Version 1.0
July 10, 2017

Secure Installation and Operation

Xerox® VersaLink® Multifunction and Single Function Printer

Document Version: 1.0 (January 2017).

Secure Installation and Operation of Your VersaLink® Multifunction and Single Function Printer

Purpose and Audience

This **docum**ent provides information on the secure installation, setup and operation. All customers, but particularly those concerned with secure installation and operation of these devices, should follow these guidelines.

Overview

This document lists some important customer information and guidelines[1] that will ensure that your device is operated and maintained in a secure manner.

I. Secure Installation and Set-up

To set up the machines in a secure manner, follow the guidelines below:

a. Set up and configure the following security protocols and functions in the evaluated configuration:

- Immediate Image Overwrite
- On Demand Image Overwrite
- Data Encryption
- FIPS 140-2 Mode
- IP Filtering
- Audit Log
- Security Certificates, Transport Layer Security (TLS)/Secure Sockets Layer (SSL) and HTTPS
- IPsec
- Local, Remote or Smart Card Authentication
- Local or Remote Authorization
- User Permissions
- Personalization
- 802.1x Device Authentication
- Session Inactivity Timeout
- USB Port Security
- Embedded Fax Secure Receive
- Secure Print
- S/MIME

System Administrator authentication is required when accessing the security features and administrative functions of the device or when implementing the guidelines and recommendations specified in this document. To log in as an authenticated System Administrator via the Embedded Web Server Interface (denoted hereafter as the Web UI), follow the instructions under "Accessing the Embedded Web Server as a System Administrator" under "Accessing Administration and Configuration Settings" in Section 2 of the applicable System Administration Guide (SAG)[2].

To log in as an authenticated System Administrator via the Local User Interface (denoted hereafter in this document as the Control Panel), follow "Accessing the Control Panel as a System Administrator" under "Accessing Administration and Configuration Settings" in Section 2 of the SAG.

To log in as an authenticated user who is not the System Administrator 'admin' user, follow the instructions for "Accessing the Embedded Web Server as a System Administrator" under "Accessing Administration and Configuration Settings" in Section 2 of the applicable System Administration Guide (SAG), except that instead of entering 'admin' for the User ID and the system administrator password the user should enter his/her User ID and his/her authentication password.

For secure operation do not use the 'Simple Login' method.

b. Follow the instructions located in Chapter 4, Security, in the SAG to set up the security functions listed in Item a above. 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 device being configured.

---

[1] All guidelines in this document apply to the System Administrator unless explicitly stated otherwise.
[2] Xerox® VersaLink® Series Multifunction and Single Function Printers System Administrator Guide, Version 1.1, April 2017

In setting up the device to be in the evaluated configuration, perform the following[3]:

1. ***Authentication Passwords***:

   Authentication passwords for unique user accounts established for all users and System Administrators should be set by the System Administrator to a minimum length of 8 alphanumeric characters unless applicable internal procedures the System Administrator must comply with require a minimum password of a greater length (the minimum length can be set to any value between 1 and 63 alphanumeric characters). Authentication passwords should always be strong passwords by using a combination of upper case and lower case letters, digits, and allowable special characters ("!", "@", "#", "$", "%", "^", "&", "*", "(", ")", and other printable ISO 8859-15 set and Unicode/UTF-8 set characters except ">"), not use common names or phrases, etc.

   The 'maximum length' can be set to any value between 8 and 63 (alphanumeric) characters consistent with the same internal procedures. Follow the instructions for "Configuring Password Rules" under "Setting Parameters for Login, Logout and Passwords" in Section 4 of the SAG to set both the minimum and maximum user authentication password lengths.

2. ***Administrator Password***:

   i. Change the Administrator password upon installation. Reset the Administrator password periodically. Change the Administrator password once a month. To change the Administrator password follow the instructions under "Changing the System Administrator Password" in Section 2 of the SAG.

3. ***Authentication***:

   i. Establish local authentication at the device via the Web UI by following the "Setting the Local Login Method" instructions in Section 4 of the SAG.

