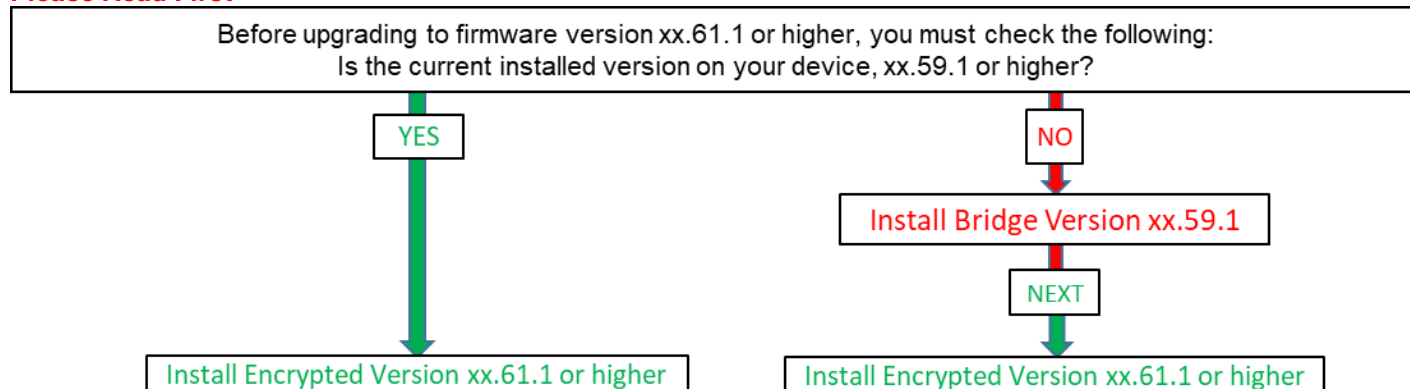# Xerox® VersaLink® Product Enhancements Document for Version xx.73.72 & xx.73.92

Description of new features and enhancements to the products specified below.

Release Date: March 10, 2023   dc23rn4142

Please Read First

Before upgrading to firmware version xx.61.1 or higher, you must check the following:
Is the current installed version on your device, xx.59.1 or higher?

YES	NO
	Install Bridge Version xx.59.1
	NEXT
Install Encrypted Version xx.61.1 or higher	Install Encrypted Version xx.61.1 or higher

In addition to the encrypted firmware file, Clone files have increased security and data validation.
Clone files created prior to firmware release xx.61.1 cannot be applied to this version or higher. A new clone file will need to be created for future use. Clone files created with firmware version xx.61.1 or newer cannot be applied to devices running older versions of firmware. Please see 'Versalink Firmware Installation v8.pdf' for more information.

Firmware Release Details

Products SPAR Release xx.73.72 & xx.73.92 (encrypted) (Click on product name to access software)	System Version	Controller ROM Version	Products *Bridge Release (Click on product name to access software)	System Version (cont 1.69.0)
Xerox® VersaLink® C7000	56.73.72	1.86.2	Xerox® VersaLink® C7000	56.59.1
Xerox® VersaLink® C7020/7025/7030	57.73.92	1.86.4	Xerox VersaLink C7020/7025/7030	57.59.1
Xerox® VersaLink® B7025/7030/7035	58.73.92	1.86.4	Xerox VersaLinkB7025/7030/7035	58.59.**11**
Xerox® VersaLink® C8000/C9000	70.73.72	1.86.2	Xerox® VersaLink® C8000/C9000	70.59.1
Xerox® VersaLink® C8000W	72.73.72	1.86.2	NA	NA
Phaser 6510	64.73.72	1.86.2	Phaser 6510	64.59.1**1**
Windows Installer Only v5.3.7.2			Windows Installer Only v5.3.7.2	
Mac Installer			Mac Installer	
WorkCentre 6515	65.73.72	1.86.2	WorkCentre 6515	65.59.**11**
Windows Installer Only v5.3.7.2			Windows Installer Only v5.3.7.2	
Mac Installer			Mac Installer	

Plugin Release Details

VersaLink Card Reader Plug-ins v13	Version
Xerox USB Card Reader	3.0.11
Modernized CAC Smart card Service Plugin	3.0.0
GemNet Smart card Service	1.0.18
CCID Terminal Plug-in	1.2.1
TWN4 Card Reader Service	1.0.0

Note: These Smartcard plugins are newer than what is available on Xerox.com and requires system firmware version xx.61.23 or later to provide all functionality.

