Document version 1.4
Last revised: 02/09/07

Secure Installation and Operation of Your WorkCentre™ 232/238/245/255/265/275 or WorkCentre™ Pro 232/238/245/255/265/275

Purpose and Audience

This document provides information on the secure installation and operation of a WorkCentre™ 232/238/245/255/265/275 or WorkCentre™ Pro 232/238/245/255/265/275. 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™ 232/238/245/255/265/275 or WorkCentre™ Pro 232/238/245/255/265/275 is operated and maintained in a secure manner.

Background

The WorkCentre™ 232/238/245/255/265/275 and WorkCentre™ Pro 232/238/245/255/265/275 product families are 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 National Information Assurance Partnership website (www.niap.nist.gov), Validated Products list or from your Xerox representative.

Details

For secure installation, setup and operation of a WorkCentre™ 232/238/245/255/265/275 or WorkCentre™ Pro /238/245/255/265/275 please follow these guidelines:

1. 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 characters and (2) change the Tools password once a month. For directions on how to change the Tools password select the:

   - **Reference → Machine Tools → Password** tabs/buttons in the System Administration (SA) CD[1]

   The only allowable characters from the machine keyboard that can be used for the Tools password are the following: digits '0' through '9', '#' and '*'.

2. For customers concerned about document files on the network controller hard disk drive, the Image Overwrite Security (IOS) option containing the Immediate Image Overwrite and On Demand Image Overwrite security features must be purchased and properly configured, installed and enabled. Please follow the applicable instructions in the **Installation → Options → Install Options** tabs/buttons in the System Administration (SA) CD[1] for proper installation and 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 screen will appear on the graphical user interface on the WorkCentre™ 232/238/245/255/265/275 or WorkCentre™ Pro 232/238/245/255/265/275 machine that tells the user that (1) an Immediate Image Overwrite in the network controller has failed for a completed job, (2) the system administrator should be notified that this error has occurred, and (3) an On Demand Image Overwrite should be run. The user closes this informational screen by pressing the Confirm button. An error sheet will also be printed indicating that there is an Immediate Overwrite Failure and requesting that an On Demand Image Overwrite be run. Finally, in the case of an Immediate Image

[1] CopyCentre™ 232/238/245/255/265/275 WorkCentre™ 232/238/245/255/265/275 WorkCentre™ Pro 232/238/245/255/265/275 System Administration CD1

Overwrite failure while processing a print job, an error message will appear at the top of this screen indicating that an On Demand Image Overwrite should be run.

- If there is a power failure or system crash of the network controller while processing a large print job, residual data might still reside on the Network Controller hard drive. In that case an error sheet will be printed indicating that there is an Immediate Overwrite Failure and requesting that an On Demand Image Overwrite be run.
- On Demand Image Overwrite is manually invoked. Follow the instructions in the **Installation → Options→ Install Options → On Demand Image Overwrite → OK** tabs/buttons in the SA CD[1] for invoking an On Demand Image Overwrite from either the Local User Interface or the Web User Interface. *Before invoking On Demand Image Overwrite verify that there are no active or pending print or scan jobs and that no user is logged into a session via network accounting, Xerox Standard Accounting, or the internal auditron.*
- When invoked from the Web UI the status of the completed On Demand Image Overwrite will not appear on the Local UI but can be ascertained from the On Demand Overwrite Confirmation Report that is printed after the Network Controller reboots.
- When On Demand Image Overwrite is invoked from the Local UI it can be aborted by a System Administrator. However, when On Demand Image Overwrite is invoked from the Web UI it cannot be aborted.
- If a System Administrator aborts an On Demand Image Overwrite, Xerox recommends that the machine be allowed to complete its system reboot before a Software Reset is attempted from the Tools Pathway via the Local User Interface. Otherwise, the Local UI will become unavailable. The machine will have to be powered off and then powered on again to allow the system to properly resynchronize.
- If there is a failure in the network controller hard disk a message recommending that an On Demand Image Overwrite be run will appear on the Local UI screen. An Immediate Image Overwrite Error Sheet will also be printed or may contain incomplete status information. The System Administrator should immediately perform the requested On Demand Image Overwrite.
- 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 shut down.