      Set up unique user accounts with appropriate credentials (user names and passwords) on the device for all users who require access to the device via the Control Panel or Web UI by following the "User Database" instructions in Section 4 of the SAG.

   ii. Establish network (remote) authentication access to network accounts from the Web UI by following the "Setting the Network Login Method" instructions in Section 4 of the SAG to set up an Authentication Server. For the most secure network authentication, the preferred authentication types are **Kerberos** or **LDAP**.

      When configuring network authentication using LDAP/LDAPS, make sure SSL is enabled for LDAP by following the instructions for enabling SSL for LDAP in "Configuring Settings for SSL/TLS" under "Managing Settings for SSL/TLS" in Section 4 of the SAG.

   iii. Establish user authentication via a Smart Card and smart card reader by following the "Setting the Smart Card Login Method" instructions in Section 4 of the SAG.

   Note that there is one other authentication methods available on the device – Convenience Authentication. Although local, network and smart card authentication are the preferred authentication methods, if use of Convenience Authentication is desired follow the "Setting the Convenience Authentication Method" instructions in Section 4 of the SAG to set up Convenience Authentication.

4. ***Authorization***:

   i. Establish authorization at the device by following the "Configuring Authorization Settings" instructions in Section 4 of the SAG.

      When adding new device and print user roles, follow the instructions for "Adding a New Device User Role" and "Creating a Customer Print User Role", respectively, under "Configuring Authentication Settings" in Section 4 of the SAG. Follow the applicable instructions under "Configuring Authentication Settings" to copy, edit or delete a device user or print user role.

      To add users to a device user or print user role, follow the instructions for "Adding Members to a Role" under "Configuring Authentication Settings" in Section 4 of the SAG.

   ii. For secure operation of the device, set the permission for all Guest Access (see "Roles and Level of Access" under "Configuring Authentication Settings" in Section 4 of the SAG) to **No Access** for Control Panel Permissions and

[3] The instructions for setting up the device in the Evaluated Configuration assume that the System Administrator has been successfully authenticated as a System Administrator at either the Control Panel or Web UI following the instructions in section I.a of this document.

setup Custom Permissions for Device Website Permissions to **Restrict** access to Home, Address Books and all Jobs.

iii. If network authorization using LDAP is desired, follow the "Configuring LDAP Permission Groups" instructions under "Configuring Authentication Settings" in Section 4 of the SAG. Make sure to only follow the instructions pertaining to setting up an LDAP Server.

5. ***Personalization***: Enable personalization by following the instructions for ""Configuring LDAP User Mappings" under "LDAP" in Section 3 of the SAG.

6. ***Immediate Image Overwrite*** (Only for VersaLink Multifunction Printers that have a Hard Disk Drive): Follow the instructions under 'To enable Disk Overwrite' under 'Managing Disk Overwrite" under "Managing Disk Drives" in Section 4 of the SAG to enable Immediate Image Overwrite from the Web UI.

7. ***Security Certificates***: Install a digital certificate on the device before enabling SSL/TLS by following the appropriate instructions under "Security Certificates" in in Section 4 of the SAG for installing any one of the three types of digital certificates – Device Certificates, CA Certificates and Trusted Certificates - the device supports. Note that the default certificate comes already installed on the device when it comes out of manufacturing, so the System Administrator has the option of using the default certificate already installed on the device or create a new certificate.

   Follow the instructions for "Selecting a Certificate" to select a certificate already uploaded onto the device for use.

   To import a certificate follow the instructions for "Importing a Certificate". Note that to import a certificate HTTPS must be enabled (see I.b.8).

   To create a self-signed certificate to use on the device follow the instructions for "Creating a Certificate".

   If no Device Certificate is available, the device can automatically create a self-signed certificate by following the instructions for "Enabling Automatic Self-Signed Certificates".

   If a CA certificate is desired a Certificate Signing Request (CSR) will have to be sent to a Certificate Authority to obtain the CA Certificate before it can be installed on the device; follow the instructions for "Creating a Certificate Signing Request" under "Security Certificates" in Section 4 of the SAG to create the CSR.