Contents

Xerox® VersaLink® Product Enhancements Document 3

Latest release information:

Product Firmware Release xx.73.72 & xx.73.92 (NW1.5 PL7-R11)

1. Delete Jobs on Logout

Improved behavior of feature - This system-level setting allows a user's jobs to be deleted from the device when a user logs out. When enabled, this feature will delete the user's job(s) when the user logs out at the device LUI.

When Delete Jobs on Logout is enabled, print jobs belonging to the user in the following states will be deleted on logout or power down:

- Processing (physically printing, or decomposing)
- Held
- Pending
- Paused (including paused jobs due to a fault)

Jobs which are displayed on the Jobs App (Panel) at the time of logout or power down will be deleted. This includes pending jobs awaiting decomposition.

Caveats: Follow You Printing
When using a Follow You print workflow, job processing time is more difficult to gauge. Jobs may be flowing in from external submission applications and/or may be large or long jobs. It is recommended that the user be fully aware of the job sets that are printing or processing in the Job Panel. If the user logs out of the device before all their job(s) have been received by the device, they run the risk of a job printing which they may not have intended after they log off.

2. Various bug fixes

- When the Versalink device uses "eMMC", then the Configuration sheet will correctly display as "eMMC" instead of "SD Card'
- After each POPO, while authenticating for the first time using the remote-control panel, the letters for the password will be masked and will not be reflected on the UI.
- Logged in users secure print jobs are not released following the Secure Print Job Policy setting has been resolved in this version. Note: Fix for this issue is available only in C70xx & B0xx. This issue will be fixed for the other VL devices in a future cadence release.
- When LDAP Authentication server is set on the WUI using hostname instead of IP address, then the issue of prompting to register the card multiple times for Prox card LDAP card authentication has been resolved.
- A faulty fuse resulted in this Booter Failed error condition. From this version, the device will now display fault code 062-395 on the LUI whenever IIT power malfunctions (faulty fuse) are detected.

Product Firmware Release xx.69.91 (NW1.5 PL7-R10)

1. SNMP Web Service Extensions

EIP SNMP Web Service Extensions adds additional capabilities which include being able to get and set multiple OIDs with a single web service request, being able to do a get-next operation on multiple OIDs with a single web service request, being able to get all OIDs in a subtree in a single "walk" operation and being able to set the output format of the OID string values to either ASCII or Hex string.

2. SW Upgrade via Print File

This provides the user the ability to upgrade the firmware remotely where port 9100 and the Web UI will not be available

3. Various bug fixes

- Xerox Workplace Kiosk app will work properly with Controller 1.81.1
- Scan to Home using Microsoft domain-based DFS with Smartcard Login will be successful if a DNS PTR Record does not exist. Fixed the error "Job Deleted. No messages were sent. Login error".
- Fixed the frequent display of the message "An authorized user is making changes..." on the LUI in this version.

- From this version, when initializing or repairing XWS on machine, the RCP function will not get disabled.
- When ECDHE cipher suites are enabled, then convenience authentication (PIN or card) will be successful.
- Fault Code 10-331 which occurs shortly after device installation has been fixed in this version.
- With this version, Server Fax application will work with XSM folder disabled
  NOTE: The feature to remove creation of the XSM folder for scans was not intended for Server Fax. The device behavior now properly creates XSM folders and successfully scans jobs using Server Fax even when the feature to remove creation of the XSM folder is enabled.

Product Firmware Release xx.69.51 (NW1.5 PL7-R9)

Warning: This PL7-R9 release does not contain the fix for "Fault Code: 10-331". So, the customers who are currently experiencing this fault code issue, are requested NOT to upgrade to PL7-R9. Kindly retain PL7-R8-U3 version until the next SPAR release PL7-R10. Any current customers experiencing this issue, should be provided with PL7-R8-U3 release only.

1. Proximity Card LDAP Login & Card Registration

Enables the user to self-register their proximity card to the LDAP server and once registered, enables users to Login with Proximity card to the configured LDAP server without any additional prompts. The user may also use Alternate Login via manual Username and Password entry to authenticate via the configured Network Authentication Server.
Note:
This feature requires an Elatec TWN4 proximity card reader to be connected to the MFD
This feature requires the EIP_API_Card_Reader_Service_Plugin be installed and activated.

