Secure Installation and Operation of Your Xerox Multi-Function Device

Version 1.0

August 6, 2012

Secure Installation and Operation of Your Xerox Multi-Function Device

Purpose and Audience

This document provides information on the secure installation and operation of a Xerox Multi-Function Device (MFD). All customers, but particularly those concerned with secure installation and operation of these machines, should follow these guidelines.

Overview

This document lists some general customer information and guidelines that will ensure that your Xerox MFD is operated and maintained in a secure manner.

Some Xerox MFDs have their own product-specific secure installation and operation guidelines; if that is the case the product-specific guidelines supersede and should be used in place of the general guidelines documented here.

Not every Xerox MFD may have all of the security functions discussed in these guidelines; follow only those guidelines below that apply to the security function(s) provided with your Xerox MFD.

Guidelines

1. Please follow the general guidelines below for secure installation, setup and operation of a Xerox MFD[1]:

   a). The security functions that should be set up by the System Administrator are:
   - Immediate Image Overwrite
   - On Demand Image Overwrite
   - Disk Encryption
   - IP Filtering
   - Audit Log
   - Secure Sockets Layer (SSL)
   - Trusted Certificate Authorities
   - IPSec
   - SNMP v3
   - Local, Remote or Smart Card Authentication (if so equipped)
   - Local Authorization and Personalization
   - 802.1x Device Authentication
   - Session Inactivity Timeout
   - Secure Print

   System Administrator login to either the Local User Interface (Local UI) or Web User Interface (Web UI), as applicable, is required when accessing the security features or when implementing the guidelines and recommendations specified in this document. To log into either the Local UI or Web UI as an authenticated System Administrator, follow the applicable instructions in the System Administration Guide (SAG) for your Xerox MFD.

   Also follow the appropriate instructions located in the SAG for your Xerox MFD to set up the security functions or to implement the guidelines noted in this document, except as indicated in the items below. Note that whenever the SAG requires that the System Administrator provide an IPv4 address, IPv6 address or port number the values should be those that pertain to the particular machine being configured.

   b). Change the Administrator password[2] as soon as possible after installation.
   - Set the Administrator password to a minimum length of eight alphanumeric characters.
   - Change the Administrator password once a month.
   - 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.).

   c). The following passcodes should be changed on a regular basis, chosen to be as random as possible and set to the indicated minimum lengths:
   - Smart Card or CAC passcode/password – 8 characters (alphanumeric)
   - Secure Print passcode/password – 6 numeric digits
   - Scan To Mailbox passcode/password – 8 characters (alphanumeric)

[1] In this document the guidelines included only apply when the MFD has the feature(s) to which the guidelines apply. For example, guidelines covering creation of individual user accounts would not apply to an MFD that does not have the ability to set up local user accounts.

[2] In this document the term "passcode" will be used to represent a password that consists entirely of digits and the term "password" will be used to represent a password that consists of alpha-numeric and special characters.

d). The System Administrator should establish or ensure that unique user accounts are established for all users, and that local usernames established on the Xerox MFD match domain names and both map to the same individual.

The System Administrator should also ensure that the ‘Minimum Length’ passwords for any unique user accounts established for all users should be set to at least 8 (alphanumeric) characters unless applicable internal procedures require a minimum password of a greater length. The ‘Maximum Length’ can be set to any value between 8 and 63 (alphanumeric) characters consistent with the same internal procedures.

e). The ability to delete a job at either the Local UI or Web UI should be set so that only the System Administrator can delete a job.

f). For customers concerned about document files on the hard disk drive(s) or Embedded Fax card memory the Immediate Image Overwrite and On Demand Image Overwrite security features, which come installed on a Xerox MFD, must be properly configured and enabled.

