a random port specified by the FTP server from a connection made from the printer.
      - **Active** mode transfers data over a fixed, known port from a connection made from the server.
    - Click **Save**.

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, including email encryption and signing
- Workflow Scanning
- NTP
- SMB Filing
- Scan to Mailbox
- Scan to USB
- Print from USB
- Print from Mailbox

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 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 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 from the WebUI by following the instructions for "Configuring IPv4" under "Configuring IP Settings in CentreWare Internet Services" under "IP" in Section 3 of the SAG.

   In the evaluated configuration IPv6 should be disabled.

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" in Section 10 of the SAG and 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.

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 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:
  - In CentreWare Internet Services, click **Properties>Services>Fax>Setup>Security**.
  - To configure fax passcode options, next to Fax Passcode Length, click **Edit**.
  - To set the passcode length, use the arrows.
  - Click **Save**.
- 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 "Fax Polling" 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***:

- 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.
- 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 will have their passwords reset to the password in the clone file.
- 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***:

- Configure encryption and signing of Scan to Email jobs as follows:

  Before you begin:
  - Configure Smart Card Authentication. For details see 1.b.2.iii.
  - Ensure that signing certificates are installed on all Smart Cards.

  - In CentreWare Internet Services, click **Properties>Security>Authentication>Setup**.
  - To edit encryption and signing settings, under 'Email Encryption/Signing', click **Edit**
  - On the Email Encryption/Signing page:
    - To enable Email Encryption, under Email Encryption Enablement, select an option:
      - **Always On; Not editable by user** restricts users from turning off Email Encryption at the control panel.
      - **Editable by user** allows users to turn Email Encryption on or off at the control panel.

      In the evaluated configuration set the 'Email Encryption Enablement' option to **Always On; Not Editable by user**

      If you select Editable by user, select the default setting for users at the control panel. Under Email Encryption Default, select **On** or **Off**.

- Under Encryption Algorithm, select an encryption method.
- To enable Email Signing, on the Signing tab, under Email Signing Enablement, select an option:
  - **Always On; Not editable by user** restricts users from turning Email Signing off at the control panel.
  - **Editable by user** allows users to turn on or off Email Signing at the control panel.

  If you select Editable by user, select the default setting for users at the control panel. Under Email Signing Default, select **On** or **Off**.
- Under Signing Hash, select a method.
- Click **Apply**.

- Configure encryption of Scan to Email jobs sent from the device over SMTP by:
  - In CentreWare Internet Services, click **Properties>Connectivity>Setup**.
  - Under Protocol, next to SMTP (Email), click **Edit**.
  - On the SMTP (Email) page, click the **Connection Encryption** tab
  - To encrypt SMTP communication, under **Encryption Mechanism used by the multifunction device when communicating with the SMTP server**, select a method that your server supports.
  - Click **Apply**.

  Note that in the evaluated configuration the [**SSL/TLS**] option should be selected.

- Configure authentication of SMTP to send Scan to Email jobs or to forward received Embedded Faxes via email by performing the following:
  - In CentreWare Internet Services, click **Properties>Connectivity>Setup**.
  - Under Protocol, next to SMTP (Email), click **Edit**.
  - On the SMTP (Email) page, click the **SMTP Authentication** tab.
  - Under SMTP Login credentials applied to email jobs sent from the machine's touch interface, select an option:
    - **None** does not require the printer to provide the server a user name or password.
    - **System** uses the information provided in the Login Name and Password Fields to access the server.

      Enable **Select to save new password** to update the password for an existing Login Name.
    - **Authenticated User** uses the credentials of the authenticated user to access the server.

      If network authentication is configured to use a Kerberos server, and you want to use Kerberos tickets, under Use Kerberos tickets, select **Always**.
  - Under SMTP Login credentials for the machine to Access the SMTP Server to send automated emails, select an option:
    - **None** does not require the printer to provide the server a user name or password.
    - **System** uses the information provided in the Login Name and Password Fields to access the server.

      Enable **Select to save new password** to update the password for an existing Login Name.
  - Click **Apply**.

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.