   If desired, certificate path validation can be performed by following the instructions for "Enabling Certificate Path Validation".

   Finally, set the options for certificate revocation by following the instructions for "Configuring Settings for Certificate Revocation".

8. ***Transport Layer Security (TLS)/Secure Sockets Layer (SSL)***:

   Note that on VersaLink devices SSL has been removed so only TLS is supported.

   i. Follow the instructions under 'Configuring DNS Settings" (under "Configuring IP Settings in the Embedded Web Server" under "IP") in Section 3 of the SAG for entering the host and domain names, to assign the machine a valid, fully qualified machine name and domain from the Web UI (required for SSL to work properly).

   ii. Enable HTTPS from the Control Panel or Web UI, respectively, by following the instructions for "Enabling HTTPS at the Control Panel" or "Enabling HTTPS in the Embedded Web Server" under "Managing Settings for SSL/TLS" in Section 4 of the SAG.

   iii. Configure SSL/TLS by following the instructions for "Configuring Settings for SSL/TLS" under "Managing Settings for SSL/TLS" in Section 4 of the SAG. For the most secure operation make sure that the 'HTTP – SSL/TLS Communication', 'LDAP – SSL/TLS Communication' and 'SMTP – SSL/TLS Communication' options are all toggled to be enabled and that SSLv3.0 is disabled in favor of TLS v1.x to avoid vulnerabilities associated with downgrading from TLS to SSLv3.0. The device has the ability to only use either TLS 1.0, TLS 1.1 and TLS 1.2 or a combination of the three. For secure operation disable TLS 1.0 by performing the following:

   - Access the WebUI by typing https://{IP Address of the device}.
   - Authenticate as a System Administrator (see I.a).
   - Select **System > Security > SSL/TLS Settings**.
   - Make sure the 'TLS 1.0' checkbox is not selected.
   - Click **OK**.

9. ***FIPS 140-2 Mode***: Encryption of transmitted and stored data by the device must meet the FIPS 140-2 Standard. Enable the use of encryption in "FIPS 140 mode" and check for compliance of certificates stored on the device to the FIPS 140-2 Standard by following the instructions for "FIPS 140-2" under "Managing Network Security Settings" in Section 4 of the SAG.

Since Kerberos and SNMPv3 are not FIPS compliant secure protocols, make sure when enabling FIPS mode that you set up the proper exceptions for both Kerberos and SNMPv3.

10. ***Data Encryption***: Disk encryption is automatically enabled on a VersaLink device and cannot be disabled.
11. ***IP Filtering***: Enable and configure filtering of IP addresses by following the instructions under "Configuring Filters for IP Addresses" in Section 4 of the SAG.

    Note also that a zero ('0') should be used and not an asterisk ('*') if a wildcard is needed for an IP address to be filtered.
12. ***Audit Log***:

    Enable the audit log, download the audit log .csv file and then store it in a compressed file on an external IT product using the Web UI by following the instructions for then audit log in "Downloading a Log File" under "Network Logs" in Section 4 of the SAG.

    The System Administrator should download and review the main Audit Log and protocol log files on a daily basis.

    The main Audit Log can contain up to 15,000 entries. Once the Audit Log is full it will overwrite the oldest event with the new event information, and it will keep logging events this way until the main Audit Log is cleared.

    The System Administrator should be aware that there is the possibility that on an intermittent basis multiple entries may be included in the audit log for the same event.
13. ***IPSec***: Enable and configure IPSec by following the instructions under "IPsec" in Section 4 of the SAG. Note that IPSec should be used to secure printing jobs; HTTPS should be used to secure scanning jobs. Use the default values for IPSec parameters whenever possible for secure IPSec setup.
14. ***Session Inactivity Timeout***: Enable the session inactivity timers (termination of an inactive session) from the Web UI by following the instructions for "Setting System Timeouts" in Section 4 of the SAG.

