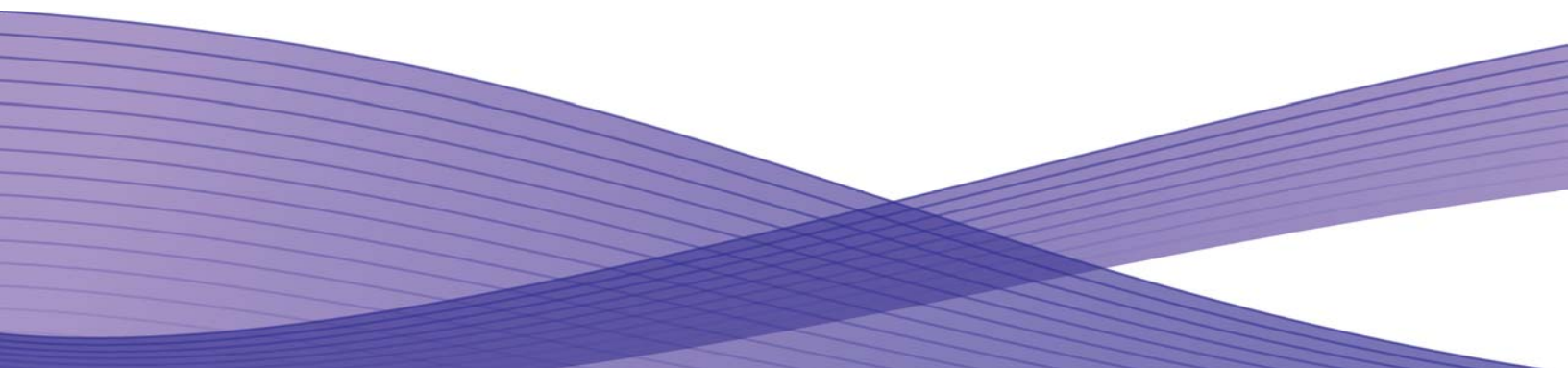
Version 1.8

Jul 30, 2010

Secure Installation and Operation of Your WorkCentre™ 5632/5638/5645/5655/ 5665/5675/5687



Secure Installation and Operation of Your WorkCentre™ 5632/5638/5645/5655/5665/5675/5687

Purpose and Audience

This document provides information on the secure installation and operation of a WorkCentre™ 5632/5638/5645/5655/5665/5675/5687 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™ 5632/5638/5645/5655/5665/5675/5687 Multifunction System is operated and maintained in a secure manner.

Background

The WorkCentre™ 5632/5638/5645/5655/5665/5675/5687 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™ 5632/5638/5645/5655/5665/5675/5687 Multifunction System:

1. The security functions in the evaluated configuration of the WorkCentre™ 5632/5638/5645/5655/5665/5675/5687 that should be set up by the System Administrator are:
   - Immediate Image Overwrite
   - On Demand Image Overwrite
   - Disk Encryption
   - IP Filtering
   - Audit Log
   - SSL (for protection of management data)
   - Trusted Certificate Authorities
   - Authentication and Authorization

   Follow the instructions located on the SA CD[1] in the **Reference → Security** tabs/buttons to set up these security functions except as noted in the items below.
2. The following services of the WorkCentre™ 5632/5638/5645/5655/5665/5675/5687 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, Network Scanning, Saved Jobs for Reprint, Reprint Saved Jobs, and ID Card Copy.
3. Secure acceptance of the WorkCentre™ 5632/5638/5645/5655/5665/5675/5687, 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™ 5632/5638/5645/5655/5665/5675/5687 Multifunction Systems Security Target, Version 1.0 and make sure that they are the same in all cases.
4. Follow the instructions located on the SA CD[1] in the **Reference → Security → Authentication and Authorization → Authentication Configuration** tabs/buttons to set up an Authentication Server. Follow the instructions located on the SA CD[1] in the **Reference → Security → Authentication and Authorization → Xerox Common Access Card** tabs/buttons to set up user authentication via a Common Access Card.
5. 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™ 5632/5638/5645/5655/5665/5675/5687 Multifunction System, must be properly configured and enabled. Please follow the applicable instructions in the **Reference → Security → Image Overwrite Security** tabs/buttons in the System Administration (SA) CD[1] for proper enablement of Immediate Image Overwrite and On Demand Image Overwrite.

