Secure Installation and Operation of Your WorkCentre™ 7655/7665

Purpose and Audience

This document provides information on the secure installation and operation of a WorkCentre 7655/7665. 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™ 7655/7665 is operated and maintained in a secure manner.

Background

The WorkCentre 7655/7665 product family 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 National Information Assurance Partnership website (http://www.niap.nist.gov), Validated Products list or from your Xerox representative.

Details

For secure installation, setup and operation of a WorkCentre7655/7665 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:

   - **Reference → Machine Tools → Password → How to Change the Admin Password** in the System Administration (SA) CD[1]

   The only allowable characters from the machine keyboard that should be used for the Tools password are the following: digits '0' through '9'. Also, the Tools password should contain at least one non-zero character.

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 **Installation → Options → Installation →** select **Immediate Image Overwrite → OK → Enable Immediate Image Overwrite** in the System Administration (SA) CD[1] for proper enablement of Immediate 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 7655/7665 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.
   - If there is a crash of the Copy Controller hard drive, the Immediate Image Overwrite Error screen may not appear. In this case the System Administrator should perform an On Demand Image Overwrite as soon as possible.
   - In the case of an Immediate Image 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.

[1] WorkCentre 7655 / 7665 System Administration CD1, Document # 701P44191

- 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.

3. On Demand Image Overwrite is manually invoked. Follow the instructions in **Installation → Options → Installation →** select **On Demand Image Overwrite → OK → Perform an Image Overwrite →** either **At the Machine** or **Over the Network** in the SA CD[1] for invoking an On Demand Image Overwrite from either the Local User Interface or the Web User Interface, respectively. *Before invoking On Demand Image Overwrite verify that (1) 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, (2) the machine is not in Sleep Mode, (3)* after a power on of the machine all subsystems must be properly synced and the Configuration Report must have printed, (4) for any previously initiated On Demand Image Overwrite requests the confirmation sheet must have printed, and (5) the Embedded Fax card must have the correct software version and must be properly configured*.*

   Notes:

   - 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. However, the System Administrator should not abort an On Demand Image Overwrite once it is invoked after indication of an Immediate Image Overwrite failure.
   - 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 perform the requested On Demand Image Overwrite as soon as possible.
   - 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.
   - In the case of an Immediate Image Overwrite failure while processing a print job, the requested On Demand Image Overwrite performed may fail. The System Administrator should carefully review the On Demand Overwrite Confirmation Report printed . If the report indicates the On Demand Image Overwrite did fail, the On Demand Image Overwrite should be rerun.

4. The security functions of the WorkCentre 7655/7665 should be set up by the System Administrator. Follow the instructions located on the SA CD[1] in **Reference → Internet Services → Properties → Security** to set up:
   - IP Filtering
   - Audit Log
   - SSL (Digital Certificates)
   - IP Sec
   - Trusted Certificate Authorities

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

5. 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.
6. 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.
   - Check the **Enable SNMP v3 Protocol** checkbox.
   - 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*** web 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.
     - Do not select any of the options inside the **Print Drivers Account** group box.
     - 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.
7. Xerox recommends that the System Administrator change the SNMP v1/v2c public/private community strings from their default string names to random string names
8. The Embedded Fax Card must be installed in accordance with the instructions in **Installation → Options → Installation →** select **Embedded Fax → OK → Install the Fax Hardware Kit** 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 **Tutorials → Machine Administration → Tools Tab Pathway → Tools Tab/User Interface Settings → Fax Service Settings//** in the User Guide[22].
9. Before upgrading software on a WorkCentre 7655/7665 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 (***Remote Software Upgrade*** screen) and the Web UI (***Upgrades*** web page).
10. System Administrator login is required when accessing the security features of a WorkCentre 7655/7665 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. If an incorrect System Administrator password is entered via the Web User Interface three times in succession the system will cancel the authentication process and require the authentication process to be re-initiated; the specific response the System Administrator will see to the cancellation of the authentication process will depend on the Web Browser being used.
11. A reboot of the system software for a WorkCentre 7655/7665 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.

