Version 1.1

March 22, 2010

Secure Installation and Operation of Your WorkCentre™ 4250/4260

Secure Installation and Operation of Your WorkCentre™ 4250/4260

Purpose and Audience

This document provides information on the secure installation and operation of a WorkCentre™ 4250/4260 Multifunction System. All customers, but particularly those concerned with secure installation and operation of these machines, should follow these guidelines.

Overview

This document lists some important customer information and guidelines that will ensure that your WorkCentre™ 4250/4260 Multifunction System is operated and maintained in a secure manner.

Background

The WorkCentre™ 4250/4260 Multifunction System is currently undergoing Common Criteria evaluation. The information provided here is consistent with the security functional claims made in the Security Target. 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 or from your Xerox representative.

Secure Evaluated Configuration Installation, Setup and Operation

Please follow the guidelines below for secure installation, setup and operation of the evaluated configuration for a WorkCentre™ 4250/4260 Multifunction System:

1. The security functions in the evaluated configuration of the WorkCentre™ 4250/4260 that should be set up by the System Administrator are:
   - Immediate Image Overwrite
   - On Demand Image Overwrite
   - Authentication
   - SSL
   - Trusted Certificate Authorities
   - SNMPv3
   - IPSec
   - Audit Log
   - IP Filtering

   Follow the instructions located in the SA Guide[1] in the **Chapter 15 Security** to set up these security functions except as noted in the items below.

   Disk encryption, also a security function in the evaluated configuration of the WorkCentre™ 4250/4260, always comes enabled and cannot be disabled or configured.

2. The following services of the WorkCentre™ 4250/4260 are also considered part of the evaluated configuration and should be enabled when needed by the System Administrator - Copy, Embedded Fax, Scan to E-mail and Network Scanning.

3. Secure acceptance of the WorkCentre™ 4250/4260, once device delivery and installation is completed, should be done by:
   - Printing out a Configuration Report by following the instructions located on the SA CD[1] in the **Reference → Reports → Configuration** tabs.
   - Comparing the software/firmware versions listed on the Configuration Report with the Evaluated Software/Firmware versions listed in Table 2 of the Xerox WorkCentre™ 4250/4260 Multifunction Systems Security Target, Version 1.0 and make sure that they are the same in all cases.

4. For customers concerned about document files on the network controller hard disk drive or Embedded Fax card memory, the Image Overwrite Security (IOS) option containing the Immediate Image Overwrite and On Demand Image Overwrite security features, which comes installed on the WorkCentre™ 4250/4260 Multifunction System, must be properly configured and enabled. Please follow the applicable instructions in the SA Guide[1] starting on **Chapter 15 Security**, **Image Overwrite Security**, page 138 for proper enablement of Immediate Image Overwrite and On Demand Image Overwrite.

   Notes:

   - Immediate Image Overwrite of a delayed print job will not occur until after the machine has printed the job.
   - If an Immediate Image Overwrite fails, an informational Immediate Image Overwrite Error message will likely appear on the graphical user interface on the WorkCentre™ 4250/4260 Multifunction System that tells the user that (1) an Immediate Image Overwrite has failed for a completed job, (2) the system administrator should be notified that this error has occurred, and (3) a Full On Demand Image Overwrite should be run. An error sheet, when enabled, will always be printed indicating that there is an Immediate Overwrite Failure and requesting that a Full On Demand Image Overwrite be run.

[1] Xerox WorkCentre 4250/4260 Series System Administration Guide

- If there is a power failure or system crash while processing a large job, residual data might still reside on the hard drive. In that case an error sheet should be printed indicating that there is an Immediate Overwrite Failure. It is recommended that a Full On Demand Image Overwrite be run.
- Two forms of On Demand Image Overwrite are manually invoked – a Standard On Demand Image Overwrite that will overwrite all image data except data stored by the Save Job for Reprint feature and data stored in Embedded Fax dial directories and mailboxes and a Full On Demand Image Overwrite that will overwrite all image data including data stored by the Save Job for Reprint feature and data stored in Embedded Fax dial directories and mailboxes. Follow the instructions in the **Security → Image Overwrite Security → On Demand Image Overwrite** section of the System Administrator Guide document for invoking a Standard or Full On Demand Image Overwrite from either the Local User Interface (Local UI) or the Web User Interface (WebUI).

  The System Administrator also has the option of scheduling either a Standard or Full On Demand Image Overwrite from the WebUI. Follow the instructions in the **Security → Image Overwrite Security → On Demand Image Overwrite → Scheduled On Demand Image Overwrite** section of the System Administrator Guide document.