[1] (WorkCentre™ 5632/5638/5645/5655/5665/5675/5687) System Administration CD1, 538E11432

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 likely appear on the graphical user interface on the WorkCentre™ 5632/5638/5645/5655/5665/5675/5687 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) an On Demand Image Overwrite should be run. The user closes this informational screen by pressing the Confirm button. An error sheet, when enabled, will always 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 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 while a network scan job is being processed, an Immediate Overwrite of the residual data will occur upon job recovery. However, the network scan job may not appear in the Completed Job Log.
- If there is a power failure or system crash of the network controller while processing a print job, residual data might still reside on the Network Controller hard drive. The System Administrator should immediately invoke an On Demand Image Overwrite once the machine has been restored.
- 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 **Installation → Security → Image Overwrite Security → On Demand Image Overwrite** tabs/buttons in the SA CD[1] for invoking a Standard of 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 **Reference → Security → Image Overwrite Security → On Demand Image Overwrite → Auto Schedule an Overwrite** tabs/buttons in the SA CD[1] to schedule an On Demand Image Overwrite.
- Before invoking an On Demand Image Overwrite 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 network controller hard disk.
  - No user is logged into a session via telnet, network accounting, Xerox Standard Accounting, or the internal auditron, or into a session accessing a directory on the network controller hard disk.
  - 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 On Demand Image Overwrite request the confirmation sheet must have printed.
  - The Embedded Fax card must have the correct software version and must be properly configured.
- 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.
- 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.
- The System Administrator may cancel an On Demand Image Overwrite only at the Local UI if it was initiated at that interface. If an On Demand Image Overwrite was initiated from the WebUI, it cannot be aborted from either the WebUI or Local UI.
- 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 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 or software reset initiated from the Local User Interface or the Web User Interface.
- The System Administrator should perform an On Demand Image Overwrite immediately before a WorkCentre™ 5632/5638/5645/5655/5665/5675/5687 Multifunction System is decommissioned, returned, sold or disposed of.

6. The WorkCentre™ 5632/5638/5645/5655/5665/5675/5687 Multifunction System supports the use of SSLv2.0, SSLv3.0, RC4 and MD5. However, customers are advised to set the cyrpto policy of their clients to request either SSLv3.1 or TLSv1.0 and to disallow the use of RC4 and MD5.
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 → IP.(Internet Protocol)**
   - 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. Xerox recommends the following when utilizing Secure Sockets Layer (SSL) on a WorkCentre™ 5632/5638/5645/5655/5665/5675/5687:
   - 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.
9. To enable HTTPS (SSL):
   - At the Web UI, select the **Properties** tab.
   - Select the following entries from the **Properties** '**Content** menu': **Connectivity → Protocols → HTTP**.
   - Select the Secure HTTP (SSL) **Enabled** checkbox in the **Configuration** group box and enter the desired HTTPS port number in the Port Number text box.
   - Select the [**Apply**] button. This will save the indicated settings. After saving the changes the *HTTP* page will be redisplayed.
10. In viewing the Audit Log the System Administrator should note the following:
    - Submittal or deletion of copy and embedded fax jobs are not recorded in the Audit Log.
    - Deletion of a file from a Saved Job for Reprint folders or deletion of a Saved Job for Reprint 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.
11. 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.
12. To enable disk encryption:
    - At the Web UI, select the **Properties** tab.
    - Select the following entries from the **Properties** '**Content** menu': **Security → User Data Encryption**.
    - Select the **Enabled** checkbox in the **User Data Encryption Enablement** group box.
    - Select the [**Apply**] button. This will save the indicated setting. After saving the changes the *User Data Encryption* page will be redisplayed.