See configuration instructions below.

1. Configure ability for Self-registration of user proximity card to LDAP:
    - Enter System credentials to allow the MFD to read/write card ID from/to LDAP on webpage: Permissions-> Login/Logout Settings-> Login Method -> Network -> Select Edit
        i. Set Network Login to "LDAP" Authentication Protocol.

        Note: To reliably apply changes made under any of the four LDAP setting details (LDAP servers, LDAP user mapping, LDAP authentication, Custom Filters) user should select Done, and then must select Restart Later in the restart pop-up.

        User will be taken back into the LDAP setup screen. When user selects Done in this screen a pop up with options Cancel and Change will appear. Select Change, which will cause the device to reboot. LDAP will then be set as the authentication mode and any changes made to the LDAP settings will be applied.

        ii. Set LDAP Servers/Directory Services page, Advanced Settings:
            1. Set Login Credentials for Database Search to be "Predefined"
            2. Set Login Credentials for Database Search, Enter Login Name and Password.

2. Configure Proximity card LDAP login & registration on webpage: Permissions-> Login/Logout Settings-> Advanced Settings, Select Edit.
    - Under Authentication Settings enable Proximity Card LDAP Server Authentication.
    - Enter LDAP server attribute name where the card ID will be written to / read from.

3. Install compatible card reader: an Elatec TWN4 proximity card reader must be connected to the MFD

4. Install compatible card reader plug-in.
    - From System -> select Plug-in Settings

- If "Xerox_USB_Card Reader_DPV_v3.0.11_sig.jar" is installed, select it, select Deactivate and Remove.
- Download latest version of VersaLink CardReader_Plug-ins from Xerox.com and unzip the folder.
- Open the EIP_API_CardReader _Plugin folder and copy the EIP_API_Card_Reader_Service_Plugin to your hard drive.
- On Plug-in Settings, select Add Plugin.
- On Add Plug-in window, click Select and navigate to the downloaded EIP_API_Card_Reader_Service_Plugin
- Select OK to upload the Plug-in.
- On the Plug-in Settings webpage, select the "EIP_API_Card_Reader plugin" then Restart to Activate

2. Delete Jobs On Logout

Enables system level setting to Delete a user's Job(s) when the user logs out.

Caveats:
- Auto Clear Timer does not pause while logged in user's jobs are printing. While a job is printing, if the auto clear timer expires, a message will be given that user's jobs will be deleted. If user does not select Continue Working (complete the job), then user is logged out and their job deleted.
- When using Convenience Authentication, if the job is held for resources, the user is not logged out after the system timer expires. Therefore, no jobs will be deleted.
- When jobs are released from Convenience Authentication solutions (such as Equitrac's Follow You Print), not all jobs may be deleted on logout. Whether the user logs out manually or if the system timer logs the user out, any of the user's jobs still in transfer from the App or already queued will not be deleted and still print.

3. Various bug fixes
- With this version, when Smart Card user fails to authenticate to the authentication server, the device will give a proper Authentication Failed message instead of the screen showing "Verifying your Passcode" with a spinner.
- After 47k web service calls, device will return the responses properly.
- Fixed an unexpected error, while attempting to disable printing protocols such LPD, IPP, Port 9100 on performing certain SET operations using EIP SNMP API tool.
- From this release, Card-Swipe login to Clustered PaperCut Server will be successful after a Failover condition
- With this version, Versalink devices will use reserved port 68 for lease renewal and the devices will not fall off the Network during DHCP expiry.

Product Firmware Release xx.68.81 (NW1.5 PL7-R8)

1. SFR 20659 Enable secondary domain controllers within same domain when using Kerberos

When Kerberos authentication is selected, the ability to add Alternate Servers with different IP Address within the same Realm as the Default Server is now supported.
The total number Kerberos servers allowed is 50 whether they are in same or different realms (except WC6515 which support 5 servers).

2. Various bug fixes
- With this version, users can print using the Client Xerox Workplace Cloud application successfully. Error code 116-324 is resolved, and the users can use the copy, print, and scan services anymore without any issues.