8. **SMB Filing**:

   - If SMB Filing is desired to specify Kerberos authentication options when filing images to SMB-shared network locations, follow the instructions for "SMB Filing" in Section 3 of the SAG.

9. **Scan to Mailbox**:

    - To set up scanning to a mailbox folder on the printer is desired, follow the instructions for "Scanning to a Folder on the Printer" in Section 7 of the SAG.

10. **Scan to USB:**

    - To enable/disable Scan to USB on the device follow the instructions for "Scan to USB" in Section 7 of the SAG.

11. **Print from USB:**

    - To enable printing from USB on the device, follow the instructions for "Enabling Print from USB" in Section 5 of the SAG.

12. **Print from Mailbox:**

    To enable the Print from Mailbox feature from the Web UI perform the following:
    - In CentreWare Internet Services, click **Properties>Services**.
    - Click **Print From > Print From Mailbox**.
    - Under **Print From Mailbox**, select **Enabled**.
    - Click **Apply**.

c. 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
- SNMPv3
- IPv6
- Software Verification Self-Test

d. 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 "Configuration Report" instructions under "Initial Setup at the Control Panel" in Section 2 of the SAG.
- Comparing the software/firmware version listed on the Configuration Report with the Evaluated Software/Firmware versions listed in Table 2 of the Xerox Multi-Function Device Security Target WorkCentre 7535/7556, latest version issued and make sure that they are the same.
- Following internal customer policies and procedures required to evaluate and install devices in your environment.

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

a. Change the following passcodes on a regular basis, chose passcodes to be as random as possible and set 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. In the evaluated configuration the System Administrator should ensure that all pathways and services are 'Locked' so that they can be accessed only by authenticated users. Follow the instructions in the 'Controlling Access to Tools and Features' under Local Authentication under Setting Up Access Rights in Section 4 of the SAG to lock all pathways and services.

c. 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.

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

e. Operation of IIO and ODIO:

- 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.
- 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.
- Immediate Image Overwrite of a delayed or secure print job will not occur until after the machine has printed the job.
- If an Immediate Image Overwrite 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.
- 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.
- 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 invoke a full ODIO once the machine has been restored.
- Once a manual or scheduled ODIO has been initiated it cannot be aborted.
- 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) [3].
  - 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.
- 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.
- 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.
- 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.
- If there is a failure in the hard disk drive a message recommending that an ODIO be run will appear on the Control Panel. An Immediate Image Overwrite Error Sheet will also be printed but may contain incomplete status information. Immediately perform the requested ODIO.
- The time shown on the On Demand Overwrite progress screen displayed on the Control Panel may not reflect Daylight Savings Time.

- 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.
- Perform a Full ODIO immediately before the device is decommissioned, returned, sold or disposed of.

f. The device supports the use of SSLv2.0, SSLv3.0, RC4 and MD5. However, customers are advised to set the cyrpto policy of their clients to request either TLSv1.x (SSLv3 should be disabled) and to disallow the use of RC4 and MD5. Security functions in the evaluated configuration make use of cryptographic ciphers listed in Table 22 of the Security Target. 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 TLSv1.x only.

g. When utilizing Secure Sockets Layer (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.

h. As part of the evaluated configuration, encryption of transmitted and stored data by the device must meet the FIPS 140-2 Standard. To 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 follow the instructions on page 76 of the SAG.

Note that the Mocana crypto module that implements IPSec and Disk Encryption was validated for the operating environment that corresponds to the one used on this product. However, as of this date the operating environment used on this product differs in terms of Linux flavor and CPU from that which the OpenSSL crypto module that implements SSL was validated against. Xerox is claiming vendor affirmation for OpenSSL as per FIPS Implementation Guidance (IG G.5).

i. 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 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.

j. 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 also filtered: tcp ports 53202, 53303, 53404 and tcp/udp port 3702.

l. 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).

m. 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.

k. 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 certified configuration.

l. 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.

m. 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.