[2] WorkCentre 7655 / 7665 Training and Information CD2, Document # 701P44189

12. Caution: A WorkCentre 7655/7665 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.
13. Depending upon the configuration of the WorkCentre™ 7655/7665, 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[3]. 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[4]. 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.
14. Xerox recommends the following when utilizing Secure Sockets Layer (SSL) on a WorkCentre 7655/7665:
    - SSL should be enabled and used for secure transmission of scan jobs for a WorkCentre 7655/7665.
    - 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".
15. Xerox strongly recommends that IPSec should be used for secure printing only; HTTPS (SSL) should be used for secure scanning.
16. In viewing the Audit Log the System Administrator should note the following:
    - Copy jobs and Embedded Fax are not recorded in the Audit Log. The completion status of both types of jobs can be checked by viewing the applicable Completed Job Log entries.
    - 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 Local (Guest) authentication is enabled, job entries in the Audit Log will be associated with the generic identity "Local User". Therefore Local (Guest) authentication is not recommended for secure configurations.
17. Xerox recommends the following when utilizing IP Filtering on a WorkCentre 7655/7665:
    - Be careful not to create an IP Filtering rule that rejects or drops incoming TCP traffic from all addresses with source port set to 80; this will disable the Web UI.
    - If an IP Filtering rule is created that rejects or drops incoming TCP/IP traffic from all addresses for any source port including Port 80, a warning message will appear on the Web User Interface; note that a different message will appear depending on whether Port 80 or any other source port is being blocked. If blocking of network traffic for the indicated source port is still desired select the "OK" button when this warning message appears.

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

[4] The primary IP address will always be displayed on the Configuration Report that can be printed for a WorkCentre 7655/7665.

18. 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.

19. The following window is available from the Local User Interface to a WorkCentre 7655/7665 with System Administrator login and authentication. This window provides standard system configuration capability:

    - ***Reset UI To Factory Settings Pop-Up*** - Allows the System Administrator to reset the Local User Interface to its factory-default values. Is accessible by selecting the following buttons in order: '**Machine Status**' hard button -> '**Tools**' button → '**User Interface Settings**' button → '**General**' group button → '**Reset UI To Factory Settings…**' button.

20. The following windows are available by a user or System Administrator from the Local User Interface to a WorkCentre 7655/7665. These windows provide user/System Administrator machine services:

    - ***Remote Destination Log In Keyboard (Password)*** - Allows the user to enter the password for a network scan job that contains destinations that require a log-in to access. Accessible by selecting the following buttons in order: '**Network Scanning**' services button on the machine → **Network Scanning** tab → {**Start**} hard button that will cause a network scanning job to a destination that requires log in to be submitted → [**OK**] button.
    - ***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 the option on the ***Job Deletion*** screen in the Tools Pathway to '**System Administrator Only**', then proper System Administrator authentication will be required to delete a job via this screen. Is accessible by selecting the '**Job Status**' hard button on the machine → selecting the desired active (incomplete) job from the **Active Job Status** Tab → selecting '**Delete**' from the pop-up menu for the selected job.
    - ***Stop*** – Pressing the 'Stop' machine hard button will interrupt the current job and display the appropriate pause window[5].
    - ***(Xerox Standard Accounting) Accounting Status*** - Allows the user to access accounting status information when Xerox Standard Accounting is enabled. Accessible by selecting the following buttons in order: '**Accounting Status**' button from one of the service screens after the user has successfully logged into a valid Xerox Standard Accounting account.
    - ***Xerox Standard Accounting Logout*** - Allows the user to logout from a Xerox Standard Account user account (assumes the user has successfully logged into a valid Xerox Standard Accounting account). Accessible by selecting the following buttons in order: Either (1) '[**Accounting Status**] button from one of the service screens and then the '**Log In/Out**' machine hard button or (2) '**Accounting Status**' button from one of the service screens → '**Logout**' button from the ***(Xerox Standard Accounting) Account Status*** screen.
    - ***Completed Job Status*** - Allows a user to check the status of completed jobs that have been submitted to a WorkCentre 7655/7665. Accessible by selecting the following buttons in order: '**Job Status**' machine hard button on the machine → '**Completed Jobs**' tab.
    - ***Job Details – Completed Job*** - Allows the user to view the available job details for a completed job that has been submitted to a WorkCentre 7655/7665. Accessible by selecting the following buttons in order: '**Job Status**' machine hard button on the machine → '**Completed Jobs**' tab → selecting one of the completed jobs.