  Before invoking an On Demand Image Overwrite verify that there are no active or pending print or scan jobs.
- Full On Demand Image Overwrite will overwrite Stored Jobs, Fax Dial Directories and Fax Mailboxes.
- Once an On Demand Image Overwrite has begun, it cannot be cancelled and will run until completion.
- If an On Demand Image Overwrite 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 the System Administrator immediately perform another On Demand Image Overwrite, but only after completion of a system reboot.

5. Follow the instructions located in the SA Guide[1] starting on **Chapter 15 Security**, **Standard Authentication**, page 129 to set up and configure Network Authentication; follow the instructions located in the SA Guide[1] starting on **Chapter 15 Security**, **Configure Local Authentication**, page 135 to set up and configure Local Authentication.
6. Xerox recommends the following when utilizing Secure Sockets Layer (SSL) for secure scanning on a WorkCentre™ 4250/4260. Follow the instructions located in the SA Guide[1] starting on **Chapter 15 Security**, **Machine Digital Certificate Management & Trusted Certificate Authorities**, page 148 to properly set up Secure Sockets Layer (SSL) and/or request a certificate signed by a Trusted Certificate Authority on a WorkCentre™ 4250/4260. Xerox recommends the following when utilizing SSL on a WorkCentre™ 4250/4260:
   - SSL should be enabled and used for secure transmission of scan jobs from a WorkCentre™ 4250/4260.
   - Any self-signed digital certificate or digital certificate signed by a Trusted Certificate Authority should have a maximum validity of 180 days.
   - If a self-signed certificate is to be used the generic Xerox root CA certificate should be downloaded from the device and installed in the certificate store of the user's browser.
7. For SSL to work properly the machine must be assigned a valid, fully qualified machine name and domain. To set the machine name and domain:
   - At the Web UI, select the **Properties** tab.
   - Select the following entries from the **Properties** '**Content** menu': **Connectivity → Protocols → TCP/IP**.
   - Enter the domain name in the '**Domain Name**' text box inside the **Domain Name** group box; enter the machine name in the '**Host Name**' text box inside the **General** group box.
8. To enable HTTPS once SSL has been properly set up:
   - At the Web UI, select the **Properties** tab.
   - Select the following entries from the **Properties** '**Content** menu': **Connectivity → Protocols → HTTP**.
   - Select the "Require SSL" option from the **HTTP Security Mode** drop-down menu.
   - Select the [**Apply**] button. This will save the indicated settings. After saving the changes the *HTTP* page will be redisplayed. The WorkCentre™ 4250/4260 must then be rebooted for the use of HTTP to be applied.
9. Follow the instructions located in the SA Guide[1] starting on **Chapter 15 Security**, **SNMPv3**, page 153 to properly set up and configure SNMPv3. Note that SNMPv3 cannot be enabled until both SSL and HTTPS are enabled on the WorkCentre™ 4250/4260; once SNMPv3 is enabled, SSL can be disabled and SNMPv3 will still function properly.

10. Follow the instructions located in the SA Guide[1] starting on **Chapter 15 Security**, **IPSec**, page 145 to properly set up and configure IPSec (IP Security). Xerox strongly recommends that IPSec should be used for secure printing only; HTTPS (SSL) should be used to secure scanning.

    Note: IPSec is not available for either the AppleTalk protocol or the Novell protocol with the 'IPX' filing transport. IPSec also does not protect the IPv6 protocol. .

11. Follow the instructions located in the SA Guide[1] starting on **Chapter 15 Security**, **Audit Log**, page 146 to enable, download and view the Audit Log.

12. Follow the instructions located in the SA Guide[1] starting on **Chapter 15 Security**, **IP Filtering**, page 144 to properly set up and configure IP Filtering. 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.

    Note: IP Filtering is available only with IPv4, and is not available for either the AppleTalk protocol or the Novell protocol with the 'IPX' filing transport.

13. Change the Tools password as soon as possible. Reset the Tools password periodically.

    Xerox recommends that you (1) set the Tools password to a minimum length of eight alphanumeric characters and (2) change the Tools password once a month.

    Follow the instructions located in the SA Guide[1] starting on **Chapter 2 Machine Connection**, **Change the Administrator Password**, page 11 to change the Admin password from the Web User Interface.