3. The security functions of the WorkCentre™ 232/238/245/255/265/275 or WorkCentre™ Pro 232/238/245/255/265/275 should be set up by the System Administrator. Follow the instructions located on the SA CD[1] in the **Reference → Internet Services → Properties → Security** tabs/buttons to set up:
   - IP Filtering
   - Audit Log
   - SSL
   - IP Sec
   - Trusted Certificate Authorities

   Follow the instructions located on the SA CD[1] in the **Installation → Options → Authentication → Network Authentication** tabs/buttons to set up an Authentication Server.

4. 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': **General Setup → 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.

5. If the use of SNMPv3 is desired, it can be set up by following these instructions:

   SNMPv3 cannot be enabled until SSL (Secure Sockets Layer) is enabled on the machine.

   - At the WebUI, select the Properties tab.
   - Select the following entries from the Properties 'Content menu': Connectivity → Protocols → SNMP. This will display the SNMP Configuration page.
   - Select the Edit SNMP v3 Properties button inside the SNMP Properties group box. This will cause the Edit SNMP v3 Properties page to be displayed.
   - On the Edit SNMP v3 Properties page:
     - Select the **Create** button inside the **Administrator Account** group box to create an administrator account.
     - Enter the desired Authentication Key in the '**Authentication Key**' text box.
     - Enter the desired Privacy Key '**Privacy Key**' text box.
     - Leave the checkboxes inside the **Print Drivers Account** group box unchecked.
     - Select the [**Apply**] button. This will create an administrator account and save the indicated settings. After saving the changes the *SNMP Configuration* page will be redisplayed.

   Once SNMPv3 is enabled, SSL can be disabled and SNMPv3 will still function properly.

6. Xerox recommends that the System Administrator change the SNMP v1/v2c public/private community strings from their default string names to random string names

7. The Embedded Fax Card must be installed in accordance with the instructions in the **Installation → Options→ Install Options → Embedded Fax** tabs/buttons in the System Administrator CD[1]. The System Administrator can then set Embedded Fax parameters and options via the Local User Interface on the machine. Follow the instructions in the **Tutorials → Machine Administration → Tools Pathway → Fax Setups** tabs in the User Guide[2].

8. Before upgrading software on a WorkCentre™ 232/238/245/255/265/275 or WorkCentre™ Pro 232/238/245/255/265/275 machine 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. To maintain the certified configuration, it is recommended that acceptance of customer software upgrades via the network be turned off/disabled on both the Local UI (***Customer Software Upgrade*** screen) and the Web UI (***Upgrade*** web page).

9. System Administrator login is required when accessing the security features of a WorkCentre™ 232/238/245/255/265/275 or WorkCentre™ Pro 232/238/245/255/265/275 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.

10. A reboot of the system software for a WorkCentre™ 232/238/245/255/265/275 or WorkCentre™ Pro 232/238/245/255/265/275 machine is necessary before a change made to the System Administrator password from the Local User Interface will be synced with and accepted by the Web User Interface. Until this system software reboot occurs, system administrator functions from the Web User Interface should not be accessed.

11. Caution: A WorkCentre™ 232/238/245/255/265/275 or WorkCentre™ Pro 232/238/245/255/265/275 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.