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

o. System Administrators and users should:

- Whenever possible use a browser to access the WebUI whose only purpose is to access the WebUI.
- Always logoff the browser immediately after completing any tasks associated with accessing the WebUI.
- Not allow the browser to either save their username/password or "remember" their login.
- Follow secure measures, only use browsers with TLS 1.0 and above and not open any malicious links or documents with their browser.

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

1. 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.

2. 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 Chapter 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].

3. 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.

4. 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.

5. Depending upon the configuration of the device, two IPv4 addresses, a primary IPv4 address and a secondary IPv4 address, may be utilized. The System Administrator selects 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]. 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.

6. 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.

7. A unique Scan-to-Mailbox mailbox should be established for each authenticated user.

8. Initiate the software verification test feature by performing the following from the Web UI:
   - Select the **Properties** tab.
   - Select the following entries from the **Properties** '**Content** menu': **Security** > **Software Verification Test**.
   - Select the [**Start**] button to initiate the software verification test.

   Note that the software verification test function will fail if one or more patches are installed on the device as is the case here for the evaluated configuration.

---

[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 can not 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 Local UI.

[11] The primary IPv4 address will always be displayed on the Configuration Report that can be printed for the device.

V. The following security-relevant window is available from the Local User Interface with System Administrator login and authentication. This window provides standard system configuration or job management capability:

- **Host Name** – Allows the System Administrator to specify the IP host name used by the device as part of the Quick Setup Home process for setting up the device's IP address. Is accessible by following the instructions under 'Accessing the Quick Setup Wizards' on page 4 of the User Guide Supplement for IP Address Settings and then follow the instructions of the Quick Setup Wizard.

VI. 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.
- **Enabling/Disabling Secure Receive** – An authenticated user with the secure receive passcode can enable or disable Secure Receive as follows:
  - At the control panel, press the Machine Status button and then the following buttons in sequence – [**Tools**] → [**Device Pathway**] → [Fax Secure Receive Enablement].
  - Use the keypad to enter the secure receive passcode number and then touch the [**Enter**] button.
  - On the resultant screen touch either [Enable] or [Disable] as desired and then touch the [**Save**] button .
- **Releasing All Secure Receive Jobs** – An authenticated user with the secure receive passcode number can release all received Embedded Faxes as follows:
  - At the control panel, press Job Status button.
  - From the **Active Jobs** tab touch any one of the incoming received Embedded Fax listed.
  - Touch the [**Release All**] button .
  - Use the keypad to enter the secure receive passcode number and then touch the [**Enter**] button.
- **Workflow Scanning Authentication Required** – Allows a user to enter the proper user credentials for a workflow scanning job being sent to a network destination that requires user login. Is accessible by selecting the following screens/buttons in order: [**Services Home**] hard button → [**Workflow Scanning**] button → [**Start**] hard button when a user is submitting a workflow scanning job to a network destination that requires user login → [**OK**] button.
- **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, Internet 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 Local UI screen until either a manual or a scheduled On Demand Overwrite is initiated.
- **User Interface Diagnostics** - Allows the user to run diagnostics on the User Interface software. Is accessible by pressing the machine hard buttons '**Dial Pause**' + '*****' + '**#**' in that order.
- **Automatic Maintenance** – Provides a notice to a user when automatic maintenance of the Internal Marking Engine on the device to perform print quality diagnostics and calibration is being performed. Applicable screens will be displayed to indicate when this automatic maintenance is about to start and is in progress; the user has the option to cancel the automatic maintenance by selecting the [**Cancel**] button on the screen that appears when automatic maintenance is about to start.