Additional Secure Configuration Installation, Setup and Operation Guidelines

1. Xerox recommends that the System Administrator change the SNMP v1/v2c public/private community strings from their default string names to random string names.
2. Before upgrading software on a WorkCentre™ 4250/4260 Multifunction System machine please check for the latest certified software versions. Otherwise, the machine may not remain in its certified configuration.
3. To maintain the certified configuration, it is recommended that acceptance of customer software upgrades via the network be turned off/disabled on either the Local UI (Customer Software Upgrade screen) or the Web UI (Upgrade Management web page). Disabling customer software upgrades also disables the ability of a WorkCentre™ 4150 Multifunction System machine to accept a clone file.
4. System Administrator login is required when accessing the security features of a WorkCentre™ 4250/4260 machine via the Web User Interface. Xerox recommends that the 'Remember my password' option not be checked so the password is not saved in the client machine's Web Browser.
5. Caution: A WorkCentre™ 4250/4260 allows an authenticated System Administrator to disable functions like Image Overwrite Security that are necessary for secure operation. System Administrators are advised to periodically review the configuration of all installed machines in their environment to verify that the proper secure configuration is maintained.
6. The WorkCentre™ 4250/4260 provides the ability to enable one-off features through the device's Local UI, behind Tools access. A user can reach the one-off features via the following path: **Machine Status → Tools → User Interface → General → SFO.** The SFO (Special Feature Option) is intended for specific customer requests that do not represent baseline device behavior and is not designed for general use. A customer request is developed as a software patch and assigned a specific SFO #. Once implemented, the customer that requested the Feature is informed of the specific number and is enabled by the SA. These SFO's cannot be changed by anyone other than the SA or a person designated by the SA who has Local UI access rights.

    To ensure the WorkCentre™ 4250/4260 Multifunction System is operated according to the certified configuration, it is recommended that SFO 7 be disabled and SFO 22 be enabled:

    - **SFO 7** – Allows the System Administrator to enable and configure Telnet on the WorkCentre™ 4250/4260. Enablement of SFO 7 will remove the WorkCentre™ 4250/4260 from the certified configuration. SFO 7 is disabled by default.
    - **SFO 22** – Requires entry on the Local UI of the Admin Password in addition to the diagnostic PIN for anyone to perform a Memory Clear of the WorkCentre™ 4250/4260 Multifunction System. SFO 22 is disabled by default. To enable SFO 22 press the following touch-pad keys from the Tools Pathway screen: **User Interface → General → SFO**, select **22** from the list, select **Enable** and press **Save**.

7. If a system interruption such as power loss occurs a job in process may not be fully written to the hard disk. 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.

8. The following windows are available from the Local UI to a WorkCentre™ 4250/4260. These windows provide standard system configuration capability (with System Administrator login and authentication) or security related user functions:

    - **Connectivity and Network Setup** – Allows access to screens to set the various parameters associated with network connectivity. It is accessible by selecting the 'Connectivity and Network Setup' button from the Tools Mode.

    - **Delete Job Confirmation** – Allows a user or System Administrator to confirm deletion of a job from an active (incomplete) job queue. It is accessible by selecting the {Job Status} hard button on the machine, selecting the desired job from the displayed Job Queue and then selecting the 'Delete' button from the displayed Job Status Job Monitor window.

    - **Pausing an active job being processed by the device –** Allows the user to pause an active scan or print job while it is being processed by the WorkCentre™ 4250/4260. It is accessible by selecting the 'Stop' machine hard button while a job is being processed by the device. Depending on the type of job being processed by the device, a Stop/Pause window should be displayed to allow the user to determine whether to delete or continue processing of the job.

    - **Job Details (Completed Jobs)** - Allows a user to view the details of a selected completed job. It is accessible by (1) selecting the {Job Status} hard button on the machine, (2) selecting the Completed Job tab on the displayed Job Queue window, (3) selecting the desired Completed job queue from the three such "Completed" job queues available using the drop-down menu, and then finally (4) selecting the desired job from the displayed "Completed" Job Queue window.

9. The following pages are available from the Web User Interface to a WorkCentre™ 4250/4260:

    - **Connectivity** – Allows access to configuration of Connectivity ports and protocols by the Admin. It is accessible by selecting **Properties -> Connectivity**.

    - **Services** – Allows access to configuration of Printing, Fax (Embedded and Server Fax), Network Scanning and E-Mail defaults by the Admin. It is accessible by selecting **Properties -> Services**.

    - **Upgrade Management** – Allows Admin to Enable or Disable software upgrades and Cloning of the device. It is accessible by selecting **Properties -> Maintenance -> Upgrade Management**.

    - **Index –** Provides a user with hyperlink pointers to each Web User Interface screen. It is accessible by selecting the **Index** button on the top of every Web User Interface page.

    - **Remote Network Debugging –** Provides the Admin with the ability to remotely retrieve a network debug log. It is accessible by browsing to **http://{IP Address}/properties/Security/TraceTracking/DebugTrackingTool.dhtml**, where {IP Address} is the IP address of the machine.

Contact

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

Disclaimer