Notes:

- Immediate Image Overwrite of a delayed or secure print job will not occur until after the machine has printed the job.
- If an Immediate Image Overwrite fails, an error message will appear at the top of the screen indicating that there is an Immediate Image Overwrite error and that an On Demand Image Overwrite should be run. This error message will persist until an On Demand Image overwrite is initiated by the System Administrator.
- 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 hard disk drive(s). The System Administrator should immediately invoke an On Demand Image Overwrite once the machine has been restored.
- Once a manual or scheduled On Demand Image Overwrite has been initiated from either the Local UI or Web UI, as applicable, it cannot be aborted.
- The System Administrator has the option of scheduling either a Standard or Full On Demand Image Overwrite from the Web UI.
- Before invoking an On Demand Image Overwrite verify that:
  - There are no active jobs, pending print or scan jobs, no active processes that will access the hard drive(s).
  - No user is logged into a session via network accounting, Xerox Standard Accounting, or the internal auditron, or into a session accessing a directory on the hard disk drive(s).
  - After a power on of the machine all subsystems must be properly synced and, if printing of Configuration Reports is enabled, the Configuration Report must have finished printing.
  - For any previously initiated On Demand Image Overwrite request the confirmation sheet must have finished printing.
  - 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 system reboots.
- If an On Demand Image Overwrite fails to complete because of an error or system crash, a system reboot or software reset should first be initiated by the System Administrator from either the Local UI or the Web UI and be allowed to complete; otherwise, the Local UI may become unavailable. If the Local UI does become unavailable the Xerox MFD will have to be powered off and then powered on again to allow the system to properly resynchronize. Once the system reboots or software reset has completed the System Administrator should immediately perform another On Demand Image Overwrite.
- If there is a failure in the hard disk drive(s) 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.
- The System Administrator should perform an On Demand Image Overwrite immediately before a Xerox MFD is decommissioned, returned, sold or disposed of.

g). The Xerox MFD can be restricted to use only SSLv3/TLSv1 by putting the device into “FIPS mode”. See the SAG for instructions.

h). For SSL to work properly the machine must be assigned a valid, fully qualified machine and domain name (FQDN).

i). When utilizing (SSL):

- 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 Xerox MFD and installed in the certificate store of the user's browser.

j). Enable HTTPS. The HTTPS protocol should be used to send scan jobs to any remote IT product.

k). When utilizing Secure Sockets Layer (SSL) for secure scanning:

- SSL should be enabled and used for secure transmission of scan jobs.
- When storing scanned images to a remote repository using an https: connection, a Trusted Certificate Authority certificate should be uploaded to the Xerox MFD so the Xerox MFD 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”.

l). Remote authentication using Kerberos will not work with Windows Server 2003. In the case of LDAP/LDAPS the System Administrator should ensure that SSL is enabled.

m). In viewing the Audit Log the System Administrator should note the following:

- Deletion of a file from the Reprint Saved Job folders or deletion of the Reprint Saved Job 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.
- Extraneous process termination events (Event 50) may be recorded in the Audit Log when the Xerox MFD is rebooted or upon a Power Down / Power Up. Extraneous security certificate completion status (Created/Uploaded/Downloaded) events (Event 38) may also be recorded.

n). In downloading the Audit Log the System Administrator should ensure that Audit Log records are protected after they have been exported to an external trusted IT product and that the exported records are only accessible by authorized individuals.

o). IP Filtering is not available for either the AppleTalk protocol or the Novell protocol with the ‘IPX’ filing transport. Also, IP Filtering will not work if IPv6 is used instead of IPv4.

p). Before enabling disk encryption the System Administrator should make sure that the Xerox MFD is not in diagnostics mode and that there are no active or pending scan jobs:

q). IPSec should be used to secure printing jobs; HTTPS (SSL) should be used to secure scanning jobs. Note: IPSec is not available for either the AppleTalk protocol or the Novell protocol with the ‘IPX’ filing transport.