    Xerox recommends that before enabling disk encryption the System Administrator should make sure that the WorkCentre™ 5632/5638/5645/5655/5665/5675/5687 is not in diagnostics mode and that there are no active or pending scan jobs.
13. The System Administrator should ensure that the Embedded Fax Card and fax software is installed in accordance with the instructions in the **Installation → Services → Embedded Fax → Complete the Fax Install Screens** and **Fax Setup** tabs in the SA 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 Interactive User Guide[2].

[2] (WorkCentre™ 5632/5638/5645/5655/5665/5675/5687) Interactive User Guide CD2, 538E11443

14. If the Save Jobs for Reprint/Reprint Saved Jobs service is enabled the private folder authentication is not working properly. The System Administrator should establish the appropriate policies and procedures to ensure that any jobs are saved only into either the default public folder or a read-only public folder. Documents of a sensitive nature should not be stored on the device until the issue is resolved.

15. 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, (2) change the Tools password once a month and (3) 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.).

    For directions on how to change the Tools password from the Local User Interface, select the:

    - **Reference → Security → Authentication and Authorization → Administrator Authentication** tabs/buttons in the System Administration (SA) CD[1]

    For directions on how to change the Tools password from the Web User Interface, select the:

    - **Reference → Security → Authentication and Authorization → Authentication Configuration → Device System Administrator Password** tabs/buttons in the System Administration (SA) CD[1]

Additional Secure Configuration Installation, Setup and Operation Guidelines

1. Xerox recommends the following when utilizing Secure Sockets Layer (SSL) for secure scanning on a WorkCentre™ 5632/5638/5645/5655/5665/5675/5687:

    - SSL should be enabled and used for secure transmission of scan jobs from a WorkCentre™ 5632/5638/5645/5655/5665/5675/5687.
    - 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. 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".

2. 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) and HTTPS (SSL) are 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 Enable SNMP v3 Protocol checkbox inside the SNMP Properties group box.
    - 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 **Account Enabled** button inside the **Administrator Account** group box to create an administrator account.
        - Enter the desired **Username** and **Authentication Password**. The **Authentication Password** must be at least 8 alphanumeric characters.
        - Enter the desired **Privacy Password** of at least 8 alphanumeric characters.
        - Select the **Account Enabled** button inside the **Print Drivers Account** group box to create an account for bi-directional print drivers / Xerox remote clients.
        - Select the [**Apply**] button. This will create an administrator account and save the indicated settings/passwords. 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.

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

4. 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. .

5. Before upgrading software on a WorkCentre™ 5632/5638/5645/5655/5665/5675/5687 Multifunction System 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).
6. Xerox recommends that customers sign up for the RSS[3] subscription service available only 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 that apply to the WorkCentre™ 5632/5638/5645/5655/5665/5675/5687 Multifunction System.
7. The WorkCentre™ 5632/5638/5645/5655/5665/5675/5687 Multifunction System 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.
8. Xerox recommends that the system administrator continuously monitor the network that the WorkCentre™ 5632/5638/5645/5655/5665/5675/5687 Multifunction System is connected to for unapproved activities and/or attempts to attack network resources, including the device itself. This should include monitoring of the number of logon tries to the Web UI.
9. Customers who encounter or suspect software problems against a WorkCentre™ 5632/5638/5645/5655/5665/5675/5687 Multifunction System should immediately contact the Xerox Customer Support Center to report the suspected problem and initiate the SPAR (Software Problem Action Request)[4] process for addressing problems found by Xerox customers.
10. System Administrator login is required when accessing the security features of a WorkCentre™ 5632/5638/5645/5655/5665/5675/5687 machine via the Web User Interface.
11. A reboot of the system software for a WorkCentre™ 5632/5638/5645/5655/5665/5675/5687 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.
12. Caution: A WorkCentre™ 5632/5638/5645/5655/5665/5675/5687 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™ 5632/5638/5645/5655/5665/5675/5687, two IPv4 addresses, a primary IPv4 address and a secondary IPv4 address, may be utilized. The System Administrator assigns the primary IPv4 address either statically or dynamically via DHCP from the ***IP (Internet Protocol)***page on the Web UI[5]. 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[6]. Xerox recommends that the 'Self Assigned Address' option from the Web UI ***IP (Internet Protocol)*** page be disabled unless either APIPA is used or Apple Rendezvous/Bonjour support is required.
14. 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.
15. The following windows are available from the Local User Interface to a WorkCentre™ 5632/5638/5645/5655/5665/5675/5687 with System Administrator login and authentication. These windows provide standard system configuration or job management capability:
    - **User Feature Enablement Code** - Allows ability to enter a valid User Feature Enablement Code to enable or disable specific machine system configuration and service functions. Is accessible by selecting the '**Enablement Code**' button from the **Authentication Login Required** or **Pathway Options** screens.

