# Secure Installation and Operation of Your WorkCentre™ M35/M45/M55 or WorkCentre™ Pro 35/45/55

## Purpose and Audience

This document provides information on the secure installation and operation of a WorkCentre™ M35/M45/M55 Copier-Printer or WorkCentre™ Pro 35/45/55 Advanced 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™ M35/M45/M55 Copier-Printer or WorkCentre™ Pro 35/45/55 Advanced Multifunction System is operated and maintained in a secure manner.

## Background

The WorkCentre™ M35/M45/M55 Copier-Printer and WorkCentre™ Pro 35/45/55 Advanced Multifunction System 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 (http://www.niap.nist.gov/), Validated Products list or from your Xerox representative.

## Details

For secure installation, setup and operation of a WorkCentre™ M35/M45/M55 Copier-Printer or WorkCentre™ Pro 35/45/55 Advanced Multifunction System 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 digits and (2) change the Tools password once a month. For directions on how to change the Tools password select either the:
   - **Reference → Machine Tools → Password** tabs in the System Administration (SA) CD[1] or
   - **Tutorials → Machine Administration → Accessing Tools Pathway** tabs in the User's Guide[2].

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 → Installation** tab 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, once enabled, automatically overwrites the image data created by a print or scan job on the Network Controller Hard Disk. The machine will only print jobs with valid print types (Postscript, PCL, TIFF, text of PDF). An illegal print job of any other type will not be printed. However, Immediate Image Overwrite will attempt to execute for an illegal print job. This could result in an erroneous 'unsuccessful' Immediate Image Overwrite status in the Complete Job Log for the job in question.

     Canceling of either a legal or illegal print job from a remote client, if done quickly after submission, could also result in an erroneous 'unsuccessful' Immediate Image Overwrite status in the Complete Job Log for the job in question. Finally, closing the connection to Port 9100 without sending any data through the port could result in an erroneous 'unsuccessful' Immediate Image Overwrite status in the Complete Job Log.

[1] CopyCentre C35/C45/C55 WorkCentre M35/M45/M55 WorkCentre Pro 35/45/55 System Administration CD1, Document Number 538E08770

[2] CopyCentre C35/C45/C55 WorkCentre M35/M45/M55 WorkCentre Pro 35/45/55 Training and Information CD2, Document Number 538E08780

- 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™ M35/M45/M55 Copier-Printer or WorkCentre™ Pro 35/45/55 Advanced Multifunction System machine. This screen 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.
- 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, once enabled, is manually invoked. Follow the instructions in the **Installation → Options→ Installation → On Demand Image Overwrite** tab 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.*
- 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.

3. The Embedded Fax Card must be installed in accordance with the instructions in the **Installation → Options→ Installation → Embedded Fax** tab 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 User Guide[2].
4. The certified configuration includes four patches, two for the Network Controller and two for HTTP, to Network Controller software versions 1.02.166.01, 1.02.266.01 and 1.02.366.01. The four patches can be obtained from http://www.xerox.com/security by linking to Xerox Security Bulletins XRX04-006, XRX04-007, XRX04-009 and XRX04-010, respectively. The four patches should be installed in the following order – the Network Controller patch documented in Xerox Security Bulletin XRX04-006 first, the HTTP patch documented in Xerox Security Bulletin XRX04-007 second, the HTTP patch documented in Xerox Security Bulletin XRX04-009 third and finally the Network Controller patch documented in Xerox Security Bulletin XRX04-010 last. After loading these four patches, please check the system Configuration Report to confirm that the Net Controller Software Version line lists 1.02.166.01.P8.P10.P17.P18, 1.02.266.01.P8.P10.P17.P18, or 1.02.366.01.P8.P10.P17.P18. If the System Configuration Report does not confirm that the Network Controller Software Version is one of these three versions, please contact Xerox Customer Support for assistance in getting your machine to the secure configuration. Further information about the issues resolved by the three patches can be found at http://www.xerox.com/security.
5. Before upgrading software on a WorkCentre™ M35/M45/M55 Copier-Printer or WorkCentre™ Pro 35/45/55 Advanced Multifunction System machine via the Manual/Automatic Customer Software Upgrade or, 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 (Auto Upgrade web page).
6. System Administrator login is required when accessing the security features of a WorkCentre™ M35/M45/M55 Copier-Printer or WorkCentre™ Pro 35/45/55 Advanced Multifunction System 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 machines Web Browser.

7. A reboot of the system software for a WorkCentre™ M35/M45/M55 Copier-Printer or WorkCentre™ Pro 35/45/55 Advanced Multifunction System 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.

8. Caution: A WorkCentre™ M35/M45/M55 Copier-Printer or WorkCentre™ Pro 35/45/55 Advanced Multifunction System 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.

9. The following Special Purpose pages are available from the Web User Interface with System Administrator login and authentication: These pages provide additional system configuration capability

   - **Exported Scan Files -** Allows the setting of the PDF encoding format for scanned files. Is accessible by typing **http://{IP Address}[3]/diagnostics/index.dhtml and** then selecting 'Exported Scan Files' from the **Diagnostics** Content Menu.
   - **Raw TCP/IP Printing -** Allows the user to enable/disable and modify several attributes for Raw TCP/IP Printing. Is accessible by typing **http://{IP Address}/diagnostics/index.dhtml and** then selecting '**Raw TCP/IP Printing**' from the **Diagnostics** Content Menu.
   - **LPR/LPD -** Allows the user to enable or disable PDL switching over LPR/LPD. Is accessible by typing **http://{IP Address}/diagnostics/ lprlpdhidden.dhtml**.
   - **This item is deleted. ~~SC Log~~ -** ~~Displays a read-only list of the last 50 entries in the Network Controller System Control (SC) log. Is accessible by typing **http://{IP Address}/diagnostics/ sclog.dhtml**.~~
   - **Secure Print Release All -** Allows the user to release all of the user's secure print jobs at one time with the same user name and password. Is accessible by typing **http://{IP Address}/diagnostics/ secureReleaseAll.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}/diagnostics/ secureattr.dhtml**.
   - **Sever Fax Edge Erase -** Allows the user to set the desired border edge erase value for a Server Fax job. Is accessible by typing **http://{IP Address}/diagnostics/index.dhtml and** then selecting '**Server Fax Edge Erase**' from the **Diagnostics** Content Menu or by typing **http://{IP Address}/diagnostics/serverfaxedgeerase.dhtml**.

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



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