The default values for IPSec parameters should be used whenever possible for secure IPSec setup. The following default values typically not listed in the product System Administrator Guide should also be used for secure IPSec setup:

- For defining policies the options listed for ‘Hosts’, ‘Protocols’ and ‘Action’ are all defaults; the System Administrator should choose the particular option that pertains to whether the hosts and protocols in each case are to be allowed or discarded and the corresponding desired action.
- The Host Group address type defaults to ‘Specific’.
- Protocol Group Custom Protocol defaults to being disabled. If Custom Protocol is enabled then the protocol defaults to ‘TCP’ and the Xerox MFD IS type defaults to ‘Server’.
- The IPSec New Actions keying method defaults to ‘Internet Key Exchange (IKE)’.
  - If ‘Manual Keying’ is selected “AH” alone should not be selected as the IPSec Security option.

r). The software verification test feature initiated from the Web UI that checks the integrity of the executable code by comparing a calculated hash value against a pre-stored value to ensure that the software has not changed.

s). The System Administrator should enable the session inactivity timers (termination of an inactive session), for both the Web UI and Local UI.

t). Private folders are available for storing confidential information when using the Scan to Mailbox feature. To use private folders, the scan policies for the Scan to Mailbox feature should be set as follows:

- Deselect [**Allow Scanning to Default Public Folder**].
- Deselect [**Require per Job password to public folders**].
- Select [**Allow additional folders to be created**]
- Select [**Require password when creating additional folders**].
- Select [**Prompt for password when scanning to private folder**].
- Deselect [**Allow access to job log data**].

u). Print jobs (other than a LANFax job) submitted to a Xerox MFD from a client or from the WebUI should be submitted as a secure print job.

v). Software upgrades via the network should normally be disabled except for those periods when software upgrades are being deployed.

2. Change the SNMP v1/v2c public/private community strings from their default string names to random string names.
3. Sign up for the RSS[3] subscription service available via the Xerox Security Web Site (Security@Xerox) at www.xerox.com/security to receive the latest Xerox Product Security Information and timely reporting of security information about Xerox products, including the latest security patches .
4. A Xerox MFD should be installed in a standard office environment. Office personnel should be made aware of authorized service calls (for example through appropriate signage) to discourage unauthorized physical attacks such as attempts to remove the internal hard disk drive(s). The System Administrator should also ensure that office personnel are made aware to pick up the outputs of print and copy jobs in a timely manner.
5. Customers who encounter or suspect software problems should immediately contact the Xerox Customer Support Center to report the suspected problem.
6. Caution: the Xerox MFD 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 configuration is maintained.
7. Depending upon the configuration of a Xerox MFD, two IPv4 addresses - a primary IPv4 address and a secondary IPv4 address - may be utilized. The System Administrator selects whether the primary IPv4 address will be obtained statically or dynamically via DHCP. The second IPv4 address is assigned via APIPA (Automatic Private IP Addressing) when the System Administrator enables the 'Self Assigned Address' option. If the 'Self Assigned Address' option is enabled (which is the default case), this secondary IPv4 address will not be visible to the SA[4]. Xerox recommends that the 'Self Assigned Address' option be disabled unless either APIPA is used or Apple Rendezvous/Bonjour support is required.
8. If a system interruption such as power loss occurs a job that is in process may not be fully written to the hard disk drive(s). 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.
9. If IPv6 is disabled and then a software upgrade is performed by a Xerox Service Technician using an AltBoot, IPv6 will still be disabled even though both the Local UI and Web UI show that IPv6 is enabled. IPv6 can be enabled again by re-enabling it on the Web UI.
10. A unique Embedded Fax or Scan-to-Mailbox mailbox should be established for each authenticated user.
11. Remote Polling should only be used by the System Administrator.
12. The Embedded Fax cover sheets should be set to not be printed with an Embedded Fax job.
13. Users should be aware that correct remote repository document pathnames for the receipt of workflow scanning jobs should start with one '\' as opposed to the two '\'s shown in a number of SAG documents.
14. Users should undergo appropriate training on how to use a Xerox MFD in a secure manner before being assigned user accounts to access the device.

[3] 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] The primary IPv4 address will always be displayed on the Configuration Report.

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 not allow the exclusion or limitation of liability for consequential damages so the foregoing limitation may not apply.

The information in this document is subject to change without notice.