Version 1.1
May 10, 2015

Secure Installation and Operation of Your WorkCentre™ 4265

Secure Installation and Operation of Your WorkCentre® 4265

Purpose and Audience

This supplemental guide provides information on the secure installation and operation of a WorkCentre 4265 Multifunction System. 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 4265 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. 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
- Local, Remote or Smart Card Authentication
- Local or Remote Authorization
- Personalization
- 802.1x Device Authentication
- Session Inactivity Timeout
- USB Port Security
- Software Verification Self-Test
- Secure Print

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 or Local User Interface (denoted hereafter in this document as the Control Panel) as an authenticated System Administrator, follow the instructions under "Accessing CentreWare Information Services as a System Administrator" or "Accessing the Control Panel as a System Administrator", respectively, under "Accessing Administration and Configuration Settings" in Section 2 of the applicable System Administration Guide (SAG)[3].

b. 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

[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 4265, Latest Version issued

[3]Xerox® WorkCentre® 4265 Multifunction Printer System Administrator Guide, Version 1.0: October 2014.

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

2. ***Authentication***:

   i. Establish local authentication at the device by following the instructions for "Configuring Local Authentication Settings" 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 "Adding User Information to 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 (Unix, Linux)**, **Kerberos (Windows ADS)** or **LDAP**.

      When configuring network authentication using LDAP/LDAPS enable SSL by following the instructions in Step 6 for "Editing LDAP Server Information" under "LDAP" in Section 3 of the SAG, making sure that 'Secure LDAP with SSL' is enabled.

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

3. ***Authorization***:

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

   Local Authorization

   i. Establish local authorization at the device by following the instructions for "Adding User Information to the User Database" in Section 4 of the SAG.

   ii. Set the permission for all Non-Logged In Users Roles (see "Configuring User Roles" in Section 4 of the SAG) to be either **Not Allowed** or **Not Allowed & Hidden**, as appropriate, for all listed services and pathways.

   Network Authorization

   i. Establish remote authorization using LDAP by following the "Configuring Authentication Server Settings for LDAP" instructions in Section 4 of the SAG.

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

4. ***Personalization***: To enable personalization perform the following:

   - In CentreWare Internet Services, click **Properties > Login/Permissions/Accounting**.
   - Click **Login Methods**.
   - Select either **Local Authentication** or **Network Authentication**.
   - Select the **Retrieve Profile Information for Authenticated User from LDAP** checkbox.
   - Click **Save.**

   Configure personalization by following the instructions for "Editing LDAP Server Information" under "LDAP" in Section 3 of the SAG.

5. ***Immediate Image Overwrite***: Follow the instructions for 'Enabling Immediate Image Overwrite' in Section 4 of the SAG to enable Immediate Image Overwrite from the Web UI.

   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 for ‘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.

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

Manual On Demand Image Overwrite is not 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 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” under “Security Certificates” 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 DNS Settings the Control Panel’ or ‘”IPV4” 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. Enable HTTPS by following the instructions for “Enabling HTTPS (SSL)” under “Secure HTTP (SSL)” in Section 4 of the SAG.

   iii. 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***: Data encryption is enabled by default on the device and there is no mechanism to disable data encryption from either the Control Panel or Web UI.

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 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 .txt file and then save it in a compressed file on an external IT product using the Web UI by following the appropriate instructions under “Audit Log” in Section 4 of the SAG. Note that HTTPS needs to be enabled in order to download the audit log.

    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.

    There is the possibility that on an intermittent basis multiple entries may be included in the audit log for the same event.

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”, both under System Timeout in Section 4 of the SAG.

14. ***Secure Print***: Set the Secure Print passcode length by following the instructions under “Configuring Secure Print Settings” in Section 5 of the SAG.

    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.

    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" or delete the secure print job at the Control Panel by following the instructions under "Deleting a Secure Print", both under "Printing Special Job Types" under "Printing Features" in Section 5 of the User Guide[4] .

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** > **General Services > Job Management**.
- Under Job Deletion, select the **Administrators Only** option.
- Click **Apply**.

15. ***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**.**

16. **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.

17. ***Software Verification Self-Test***: 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

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
- SNTP
- Scan to USB
- Print from USB

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 the instructions for "Enabling TCP/IP" under "TCP/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 "TCP/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 performing the following:

[4] Xerox® WorkCentre® 4265 Multifunction Printer User Guide, Version 1.0: October 2014.