12. Depending upon the configuration of the WorkCentre™ 232/238/245/255/265/275 or WorkCentre™ Pro 232/238/245/255/265/275, two IP addresses, a primary IP address and a secondary IP address, may be utilized. The System Administrator assigns the primary IP address either statically or dynamically via DHCP from the ***TCP/IP*** page on the Web UI[2]. The second IP address is assigned via APIPA when the System Administrator enables the 'Self Assigned Address' option from the ***TCP/IP*** page on the Web UI. If the 'Self Assigned Address' option is enabled (which is the default case), this secondary IP address will not be visible to the SA[3]. Xerox recommends that the 'Self Assigned Address' option from the Web UI ***TCP/IP*** page be disabled unless either APIPA is used or Apple Rendezvous/Bonjour support is required.
13. Xerox recommends the following when utilizing Secure Sockets Layer (SSL) on a WorkCentre™ 232/238/245/255/265/275 or WorkCentre™ Pro 232/238/245/255/265/275:
    - SSL should be enabled and used for secure transmission of scan jobs of a WorkCentre™ 232/238/245/255/265/275 or WorkCentre™ Pro 232/238/245/255/265/275.
    - Any self-signed digital certificate or digital certificate signed by a Trusted Certificate Authority should have a maximum validity of 180 days.
    - 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.
    - 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.
    - 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. The System Administrator should be aware that 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".
14. Xerox strongly recommends that IPSec should be used for secure printing only; HTTPS (SSL) should be used to secure scanning.
15. In viewing the Audit Log the System Administrator should note the following:
    - Copy jobs are not recorded in the Audit Log.
    - Embedded Fax jobs are not recorded in the Audit Log.
    - For a LAN Fax job the event in the Audit Log will be recorded under the title of "print/driver fax".
    - To record the user's name in the Audit Log, network authentication must be configured and enabled. For directions on how to configure and enable Network Authentication select the:

      Installation → Options → Authentication tabs/buttons in the System Administration (SA) CD[1].

      Note: If 'Guest Access' is enabled, job entries in the Audit Log will be associated with the generic identity "Local User". Therefore 'Guest Access' is not recommended for secure configurations.
    - For a scan-to-mailbox job there may not be an entry made in the Audit Log for this job, although the job completion status will be reported in the Completed Job Log. If a scan-to-mailbox job is deleted from its scan-to-mailbox folder, there will be no entry created in either the Completed Jobs Log or the Audit Log for the job deletion.
16. 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.

[2] The primary IP address can also be assigned dynamically via DHCP from the Dynamic Addressing screen on the Local UI.

[3] The primary IP address will always be displayed on the Configuration Report that can be printed for a WorkCentre™ 232/238/245/255/265/275 or WorkCentre™ Pro 232/238/245/255/265/275.

17. If a system interruption such as power loss occurs a job in process may not be fully written to the Network Controller 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.

18. The following windows are available from the Local User Interface to a WorkCentre™ 232/238/245/255/265/275 or WorkCentre™ Pro 232/238/245/255/265/275 with System Administrator login and authentication. These windows provide standard system configuration capability:

    - **Connectivity and Network Setup -** Allows access to screens to set the various parameters associated with network connectivity; if a change is made to the Ethernet speed the system will automatically reboot. Is accessible by selecting the **'Connectivity and Network Setup**' button from the **Tools Mode Screen 1 of 3** screen.

    - **Delete Job Confirmation** – Allows a user or System Administrator to confirm deletion of a job other than an Internet Fax job from an active (incomplete) job queue; if the System Administrator sets Job Operation rights to 'SA/KO', then proper System Administrator authentication will be required to delete a job via this window. Is accessible by selecting the {**Job Status**} button on the machine, then selecting a 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™ 232/238/245/255/265/275 or WorkCentre™ Pro 232/238/245/255/265/275. 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, 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, **Scanning/Printing (Two Jobs) Pause** window, Resume **Marking/Incomplete Scan Job Pause** window, **Marking/Scanning Job Pause** window, **Build Job/No Marking Pause** window, **Build Job/ Marking Pause** window, **Build Job Sample Printing/ One Segment Scanned Pause** window or **Build Job Sample Printing/More Than One Segment Scanned Pause** window.