Product Firmware Release xx.68.62 (NW1.5 PL7-R7-U2)

1. Secure Print Jobs Release Policies

Secure Print Job Release policies have been added to the WebUI on the Jobs / Policies / Secure Print Job Settings webpage. The Policies include:
- Manual Release of Secure Print Jobs <Default>.
  - This is the device previous behavior.
- Always Auto-Release Secure Print Jobs When User Logs-in
  - When this new capability is enabled, at login, if the user has secure print jobs held on the device, they will all be printed.
- Confirm Before Auto-Release Secure Print Jobs When User Logs-in.
  - When this new capability is enabled, at login, if the user has secure print jobs held on the device, the user will be prompted "You have one or more jobs being held. Do you want to print them now?". The user may select either "Not Now" or "Print All".

Product Firmware Release xx.68.31 (NW1.5 PL7-R7)

1. Various bug fixes
- With this version, VersaLink device will print the barcode along with human readable text using installed fonts "LibreBarcode39Text-Regular.ttf and LibreBarcode128Text-Regular.ttf".
- Support for new LUI IC chips has been added for future use.
- Changes have been made in SB/LX finisher firmware to protect the fuse from cutting-off and avoid an issue that could lead to finisher failure.
- Fixed an intermittent fuser error while printing large volumes of paper whose width is less than 148mm.
- Fixed an Error 016-322, "JBA Account Full RAP" after enabling Network Accounting.
  Fixed with caveat: If you have network accounting enabled and have JBA data still in the device JBA log (JBA data that has not been retrieved by the Accounting server) and then you disable and re-enable JBA on the device, the device deletes the existing data in the JBA log.

Product Firmware Release xx.67.91 (NW1.5 PL7-R6)

1. Support to Print Compressed Jobs via the Print from URL Submission
This release adds support for printing compressed jobs submitted from Print From URL. File types supported for compressed jobs is gzip.

2. Support for SMB dialect v3.1.1
Support for SMB dialect v3.1.1 has been added.

SMBv3.1.1 will be enabled by default.

The legacy dialects 1 through 3 will also be enabled by default. NVMs to enable/disable SMB legacy dialects are as follows.
- SMB1:   771-925 (0: disabled, 1: enabled [default])
- SMB2:   771-926 (0: disabled, 1: enabled [default])
- SMB3:   771-927 (0: disabled, 1: enabled [default])
- SMB3.1.1: 772-101 (0: disabled, 1: enabled [default])

Cloning will not carry over the value of the NVM. The NVM must be set on the local UI.

Product Firmware Release xx.66.91 (NW1.5 PL7-R5)

1. Increase SMTP password to 128 characters
This release adds the ability to support SMTP password length longer than 60 Characters for Outgoing SMTP Authentication. SMTP password length max supported is 128 characters.
Many mail server applications now begin enforcing MFA on all User accounts and starting to use API key (essentially a 69 Character password) for SMTP Authentication.

2. Bypass mode support for Bypass Tray

This release adds the ability to support the jobs to print to any media loaded in the Bypass Tray by suppressing the mismatch between the media that is in the tray and the media specified in the print job. The media to be used for the job is in the discretion of the user.

The following SFR key is required to enable/disable Bypass Mode for the C8000/C9000:

Product Model	Enablement Key	Disablement Key
Xerox® VersaLink® C8000/C9000	*3023420751	*3023420750

Specific Details when Bypass Mode is enabled:
- In Bypass Mode and the tray is not empty, the print job will always print on the media in the Bypass Tray.
- In Bypass Mode, the user will not be prompted to enter media attributes when the Bypass Tray is loaded.
- In Bypass Mode and the bypass tray is empty but an internal tray has the correct media, the internal tray will be used
- In Bypass mode when there is no media in the bypass tray and an internal tray does not have the media that matches the job, the user shall be notified to add media in a tray based on the tray priority. If the size is allowed only for the bypass tray, it will be selected.
- Paper size of Bypass tray shall utilize the current paper size setting, which has been set with non-bypass mode most recently. If media size/type needs to be modified, disable Bypass Mode, remove and reinsert media in Bypass tray, change media size on Media Popup screen then and re-enable Bypass Mode.