[5] **Scanning Pause** window, **Printing Pause** window, **Scanning/Printing (Single Job) Pause** window, **Scanning/Printing (Two Jobs) Pause** window, **Scanning Build Job Segment (No Printing) Pause** window, **Printing Build Job Segment (No Scanning) Pause** window, or **Scanning Build Job Segment (With Printing) Pause** window

21. The following pages are available from the Web User Interface to a WorkCentre 7655/7665 with System Administrator login and authentication (unless otherwise indicated). These pages provide standard system configuration capability:

    - ***Configuration Overview*** - Allows the System Administrator access to the web pages for configuring the machine. Accessible by selecting the **Properties** tab (will come up by default) or by selecting **Configuration Overview** from the **Properties** 'Content Menu'. System Administrator login and authentication is not required to access this web page.

      If the '**View Checklist**' button is selected from the ***Configuration Overview*** page, the ***Print Checklist*** page will appear that provides a checklist for helping the System Administrator configure a WorkCentre 7655/7665.machine.

    - ***Internationalization*** - Allows the System Administrator to install a base product version worldwide using the Unicode 3.0/ISO-10646 character set. Accessible by selecting the **General Setup** button → **Internationalization** button from the **Properties** 'Content Menu'.

    - ***Sleep Mode Settings*** - Allows the System Administrator to set network controller sleep mode settings. Accessible by selecting the **General Setup** button → **Sleep Mode Settings** button from the **Properties** 'Content Menu'. If the '**Advanced Settings**' button is selected from the ***Sleep Mode Settings*** page, the ***Sleep Mode Settings – Advanced*** page will be accessed that allows the System Administrator to set advanced network controller sleep mode settings.

    - **SNMP Configuration – Edit IP Address** - Allows the System Administrator to edit the IP address for traps when setting up SNMP. Accessible by selecting from the **Connectivity** button the **Properties** 'Content Menu' → **Protocols** button → **SNMP** button → '**Advanced**' button on the **SNMP Properties** group box on the ***SNMP Configuration*** page → '**Edit**' button on the ***SNMP Configuration – Advanced*** page.

    - ***LDAP Group Access*** - Allows the System Administrator to set settings for searching a name and desired E-mail environment. Accessible by selecting from the **Properties** 'Content Menu' the **Connectivity** button → **Protocols** button → **LDAP** button → '**LDAP Group Access**' button on the ***LDAP Directory*** page.

    - ***Validation Servers*** - Allows the System Administrator to select up to six Network Scanning validation servers. Is accessible by selecting the **Services** button from the **Properties** 'Content Menu' → **Network Scanning** button → **Validation Servers** button. On the ***Validation Servers*** page, if either the '**Edit**' button is selected after selecting an existing server or the '**Add**' button is selected, the *Add/Edit Validation Servers* page will be accessed to allow the System Administrator to edit or add, as applicable, validation server settings.

    - ***Scan Template Management*** - Allows the System Administrator to set up management of a scan template. Is accessible by selecting the **Services** button from the **Properties** 'Content Menu' → **Network Scanning** button → **Scan Template Management** button.

    - ***Validation Options*** - Allows the System Administrator to setup validation request messages to users. Is accessible by selecting the **Services** button from the **Properties** 'Content Menu' → **Custom Services** button → **Validation Options** button.

22. The following Special Purpose pages are available from the Web User Interface to the WorkCentre 7655/7665 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}[6]/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}[6]/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}[6]/diagnostics/secureattr.dhtml**.
    - **Scanning Lock Files -** Allows the user to bypass the filename locking mechanism when performing scanning. Is accessible by typing **http://{IP Address}[6]/diagnostics/index.dhtml** and then selecting [**Scanning Lock Files**] from the **Diagnostics** Content Menu or by typing **http://{IP Address}[6]/diagnostics/lockFiles.dhtml**.
    - **Raw TCP/IP Printing Hidden -** Allows the user to set parameters for Raw TCP/IP (Port 9100) printing. Is accessible by typing **http://{IP Address}[6]/diagnostics/ rawTcpIphidden.dhtml**.
    - **Suppress Job Name -** Allows the user to suppress the job name on the banner page for a print job. Is accessible by typing **http://{IP Address}[6]/diagnostics/ jobNameSuppress.dhtml**.

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.

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