[3] RDF Site Summary, or Rich Site Summary, or 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**.

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

[5] The primary IPv4 address can also be assigned dynamically via DHCP from the Dynamic Addressing screen on the Local UI.

[6] The primary IPv4 address will always be displayed on the Configuration Report that can be printed for a WorkCentre™ 5632/5638/5645/5655/5665/5675/5687.

- **USB Printer Port** - Allows ability to enable/disable and set the configuration of the USB Printer Port connectivity. Is accessible by selecting the following screens/buttons in order: **Tools Mode Screen 1 of 3** screen → **Connectivity and Network Setup** button → **Direct Connection** button → USB Printer Port button.

- **Parallel Port** - Allows ability to enable/disable and set the configuration of parallel port printing. Is accessible by selecting the following screens/buttons in order: **Tools Mode Screen 1 of 3** screen → **Connectivity and Network Setup** button → **Direct Connection** button → Parallel Port button. Note that this window is only available to WorkCentre™ 5632/5638/5645/5655/5665/5675/5687 Multifunction Systems that have the Multi-Board Controller (MBC) hardware configuration.

- **SA Delete Job** – For jobs other than an Internet Fax job that do not require a Secure ID PIN but do require System Administrator authentication (i.e., the System Administrator has set Job Operation rights to 'System Administrator' and the job was not submitted as a Secure Print or Secure Fax job), allows the System Administrator to be authenticated as a valid System Administrator and then delete the job. 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.

- **Dual Authentication Delete Job** – For jobs other than an Internet Fax job that require both a Secure ID PIN and System Administrator authentication (i.e., the System Administrator has set Job Operation rights to 'System Administrator' and the job was submitted as a Secure Print or Secure Fax job), allows the System Administrator to be authenticated as a valid System Administrator and then delete the job. 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.

16. The following windows are available from the Local User Interface to a WorkCentre™ 5632/5638/5645/5655/5665/5675/5687 with no System Administrator login and authentication required. These windows provide standard machine services or job management capability:

    - **Delete Job Confirmation** – For jobs other than an Internet Fax job that do not require either a Secure ID PIN or System Administrator authentication (i.e., the System Administrator has set Job Operation rights to 'All Users' and the job was not submitted as a Secure Print or Secure Fax job), allows a user to confirm deletion of the job. 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 copy, print, scan or Embedded Fax job while it is being processed by the WorkCentre™ 5632/5638/5645/5655/5665/5675/5687. 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.

    - **Pause to Unload Finisher Hard Button** - Allows the user to remove output from a finisher's Stacker Tray while preventing the device from outputting marked sheets to the finisher at the same time. Is accessible by selecting the **Pause to Unload** hard button **on the finisher**.

    - **CPSR (Capture/Print, Save and Reprint) Information Pop-Up Screen** – Provides error information and/or required actions to the user after the user has exercised selected screens and buttons (e.g., creation and deletion of a folder or job) of the 'Save Job for Reprint' and 'Reprint Saved Jobs' Feature Pathways .on a WorkCentre™ 5632/5638/5645/5655/5665/5675/5687. The **CPSR Information** pop-up screen will appear automatically when the proper screens and/or buttons are selected by the user and will provide the user with the needed information or actions to complete the desired 'Save Job for Reprint' and 'Reprint Saved Jobs' functions.