- At the printer control panel, press the **Machine Status** button, then touch the **Tools** tab.
- Touch **Device Settings**, then touch **General**.
- Touch **Set Zone, Date, Time**.
- Select the applicable time zone and touch **Next**.
- Set the date format option and touch **Next**.
- Set the month, day and year and touch **Next**.
- Set the time (hour and minutes).
- Click **Done.**

Set the date and time from the Web UI by performing the following:

- In CentreWare Internet Services, click **Properties** > **General Setup**.
- Click **Date and Time**.
- Select the applicable time zone, select the date and time format option and set the date (month, day, year) and time (hour and minutes).
- Click **Apply.**

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 “Fax” in Section 8 of the SAG.

- Enable and set (Embedded Fax) Secure Receive passcode from the Control Panel by following the instructions for “Setting Incoming Fax Defaults” under “Setting Fax Defaults” under “Fax” in Section 8 of the SAG

- Enable Fax Forwarding on Receive and establish up fax forward rules from the Web UI by following the instructions for “Fax Forwarding” under “Fax” in Section 8 of the SAG. Only add E-mail addresses to the fax forward rules established by setting the ‘Forward To’ option to **Email Address**.

- 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 reports is not included in the evaluation.

4. ***Scan to Email***:

- Configure encryption and signing of Scan to Email jobs by following the instructions for “Configuring Email Security Settings” under “Email” in Section 7 of the SAG.

- Configure authentication and encryption of SMTP to send Scan to Email jobs or to forward received Embedded Faxes via email by following the instructions in “Configuring SMTP Server Settings” under “Email” in Section 7 of the SAG.

6. ***Workflow Scanning***:

- To configure a file repository for Workflow Scanning follow the instructions for “Configuring File Repository Settings” under “Workflow Scanning” in Section 7 of the SAG

- To configure a template pool repository perform the following:
  - In CentreWare Internet Services, click **Properties** > **Services**.
  - Click **Workflow Scanning** > **Advanced** > **Template Pool Setup**.
  - Under Settings, select the desired protocol from the menu.
  - Type the required information for the protocol. Follow the same steps used for setting up a file repository for the protocol.
    Note: The format for a directory path for FTP is /directory/directory, while the format for a directory path for SMB is \directory\directory.
  - Click [**Apply**] to save the new settings.

- When configuring either workflow scanning file repositories or template pool repositories set the transfer protocol to be HTTPS.

7. **SNTP**:

   - 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 "Configure SNTP" in Section 3 of the SAG.

8. **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.

9. **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.

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
- Web Services
- SNMPv3
- IPv6
- IPsec

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 9 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.

- Comparing the software/firmware version listed on the Configuration Report with the Evaluated Software/Firmware version listed in Table 2 of the Xerox Multi-Function Device Security Target WorkCentre 4265, 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 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

b. In the evaluated configuration the System Administrator should ensure that all pathways and services are 'Not Allowed' or 'Not Allowed & Hidden' for guest users so that they can be accessed only by authenticated users. Follow the instructions in the "Configuring User Roles" under "User Roles" under "User Permissions" in Section 4 of the SAG to lock all pathways and services for guest users.

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.

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.
- 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.
- 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.
  - 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.
  - 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 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.
- 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.
- If an On Demand Image Overwrite fails to complete because of an error or system crash, Xerox recommends that another On Demand Image Overwrite be immediately perform, but only after completion of a system reboot.
- 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 crypto policy of their clients to request TLSv1.0 (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 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. 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 closed: 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.

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 logoff immediately after using the Web UI. They should also not allow their browser to either save their username/password or "remember" their login.

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. To enable SNMPv3 follow the instructions for "Configuring SNMPv3" in Chapter 3 of the SAG.

c. Customers should sign up for the RSS[5] 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)[6] 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. The System Administrator selects whether the primary IPv4 address will be obtained statically or dynamically via DHCP from the ***TCP/IP*** page on the Web UI. 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[7]. The 'Self Assigned Address' option from the Web UI ***TCP/IP*** page should be disabled unless either APIPA is used or Apple Rendezvous/Bonjour support is required.

[5] 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.**

[6] A SPAR is the software problem report form used internally within Xerox to document customer-reported software problems found in products in the field.

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

f. ***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: IPsec is disabled when the device is placed in FIPS 140-2 mode. The system administrator should not enable IPsec when the device is already placed in FIPS 140-2 mode.

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:

- **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.

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 '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.

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

- **Index** - Provides the user with hyperlink pointers to each Web User Interface screen organized by Web UI tab. Is accessible by selecting the [**Index**] 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.

VIII. 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
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.