    The default session timeout limits are 90 seconds for the Control Panel and 20 minutes for the Web UI.
15. ***Secure Print***: For best security print jobs (other than LANFax jobs) submitted to the device from a client or from the Web UI should be submitted as a secure print job. To ensure that print jobs can only be submitted as secure print jobs, set up the Printing User Roles (see I.b.4) as follows:

    - Under Basic Printing User select **Edit**.
    - Select **Custom Permissions** and then touch **OK**
    - Under 'Allowed Print Types' toggle **Secure** to enabled and toggle the other print types to disabled.
    - Touch **OK**
16. ***802.1x Device Authentication***: Enable and configure 802.1x device authentication from the Control Panel by following the instructions for "802.1x" under "Managing Network Security Settings" in Section 4 of the SAG.
17. **USB Port Security**: Enable or disable the USB Ports using the Web UI by following the instructions for "Enabling and Disabling USB Ports" under "USB Port Security" in Section 4 of the SAG.
18. **S/MIME**: S/MIME should be enabled and configured for supporting MIME data for scan to email by following the instructions for "S/MIME" In Section 3 of the SAG.

c. The following protocols, services and functions should be enabled when needed:

- TCP/IP
- Date and Time
- Copy
- Embedded Fax
- Fax Forwarding on Receive (for received Embedded Faxes)
- Scan to E-mail
- Scanning
- Scan to USB
- Print from USB
- SNTP
- SNMPv3
- Wireless

When setting up the device to be secure, perform the following special setup for the above services (otherwise follow the appropriate instructions in the appropriate section of the SAG to set up and/or configure the protocol/service/function):

1. ***TCP/IP***:

   - Enable and configure IPv4 and IPv6 from the Control Panel by following the instructions for "Configuring IP Settings at the Control Panel" under "IP" in Section 3 of the SAG.

   - Enable and configure IPv4 and IPv6 from the Web UI by following the instructions for "Configuring IP Settings in the Embedded Web Server" under "IP" in Section 3 of the SAG.

2. ***Date and Time***:

   - Ensure that the date and time on the device is correct and is set for the correct time zone where the device is located. Set the date and time from the Control Panel by following the instructions in "Setting the Date and Time" under "Initial Setup at the Control Panel" in Section 2 of the SAG.

     Set the date and time from the Web UI by following the instructions in "Setting the Date and Time" under "Initial Setup in the Embedded Web Server" in Section 2 of the SAG.

     The 'Date and Time Setup' option can be set to either manual time and date settings or configuring SNTP settings (see 1.c.6).

3. ***Embedded Fax***:

   - Ensure that Embedded Fax is properly installed. The procedure for sending an Embedded Fax and the features and settings available to a user for configuring/sending an Embedded Fax are described under the Fax section of the applicable User Guide.

   - Set Embedded Fax parameters and options on the device by following the instructions for "Configuring General Settings and Policies" under "Faxing" in Section 8 of the SAG.

   - Enable and set (Embedded Fax) Secure Receive passcode from the Control Panel by performing the instructions for setting **Secure Fax Receive** in "Configuring the Fax Settings at the Control Panel" under "Configuring General Settings and Policies".

   - Enable Fax Forwarding on Receive by performing the instructions for setting **Fax Forwarding** in "Configuring the Fax Settings at the Control Panel" under "Configuring General Settings and Policies".

4. ***Scan to Email***:

   - Set the domain filtering to limit the domains to which Scan to E-mail jobs can be sent. Enable the domain filtering option by following the instructions under "Setting Up Scanning to an Email Address" in Section 7 of the SAG and making sure the **Domain Filtering** option is set to either 'Allow Specific Domains" or 'Block Specific Domains' and the domains to be allowed or blocked are defined.

   - Configure authentication of SMTP to send Scan to Email jobs or to forward received Embedded Faxes via email by following the instructions for **SMTP Authentication** under "Setting Up Scanning to an Email Address" in Section 7 of the SAG. Make sure to select SSL/TLS for the Connection Security..