    - **User Interface Diagnostics** - Allows the user to run diagnostics on the User Interface software. Is accessible by pressing the machine hard buttons '**Dial Pause**' + '*' + '**#**' in that order.

    - **Encryption/Decryption in Progress Pop-Up Screen** – Informs the user that a WorkCentre™ 5632/5638/5645/5655/5665/5675/5687 is performing an encryption or decryption of data stored on the Network Controller hard disk. The **Data Encryption/Decryption in progress** pop-up screen will appear automatically whenever a machine that is in an operational mode receives a request that requires data stored on the Network Controller hard disk to be either encrypted or decrypted.

17. The following pages are available from the Web User Interface to the WorkCentre™ 5632/5638/5645/5655/5665/5675/5687 with System Administrator login and authentication. These pages provide additional system functional capability:

- **Reboot Machine** – Provides ability to reboot the machine from the Internet. Is accessible from the Description & Alerts page by selecting the **Status** tab and then selecting **Descriptions and Alerts** from the **Status** tab content menu.
- **Public Address Book** – Allows the System Administrator to set up the contents and access rights for the Public Address Book. Is accessible by selecting the **Public Address Book** tab. From the **Public Address Book** tab content menu the System Administrator can access the following pages to setup the Public Address Book:
  - **View All Names** – Displays the Public Address Book page and provides access to all names in the Public Address Book.
  - **Edit** – Edits a Public Address Book name selected from the Public Address Book page.
  - Add New Name – Accesses the **Add New Name** page to add a new name to the Public Address Book.
  - **Import** – Accesses the **Import** page to import of names from a file that will be added to the Public Address Book. A **Next** button on the **Import** page allows the System Administrator to set options on how the names are to be imported.
  - **Export** – Accesses pages to export the Public Address Book to a user-defined file.
  - **Download Sample** – Allows the System Administrator to download a sample Public Address Book into a user-defined file where names can be added at a later time.
  - **Delete All Names** – Allows the System Administrator to delete all names from the Public Address Book.
  - **Access Rights** - Allows the System Administrator to set the access rights to the Public Address Book.
- **Web Services** – Allows the System Administrator to set up various Web Services that utilize the HTTP protocol. Is accessible by selecting the **Properties** tab and then selecting **Connectivity → Protocols → HTTP → Web Services** tab from the **Properties** tab content menu.
- NTP - Allows the System Administrator to set the device date and time using an external server. Is accessible by selecting the **Properties** tab and then selecting **Connectivity → Protocols → NTP** from the **Properties** tab content menu.
- **FTP** – Allows the System Administrator to set the parameters for the FTP protocol used in network filing. Is accessible by selecting the **Properties** tab and then selecting **Connectivity → Protocols → FTP** from the **Properties** tab content menu.
- **WSD (Web Services for Devices)** – Allows the System Administrator to enable Web Services on the device. Is accessible by selecting the **Properties** tab and then selecting **Connectivity → Protocols →** WSD (Web Services for Devices) from the **Properties** tab content menu.
- **E-mail Domain Filter** – Allows the System Administrator to set how address books search domains for E-mail addresses. Is accessible by selecting the **Properties** tab and then selecting **Services → E-mail →** Domain Filter from the **Properties** tab content menu.
- **Web Services Advanced Setting**s – Allows the System Administrator to clear the Web Services IP Address Lockout cache. Is accessible by either (1) selecting the **Properties** tab and then selecting **Connectivity → Protocols → HTTP → Web Services** tab → **Advanced Settings** button from the **Properties** tab content menu or (2) by typing **http://{IP Address}**[7]**/diagnostics/ipLockout.php.**
- **(Workflow Scanning) Display Setting**s – Allows the System Administrator to setup how the Workflow Scanning template list is displayed on the Local UI. Is accessible by either (1) selecting the **Properties** tab and then selecting **Services → Workflow Scanning → Display Settings** from the **Properties** tab content menu or (2) selecting the '**Refer to Display Settings for more template controls**' hyperlink from any of the scan and network scanning template pages.
- **Validation Options** – Permits the System Administrator to allow the user name to be sent with the validation request if the user is authenticated at the Local UI. Is accessible by selecting the **Properties** tab and then selecting **Services → Custom Services → Validation Options** from the **Properties** tab content menu.
- **Fax Forward on Receive** – Allows the System Administrator to enable forwarding of receive Embedded Faxes to alternate destinations such as E-mail addresses or file repositories. Is accessible by selecting the **Properties** tab and then selecting **Services → Embedded Fax → Fax Forward** from the **Properties** tab content menu. From the **Fax Forward on Receive** page the System Administrator can access the following pages to setup Fax Forward on Receive:
  - **Edit** – Displays the **Rule** page to set or modify the alternate destinations for a received Embedded Fax.
  - **Customize** – Displays the **Custom File Name** or **Custom Attachment Name** page, depending on the type of alternate destination, to customize the name of the file or attachment the received Embedded Fax will be stored in.
- **Authentication Configuration – CAC (Common Access Card)** - Provides ability to set up the Domain Controller and other elements needed to configure CAC authentication on a WorkCentre™ 5632/5638/5645/5655/5665/5675/5687. The main *Authentication Configuration > CAC/PIV Setup* page is accessible by selecting the following entries from the Properties 'Content menu': Security → Authentication Configuration → **Edit** or **Configure** (Device User Interface Authentication Method) button (where [CAC/PIV] is the Device User Interface Authentication Method chosen on the *Authentication*