VII. 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:

- **Certificate Key Length** - Allows the System Administrator to define the minimum encryption key length. Is accessible by selecting the **Properties** tab and then selecting the following entries from the Properties 'Content menu': **Security → Security Certificates -> Certificate Key Length**.
- **E-mail Encryption and Signing** – Allows the System Administrator to set up encryption for e-mails sent from the device over SMTP. Is accessible only after Smart Card use has been installed and enabled by selecting the **Properties** tab and then selecting from the Properties 'Content menu': { Either (1) **Security → Authentication → Setup** when Authentication, Authorization & Personalization (AA&P) is not being set up for the first time or (2) **Security → Authentication → Setup →** [**Save**] button from the *Authentication, Authorization and Personalization* page when AA&P is being set up for the first time or after AA&P methods have been updated } → **Edit** hyperlink from the 'E-mail Encryption / Signing' row in the table on the page.
- **LDAP Policy** - Allows the System Administrator to set the use of Simple Authentication and Security Layer (SASL) to authenticate and encrypt LDAP. Is accessible by selecting the **Properties** tab and then selecting the following entries from the Properties 'Content menu': { Either **Connectivity → Protocols → LDAP** or **Security → Authentication → Setup →** Edit hyperlink under 'Actions' from the **LDAP Servers** line } → [**LDAP Policies**].
- **Acquiring an Authenticated User's E-mail Address** - Allows the System Administrator to set how an authenticated user's e-mail address is acquired. Is accessible by selecting the **Properties** tab and then selecting the following entries from the Properties 'Content menu': { Either (1) **Security → Authentication → Setup** when AA&P is not being set up for the first time or (2) **Security → Authentication → Setup →** [**Save**] button when AA&P is being set up for the first time or after the AA&P methods have been updated } → **Edit** hyperlink from the 'Acquiring Logged In User's E-mail Address' row in the table.
- **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.
- **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.dhtml**.
- **Gray Other Queue Button -** Allows the System Administrator to grey out the 'Other Queue' button on the Local UI. 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 Print Alphanumeric PIN -** Allows the System Administrator to set the secure print PIN to be alphanumeric characters instead of just digits. Is accessible by typing either **http://{IP Address}/diagnostics/index.dhtml** and then selecting '**Secure Alphanumeric PIN**' from the **Diagnostics** Content Menu or by typing **http://{IP Address}/diagnostics/secureprintalphanumericpin.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**.
- **Suppress Job Name -** Allows the System Administrator to suppress displaying the job name on the Banner Page when submitting a print job. Is accessible by typing **http://{IP Address}/diagnostics/jobNameSuppress.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.**
- **XSA Reports with User IDs -** Allows the device to generate Xerox Standard Accounting reports with User IDs. Is accessible by typing **http://{IP Address}/diagnostics/enableUserID.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**.
- **Filename Extension -** Allows the authorized user to select all filename extensions to be created in either lower case or upper case. Is accessible by typing **http://{IP Address}/diagnostics/fileExtensionCase.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**.
- **Color Copy Control Test Result -** Allows the System Administrator to view the Color Copy Control test results. Is accessible by typing **http://{IP Address}/diagnostics/testResult.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**.
- **Print Behavior Settings -** Allows the System Administrator to configure/enable alternate media dimension settings for print jobs. Is accessible by typing **http://{IP Address}/diagnostics/alternateMedia.php**.
- **Show WebUI Configuration Page -** Allows the System Administrator to enable users who are not authenticated administrators to view the WebUI Configuration Page. Is accessible by typing **http://{IP Address}/diagnostics/ShowConfigPage.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**.
- **Display CAC/PIV Feature -** Allows the System Administrator to enable the display of the CAC/PIV feature. Is accessible by typing **http://{IP Address}/diagnostics/enableCAC.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**.
- **Color Preset Screen -** Allows the System Administrator to enable/disable the "Color Preset Screen" feature before a copy job. Is accessible by typing **http://{IP Address}/diagnostics/ColorPresetScreen.php**.
- **CRU Low/Reorder Message Suppression -** Allows the System Administrator to set whether the CRU Low/Reorder messages are enabled/disabled. Is accessible by typing **http://{IP Address}/diagnostics/CRULowReorderMessageSuppression.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 certified configuration.

VIII. 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.

IX. 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 certified configuration.

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

Disclaimer
The information provided in this Xerox Product Response is provided "as is" without warranty of any kind. Xerox Corporation disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall Xerox Corporation be liable for any damages whatsoever resulting from user's use or disregard of the information provided in this Xerox Product Response including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Xerox Corporation has been advised of the possibility of such damages. Some states do no allow the exclusion or limitation of liability for consequential damages so the foregoing limitation may not apply.