5. ***Scanning***:

   - Set the domain filtering to limit the domains to which scanning jobs can be sent. Enable the domain filtering option by following the instructions for the scan to destination of interest in Section 7 of the SAG and making sure the **Domain Filtering** option is set to either 'Allow Specific Domains" or 'Block Specific Domains' and the domains to be allowed or blocked are defined.

   - In a secure configuration FTP should be disabled. In the instructions for FTP in Section 3 of the SAG, make sure FTP is not toggled to enabled.

   - For Scan to My Folder follow the instructions for "Scanning to My Folder on the Printer" in Section 7 of the SAG; it is preferable from a security perspective that the login method used to access each user's folder on the device is either Network or Smart Card authentication.

   - For Scan to USB follow the instructions for "Scanning to USB" in Section 7 of the SAG.

6. **SNTP**:

   - If it is desired to use an NTP server to synchronize and set the internal system time used by the device, follow the instructions under "SNTP" in Section 3 of the SAG.

7. **SNMPv3**:

- SNMPv3 cannot be enabled until SSL and HTTPS (SSL) are enabled on the machine. To enable SNMPv3 follow the instructions for "Configuring SNMPv3" under "SNMP" in Section 3 of the SAG.

  Be aware that in configuring SNMPv3 there is the option of resetting both the Privacy and Authentication passwords back to their default values. This option should only be used if necessary since if the default passwords are not known no one will be able to access the SNMP administrator account[4].

8. **Wireless**:

   - Connection of the printer to a wireless network from a security perspective is not considered totally secure. However, if such a connection is absolutely required, follow the instructions for either "Connecting to a Wireless Network from the Control Panel" or Connecting to a Wireless Network Using the Embedded Web Server" as applicable, in Section 2 of the SAG. Make sure that for security settings WPA2 is enabled and configured and WEP is disabled.

d. The following additional features and protocols are not considered secure and should be used at the discretion of the device user:
   - Xerox Extensible Interface Platform®
   - Accounting
   - Internet Fax
   - Use of Embedded Fax mailboxes
   - Xerox App Gallery

e. Customer software upgrades should not be enabled for general use. Administrators should only enable software upgrades when performing an upgrade, and software upgrades disabled when complete. Software upgrades can be enabled/disabled by following the instructions for 'Enabling Upgrades' under 'Updating the Printer Software' in Section 10 of the SAG.

f. Firmware verification that software upgrade files for the device are properly certified for that device should be enabled by following the instructions for "Enabling Firmware Verification" in Section 4 of the SAG.

g. Following internal customer policies and procedures required to evaluate and install devices in your environment.

III. Secure Operation of Device Services/Functions

a. Change the following passcodes on a regular basis, choose passcodes to be as random as possible and set them to the indicated minimum lengths:
   - Smart Card or CAC passcode – 8 characters (alphanumeric)
   - Secure Print passcode – 6 digits

b. Ensure that local usernames established on the device match domain names and that both map to the same individual.

c. Operation of IIO and ODIO (only for VersaLink Multifunction Printers that have a Hard Disk Drive):

   1. If a manual ODIO is to be run set up and initiate a manual ODIO follow the "To Start a Disk Overwrite Manually" instructions under "Managing Disk Drives" in Section 4 of the SAG.
   2. If a scheduled ODIO is to be run set up and initiate a scheduled ODIO follow the "To Schedule a Disk Overwrite" instructions under "Managing Disk Drives" in Section 4 of the SAG.
   3. IIO of a delayed or secure print job will not occur until after the machine has printed the job.
   4. If an overwrite fails, the error is handled as system failure and an error message is displayed on Control Panel.
   5. ODIO is not executed when device is in the following status:
      - Device power is turned off or device is being shut down
      - Device is being initialized
      - System failure occurs
   6. When system failure occurs while this function is in progress, after completing transition to system failure status, the device reboots regardless of system failure type.
   7. Even if there is a reserved job such as Delayed Print and Delayed Fax, the documents are deleted.

[4]The SNMP administrator account is strictly for the purposes of accessing and modifying the MIB objects via SNMP; it is separate from the System Administrator "admin" user account or user accounts given SA privileges by the System Administrator "admin" user. The administrator account cannot perform any System Administrator functions.