3. Addition of DHCP IPv6 Unique Identifier (DUID) to Configuration Sheet

The DHCP IPv6 Unique Identifier (DUID) in Link Layer format will be displayed on the printed configuration sheet when IPv6 is enabled. The DUID information is labeled "DUID (DHCP Unique Identifier)" under the Protocols heading. Additionally, the DUID identifier can be obtained from the EWS Configuration Report when IPv6 is enabled

4. New CIS (Contact Image Sensor) support has been added for A4 Models.

062-396 Error when loading System Software lower than xx.66.01 on to a Tag #10 Device.
Tag #10 Devices are not compatible with System Software below xx.66.01. Due to a factory fire, alternative components needed to be sourced for manufacturing of CIS used in the IIT assembly. The new part requires changes to the System Software to support the change and is not compatible with older System Software. The new components are installed in devices manufactured with Tag #10

5. Various Bug Fixes

- Fault code (18-505) no longer occurs while scanning to the Isilon server.
- In this release, device pulls correct hostname from DHCP server
- With this version, Scanning the printer with NMAP will show TCP port 3000 as closed
- When language is set to French, AZERTY layout keyboard will be shown in Email - To, Cc, BCC Fields.

Product Firmware Release xx.66.11 (NW1.5 PL7-R4)

1. SIPRNet Plug-ins Upgrade

This release adds the ability to upgrade / downgrade the SIPRNet plug-ins from the Web UI via the System / Plug-in Settings webpage. To install new SIPRNet plug-ins, upload the new plug-ins to the device and restart the device to activate. After the device has restarted, the old plug-ins will have been removed and the new plugins are activated.

2. Hardware reliability improvements

Fault code 062-396 when loading System Software lower than xx.66.01 on a machine with tag #10 hardware components. Devices with tag #10 hardware are not compatible with System Software below xx.66.01. Alternative components needed to be sourced for manufacturing of CCD Lens Kits used in the IIT assembly. The new part requires changes to the System Software to support the change and is not compatible with older System Software. The new components are installed in devices manufactured with Tag #10

3. Security Fix

This release corrects a parameter validation issue in the PJL interpreter that could result in 116-324 errors in the field."

4. Various bug fixes

- Reduction of 024-747 faults when printing Comm10 Envelopes.
- Some Hungarian characters are no longer missing.
- Important A4 device reliability improvements added to this version. It is strongly recommended that A4 devices be upgraded to this version or higher.

Product Firmware Release xx.65.51 (NW1.5 PL7-R3)

5. Mask User's Names in Job Queue

This release enables the ability to conceal the User's name in the LUI and Web UI job Queue. This feature must be enabled with Conceal Job Names. The settings for this feature can be found on the Web UI in the Jobs Tab under Policies.

Conceal Job Names
- ⭕ Show All Job Names
- 🔵 Conceal All Job Names

Conceal User Names
- ⭕ Show All User Names
- 🔵 Conceal All User Names

6. Various bug fixes

- Fault code 116-324 no longer occurs during card swipe
- BOOTER FAILED message no longer occurs while performing clone file using the parameters in "Protocol" section in device webpage
- Remote command injection is not possible to perform using the clone file
- Ability to receive the email notifications, has been improved
- Finisher firmware has been upgraded from 2.6.0 to 2.8.0 to address the fault code 041-391 which occurred while trying to login into LUI

Product Firmware Release xx.65.21 (NW1.5 PL7-R2)

1. Print From URL to support concurrent spooling and rendering on the active job

This release adds support for concurrent spooling and rendering of multi-page active job submitted from Print From URL. File types supported are PCL and Postscript.

2. Ability to perform scan to home using the NetApp Filer/Appliance

Scan to home with smartcard login no longer results in fault code 018-505 when scanning to a NetApp Filer/Appliance

3. Improvements to Wireless connection

This version fixes the display of fault code 018-426 which displays in device LUI until device is rebooted manually. With this version, reboot is not required to clear the fault code 018-426. Once the device is connected to wireless network with good signal quality, fault code 018-426 will be cleared automatically.

4. Vulnerability fixes

TLS Padding Oracle Vulnerability (Zombie POODLE and GOLDENDOODLE) will no longer be detected in the device while running Qualys scan

Product Firmware Release xx.64.51 (NW1.5 PL7-R1)

1. Ability to send an encrypted email to a recipient where the destination email address is different than what is contained in the destination recipient's email encryption certificate.