[7] {IP Address} is the IPv4 address of the machine

Configuration Setup page); from that page the other pages needed to configure CAC are accessible. When configuring the CAC domain controller the System Administrator should make sure that the Port Number entered is less than 65536.

- **System Timeout** – Permits the System Administrator to set up a WebUI inactivity timer for the device. Is accessible by selecting the **Properties** tab and then selecting **Security → System Timeout** from the **Properties** tab content menu.
- **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}[8]/diagnostics/index.dhtml** and then selecting '**Authentication Domain/Context Query**' from the **Diagnostics** Content Menu.
- **Scanning Lock Files -** Allows bypassing the filename locking feature. Is accessible by typing **http://{IP Address}[9]/diagnostics/index.dhtml** and then selecting '**Scanning Lock Files**' from the **Diagnostics** Content Menu or by typing **http://{IP Address}[4]/diagnostics/lockFiles.dhtml**.
- **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}[9]/diagnostics/secureattr.dhtml**.
- **Suppress Job Name -** Allows the System Administrator to suppress displaying the job name on the Banner Page when submitting a print job. Is accessible by typing **http://{IP Address}[9]/diagnostics/jobNameSuppress.dhtml**.
- **Job Log File Format -** Allows the System Administrator to set the XML job log file format. Is accessible by typing **http://{IP Address}[9]/diagnostics/jobLog.dhtml**.
- **File Extension Case -** Allows the System Administrator to select all file extensions to be created in either lower or upper case. Is accessible by typing **http://{IP Address}[9]/diagnostics/fileExtensionCase.dhtml**.
- **Email Security -** Allows the System Administrator to secure the device's email service. Is accessible by typing **http://{IP Address}[9]/diagnostics/emailSecurity.php**.
- **Binary Printing Support -** Allows the device to accept printing jobs that are identified as binary files. Is accessible by typing **http://{IP Address}[9]/diagnostics/binaryAllow.php.**
- **XSA Reports with User IDs -** Allows the device to generate Xerox Standard Accounting reports with User IDs. Is accessible by typing **http://{IP Address}[9]/diagnostics/enableUserID.php**.
- **Postscript Filter PDL Guessing Policy -** Allows the System Administrator to select whether the Postscript Filter guess algorithm will use a strict or loose interpretation. Is accessible by typing **http://{IP Address}[9]/diagnostics/postScriptTokens.php**.
- **Service Registry Reset -** Allows the System Administrator to reset the device's Service Registry to its default values. Is accessible by typing **http://{IP Address}[9]/diagnostics/registryReset.php**.
- **Job Queue Limit -** Allows the System Administrator to set the maximum number of jobs that can be listed in the device's job queues. Is accessible by typing **http://{IP Address}[9]/diagnostics/jobLimit.php**.
- **DLM Maker -** Allows the System Administrator to create a DLM out of any file. Is accessible by typing **http://{IP Address}[9]/diagnostics/dlmMaker.php**.
- **Barcode Space Character Interpretation -** Allows the System Administrator to choose how the device renders space characters within barcode fonts. Is accessible by typing **http://{IP Address}[9]/diagnostics/barcodeSpaceToggle.php**.
- **DHCP v6 -** Allows the System Administrator to choose which compliance option will be followed when DHCP v6 is used. Is accessible by typing **http://{IP Address}[9]/diagnostics/ dhcpv6Options.php**.
- **View Service Registry Contents -** Allows the System Administrator to view the contents of the device's Service Registry. Is accessible by typing **http://{IP Address}[9]/diagnostics/viewRegistry.php**.