19. The following pages are available from the Web User Interface to a WorkCentre™ 232/238/245/255/265/275 or WorkCentre™ Pro 232/238/245/255/265/275 with System Administrator login and authentication. These pages provide standard system configuration capability:

    - **Upgrades -** Allows the System Administrator to enable automatic and manual software upgrades. Is accessible by selecting the **Services** -> **Machine Software** -> **Upgrades tabs** from the **Properties** Content Menu.

    - **SNMP Configuration - Advanced** - Allows the System Administrator to access advanced SNMP configuration options. Is accessible by selecting the **Connectivity** -> **Protocols** -> **SNMP tabs** from the **Properties** Content Menu and then selecting the 'Advanced' button.

    - **SNMP Configuration – IP Trap Addresses -** Allows the System Administrator to set or update IP trap addresses. Is accessible by selecting the **Connectivity** -> **Protocols** -> **SNMP tabs** from the **Properties** Content Menu, selecting the 'Advanced' button and then selecting the 'Add IP Address' button on the ***SNMP Configuration – Advanced*** **page**.

    - **SNMP Configuration – IPX Trap Addresses -** Allows the System Administrator to set or update IPX trap addresses. Is accessible by selecting the **Connectivity** -> **Protocols** -> **SNMP tabs** from the **Properties** Content Menu, selecting the 'Advanced' button and then selecting the 'Add IPX Address' button on the ***SNMP Configuration – Advanced*** **page**.

    - **Raw TCP/IP Printing – Advanced** - Allows the System Administrator to enable advanced setup options for Raw TCP/IP printing. Is accessible by selecting the **Connectivity** -> **Protocols** -> **Raw TCPO/IP Printing tabs** from the **Properties** Content Menu and then selecting the 'Advanced' button.

20. The following Special Purpose pages are available from the Web User Interface to the WorkCentre™ 232/238/245/255/265/275 or WorkCentre™ Pro 232/238/245/255/265/275 with System Administrator login and authentication. These pages provide additional system configuration capability:

    - **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}[4]/diagnostics/index.dhtml** and then selecting '**Authentication Domain/Context Query**' from the **Diagnostics** Content Menu.
    - **E-mail Security -** Allows the user to automatically include an authenticated user's E-mail address in the CC: field of an E-mail. Is accessible by typing **http://{IP Address}[4]/diagnostics/index.dhtml** and then selecting '**Email Security**' from the **Diagnostics** Content Menu.
    - **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}[4]/diagnostics/secureattr.dhtml**.
    - **Scanning Lock -** Allows bypassing the filename locking feature. Is accessible by typing **http://{IP Address}[4]/diagnostics/index.dhtml** and then selecting '**Scanning Files**' from the **Diagnostics** Content Menu or by typing **http://{IP Address}[4]/diagnostics/lockFiles.dhtml**.
    - **Enable Alphanumeric SA Passwords -** Allows the System Administrator to use alphanumeric instead of just numeric characters for the System Administrator password. Is accessible by typing **http://{IP Address}[4]/diagnostics/index.dhtml** and then selecting '**Alphanumeric SA Passwords**' from the **Diagnostics** Content Menu or by typing **http://{IP Address}[4]/diagnostics/alphanumericSaPasswords.dhtml**.
    - **LDAP -** Allows the System Administrator to set the desired LDAP Server search filters. Is accessible by typing **http://{IP Address}[4]/diagnostics/index.dhtml** and then selecting '**LDAP**' from the **Diagnostics** Content Menu or by typing **http://{IP Address}[4]/diagnostics/ldapFilter.dhtml**.
    - **Network Scanning Filename -** Allows the System Administrator to set the Network Scanning file naming conventions. Is accessible by typing **http://{IP Address}[4]/diagnostics/index.dhtml** and then selecting 'Network **Scanning Filename**' from the **Diagnostics** Content Menu.
    - **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}[4]/diagnostics/jobNameSuppress.dhtml**.
    - **File Naming Convention -** Allows the System Administrator to set the file naming convention. Is accessible by typing **http://{IP Address}[4]/diagnostics/Auto.html**.

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.

[4] {IP Address} is the IP address of the machine