This version fixes a problem where if the scan to email recipient's email address in the "To:" field is different from the email address that is contained within the recipient's encryption certificate retrieved from LDAP.

Product Firmware Release xx.64.1 (NW1.5 PL7)

1. Remote Services Communication Fix

A software problem has been fixed that caused some devices to stop communicating to the Xerox Remote Servers if the feature was enabled. This services provide meter reads and supplies usage to automate replenishment billing.

Product Firmware Release xx.61.23 (PL6-R3 re-spin)

1. Improvements to ECHDE Ciphers

This version fixes an issue that could result in 116-324 faults when using the ECHDE cipher feature logging into a solution with convenience authentication. It is recommended that you upgrade to at least this version if you are going to enable the ECHDE cipher feature. The ECHDE Cipher enablement codes are found in the PL5-R1 section.

2. EIP SNMP Web Service improvement

Enabling only SNMP v3 on the device no longer impacts the use of the EIP SNMP Web service.

3. Firmware and Clone file security enhancements

Starting with firmware version xx.61.1 the actual firmware file is encrypted. This was done to provide increased security for the VersaLink software. Devices with firmware versions xx.52.1 and older, cannot utilize an encrypted software file to perform a firmware upgrade. The xx.59.1 release can read the encrypted file and act as a bridge from the old version to the new version. A bridge version must be installed before installing the encrypted file.

In addition to the encrypted firmware file, Clone files have increased security and data validation. Clone files created prior to firmware release xx.61.1 cannot be applied to this install or higher. A new clone file will need to be created for future use. Clone files created with firmware version xx.61.1 or newer, cannot be applied to devices running older versions of firmware

4. SMBv3 support for encryption and signing (only)

This release adds support for SMBv3 with the 3.0.0 dialect. Also supports scan to encrypted SMBv3 shares.

5. Display installed SFR Keys on device printed and downloadable configuration sheet

With this release any installed SFR key will be displayed on the printed configuration report under the heading of "Special Features". The SFR key will also be displayed on the downloadable configuration report. This will enable the customer to know if any hidden features are enabled on the device. SFR key consists of 4-digit product-unique number which will be masked, 5-digit feature number, and 1-digit of feature enablement. Eg: ****456781.

6. Ability to strip domain info for SMB Authentication

This feature provides for the following ability for SMB authentication:
- Use the username only (the domain will be removed) in cases where the user specifies a user ID in NetBIOS format (i.e. domain/username).
- Use the user ID as entered by the user when user ID is in the sAMAccountName or? userPrincipalName format (i.e. username and username@domain).

   The following keys are used to enable and disable this feature.

Product	Enablement Key	Disablement Key
VersaLink C405 (MFP)	*5002482911	*5002482910
VersaLink B405 (MFP)	*5003482911	*5003482910
WC 6515	*5005482911	*5005482910
VersaLink B7025,B7030,B7035	*5004482911	*5004482910
VersaLink C7020.C7025,C7030	*5014482911	*5014482910
VersaLink C505/C605 MFP	*5016482911	*5016482910
VersaLink B605/B615 MFP	*5020482911	*5020482910

NOTE:
- Feature is not supported when using Kerberos tickets for SMB filing
- Feature is not supported when using Logged in user Credentials for SMB filling

7. Add dynamic data to Doc name

With this release the device support one or more codes for the dynamic data that is automatically added to the document name for all scan services (Scan To, Email, My Folder, USB). These codes can be entered by the User at time of scanning or set by the admin as part of the default file name on CWIS.

The following dynamic data codes are supported.