- **Diagnostics Tree -** Allows the System Administrator to view the selectable list of diagnostics Special Purpose Pages. Is accessible by typing **http://{IP Address}[9]/diagnostics/tree.php**.
- **Color Copy Control Test Result -** Allows the System Administrator to view the Color Copy Control test results. Is accessible by typing **http://{IP Address}[9]/diagnostics/testResult.php**.
- **PCL Advanced Configuration -** Allows the System Administrator to enter the desired PCL advanced configuration paper size code. Is accessible by typing **http://{IP Address}[9]/diagnostics/pclSetup.php**.
- **Grey Other Queue Button -** Allows the System Administrator to grey out the 'Other Queue' button on the Local UI. Is accessible by typing **http://{IP Address}[9]/diagnostics/hideotherqueuesbutton.php**.

- **Download DLM PCL Forms -** Allows the System Administrator to download the DLM PCL forms into the device. Is accessible by typing **http://{IP Address}[9]/diagnostics/ dl_pcl.php**.
- **Download DLM Authentication Settings -** Allows the System Administrator to download the DLM authentication settings into the device. Is accessible by typing **http://{IP Address}[9]/diagnostics/dl_auth_settings.php**.
- **Multiple Pages per JBIG2 Dictionary -** Allows the System Administrator to enable the multiple pages per JBIG2 dictionary feature (for PDF and PDF/A only). Is accessible by typing **http://{IP Address}[9]/diagnostics/disableMultiplePages.php**.
- **Print Behavior Settings -** Allows the System Administrator to configure/enable alternate media dimension settings for print jobs. Is accessible by typing **http://{IP Address}[9]/diagnostics/alternateMedia.php**.
- **Show WebUI Configuration Page -** Allows the System Administrator to enable users who are not authenticated administrators to view the WebUI Configuration Page. Is accessible by typing **http://{IP Address}[9]/diagnostics/ShowConfigPage.php**.
- **NTLM v2 Response -** Allows the System Administrator to enable the device to send only the NT Lan Manager (NTLM) Version 2 protocol (and refuse the LM & NTLM versions). Is accessible by typing **http://{IP Address}[9]/diagnostics/NTLMSecurity.php**.
- **Secure Print Alphanumeric PIN -** Allows the System Administrator to set the secure print PIN to be alphanumeric characters instead of just digits. Is accessible by typing either (1) **http://{IP Address}[9]/diagnostics/index.dhtml** and then selecting '**Secure Alphanumeric PIN**' from the **Diagnostics** Content Menu or (2) **http://{IP Address}[8]/diagnostics/secureprintalphanumericpin.php**.
- **Custom Size Allowed -** Allows the System Administrator to allow custom size paper to be used for print jobs. Is accessible by typing **http://{IP Address}[9]/diagnostics/customSizeAllowed.php**.
- **Suppress Last Blank Page -** Allows the System Administrator to suppress a last blank page for print jobs. Is accessible by typing **http://{IP Address}[9]/diagnostics/suppresslastblankpage.php**.
- **Display CAC/PIV Feature -** Allows the System Administrator to enable the the display of the CAC/PIV feature. Is accessible by typing **http://{IP Address}[9]/diagnostics/enableCAC.php**.
- **Install 00022121 (View Scan Templates Created by WIA Driver) -** Allows the System Administrator to install the #00022121 Network Controller version to view templates created by the Microsoft Windows Image Acquisition (WIA) driver. Is accessible by typing **http://{IP Address}[9]/diagnostics/00022121.dhtml**. The System Administrator should be aware that installing this Network Controller version will result in the WorkCentre™ 5632/5638/5645/5655/5665/5675/5687 no longer being in the certified configuration.