8. 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. Immediately initiate a full ODIO once the machine has been restored.
9. Once a manual or scheduled ODIO has been initiated, it cannot be aborted.
10. For a scheduled ODIO, If, upon switching back to Standard Time from Daylight Saving Time, the scheduled time is arrived at for a second time in the same day, this feature is not executed.
11. Perform a Full ODIO immediately before the device is decommissioned, returned, sold or disposed of.

e. The device supports the use of TLS 1.0; SSLv2.0, SSLv3.0, RC4 and MD5 have been removed on the device. However, customers are advised to set the crypto policy of their clients to request either TLS 1.1 and TLS 1.2 and to disallow the use of TLS 1.0. The cryptographic module supports additional ciphers that may be called by other unevaluated functions.

Using the device in FIPS mode will automatically restrict the device to using TLS 1.x only.

f. Audit Log Notes:

- In viewing the main Audit Log the System Administrator should note the following:
  - ✓ Audit Log entries can sometimes include extraneous characters.
  - ✓ Extraneous events may be recorded in the Audit Log.
  - ✓ Duplicate audit log entries may appear in the Audit Log for some events.
  - ✓ Download and review the Audit Log on a daily basis. 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.

g. Be careful for IP Filtering not to reject incoming TCP traffic from all addresses with source port set to 80; this will disable the Web UI. Also, configure IP filtering so that traffic to open ports from external users (specified by subnet mask) is dropped.

h. Ensure the user permission roles names do not contain single quotes (‘) or double quotes (“).

i. Users should be provided with appropriate training on how to use the device in a secure manner before being assigned user accounts to access the device.

j. Users experiencing problems logging in to the device using the Web UI only on a particular web browser are advised to switch to a different web browser.

k. The device 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 drive(s). Ensure that office personnel are made aware to pick up the outputs of print and copy jobs in a timely manner.

l. Caution: The device allows an authenticated System Administrator to disable functions like Disk Overwrite that are necessary for secure operation. Periodically review the configuration of all installed machines in your environment to verify that the proper evaluated configuration is maintained.

m. System Administrators should avoid opening emails and attachments from unknown sources unless the emails and attachments have been properly scanned for viruses, malware, etc.

n. System Administrators and users should:

- Whenever possible use a browser to access the Web UI whose only purpose is to access the Web UI.
- Always logoff the browser immediately after completing any tasks associated with accessing the Web UI.
- Not allow the browser to either save their username/password or “remember” their login.
- Follow secure measures, only use browsers with TLS 1.0 and above and not open any malicious links or documents with their browser.

u. The latest general software release available from www,xerox.com can be found by accessing the following in the order stated:

- Select the **Support** > **Support and Drivers** links
- In the text box enter the model number of your device. A menu list of all Xerox devices with that model number will appear; select the one that corresponds to the product you have.
- Select the **Drivers & Downloads** link
- Scroll down the resultant page; under ‘Firmware’ will be the latest general release. Click on the release link and a page will be displayed that allows you to download the release onto a desired location.

v. Additional items:

1. All passwords entered on the Control Panel for authentication purposes will be obfuscated by '*'s. All passwords entered on the WebUI for authentication purposes will also be obfuscated, but the character that does the obfuscation will depend on the web browser used. This applies to all the models covered by these guidelines.
2. The System Administrator does not have to configure or perform any actions to utilize the random number generation needed for key generation and for the encryption algorithms the products covered by these guidelines use for the security features described in I. and III.
4 Change the SNMPv1/v2c public/private community strings from their default string names to random un-guessable string names of at least 8 characters in length.
5 Customers should sign up for the RSS[5] subscription service available 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.
6 Customers who encounter or suspect software problems should immediately contact the Xerox Customer Support Center to report the suspected problem and initiate the SPAR (Software Problem Action Request)[6] process for addressing problems found by Xerox customers.

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 the evaluated configuration.

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

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

[5] 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.

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