18. The following pages are available from the Web User Interface to a WorkCentre™ 5632/5638/5645/5655/5665/5675/5687 with no System Administrator login and authentication required:
    - **Site Map** - Provides the user with hyperlink pointers to each Web User Interface screen organized by Web UI tab. Is accessible by selecting the [**Site Map**] button in the upper right hand corner of every Web User Interface page.
    - **Exit from Sleep Mode** – Automatically informs the user, when the Network Controller on a WorkCentre™ 5632/5638/5645/5655/5665/5675/5687 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.

19. The following augments guidance contained in the SA CD[1]:
    - Under the Reference Tab, the pages obtained by selecting the **Internet Services** -> **Connectivity** -> **Protocols** -> **Proxy Server tabs/buttons** should indicate that the Proxy Server allows the System Administrator to enter the address of the Proxy Server which the device can use. Proxy Server setup is accessible by selecting the **Properties** tab and then selecting **Connectivity → Protocols → Proxy Server** from the **Properties** tab content menu. To setup the Proxy Server the System Administrator should check the [Enabled] box on this page, enter the IP address or host name of the Proxy Server and then click the [Apply] button.
    - Under the Reference Tab, the **Internet Services** -> **Connectivity** -> **Protocols** -> **NTP tab/buttons should point to a page that describes NTP (Network Time Protocol) and how the** System Administrator can **set it up. Item #17 above describes how to access the NTP page.** To setup NTP the System Administrator should check the [**Enabled**] box on the NTP page, enter the IP address or host name of the primary and backup NTP Server and then click the [**Apply**] button.

20. The following augments guidance contained in the Interactive User Guide[2]:

- The animation in the **Overview** page under the **Tutorials** -> **Authentication and Accounting** Tabs was inadvertently omitted. This animation was intended to show the user at a high level the authentication process and define what authentication means (i.e., the process of logging in, where a username and password is checked against a database; once the username and password are found the user is authenticated).
- Text and animation in the Login page under the **Tutorials** -> **Authentication and Accounting** Tabs was also inadvertently omitted. This text and animation was intended to show the user how to log in (i.e., enters the proper username and password) to access a service on the device and how to log in when either Xerox Standard Accounting, the Internal Auditron, Network Accounting or the Foreign Device Interface is enabled on the device[8].
- Under the **Tutorials** -> **Authentication and Accounting** Tabs, the Logout page should state that when the user finishes a session the user should logout by pressing the Access hard button on the device's control panel which opens the Accounting/Authentication logout screen. To log out the user selects the Logout button. .

21. Customers who required specialized changes to support unique workflows in their environment may request specific changes to normal behavior. Xerox will supply these SPAR releases to the specific customers requesting the change. Please note that in general enabling a specialized customer-specific feature will take the system out of certified configuration.

Contact

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

Disclaimer

[8]The Internal Auditron, Network Accounting and the Foreign Device Interface are not part of the evaluated configuration for a WorkCentre™ 5632/5638/5645/5655/5665/5675/5687.