    a. %D date (YYYYMMDD)
    b. %T time (24 hour format)
    c. %Y year
    d. %H hour
    e. %M minute
    f. %S second
    g. %m month
    h. %d day of month
    i. %sn device serial number
    j. %ui user id
    k. %ji job id
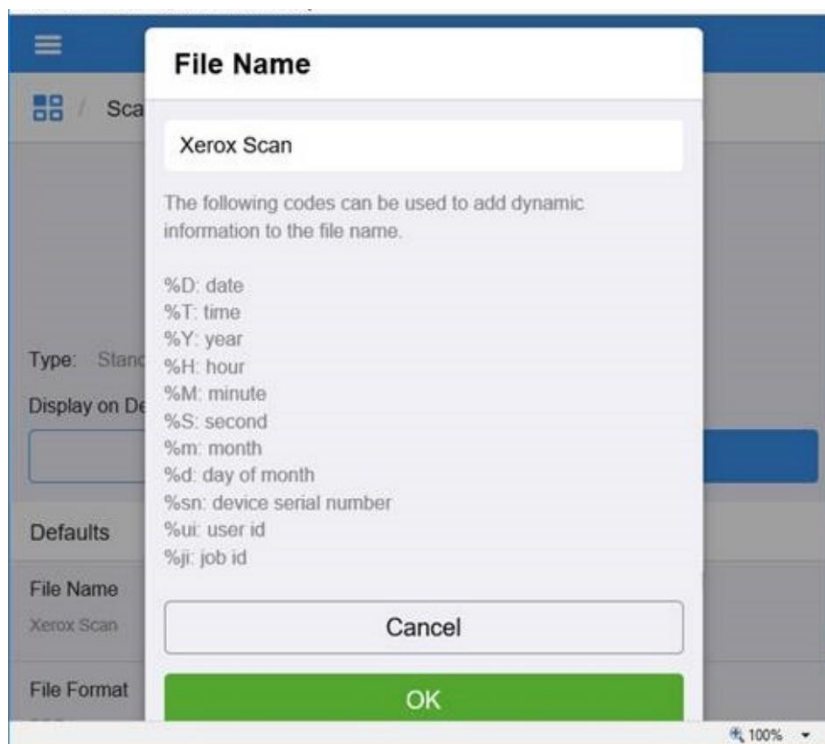
8. Multi-Factor Authentication support when using @PrintByXerox

Supports Multi-Factor Authentication when using @PrintByXerox app with Azure AD credentials. The device will now support a confirmation pop-up for the MFA challenge if required by the MFA provider.

9. Enable Full UPN when authenticating using a Smartcard

This feature enables the Full UPN as defined in a Users LDAP directory to be used for the User's name. This feature requires an SFR Key to enable. Without this feature enabled VersaLink does not include the User's domain information in the UPN. The full UPN is needed for many third-party applications such as Follow You Printing.

The following keys are used to enable and disable this feature

	Enable	Disable
VersaLink C405 (MFP)	*5002484521	*5002484520

VersaLink C400 (Printer)	*5006484521	*5006484520
VersaLink B405 (MFP)	*5003484521	*5003484520
VersaLink B400 (Printer)	*5007484521	*5007484520
WC 6515	NA	NA
VersaLink B7025,B7030,B7035	*5004484521	*5004484520
VersaLink C7020/C7025,C7030	*5014484521	*5014484520
VersaLink C7000 (Printer Only)	*5015484521	*5015484520
VersaLink C505/C605 MFP	*5016484521	*5016484520
VersaLink C500/C600 (Printer)	*5017484521	*5017484520
VersaLink B605/B615 MFP	*5020484521	*5020484520
VersaLink B600/B610 (Printer)	*5021484521	*5021484520
VersaLink C8000/C9000	*5023484521	*5023484520
VersaLink C8000W	*5064484521	*5064484520

Note: To enable this feature in C8000W, minimum version required is 72.65.21 (PL7-R2) or higher.

Product Firmware Release xx.55.51

1. Modernized CAC Cards Support with CAC/PIV Rollover

The plugin provides support for new Common Access Cards with reduced / realigned certificate profiles including:
- A single certificate for each major PKI function: PIV-Auth for authentication, Signature for email and document signing, and Encryption for encryption.
- Addition of an asymmetric card authentication certificate (aCAK) for physical security.
- Elimination of the Identity certificate present on previous versions of the CAC card.

The following cards/tokens are now supported:
1. Giesecke + Devrient Mobile Security FIPS201 SmartCafe Expert 7.0 with HID Global ActivID Applet v2.7.5
   ATR: 3b f9 18 00 00 00 53 43 45 37 20 03 00 20 46
2. Gemalto TOP DL V2.1 128K with HID Global ActivID Applet v2.7.4
   ATR: 3B 7D 96 00 00 80 31 80 65 B0 75 49 17 0F 83 00 90 00

This release also provides ability to search through all certificates on the card and attempt authentication with each valid certificate that supports smartcard logon before communicating failure to the end user.

Plugin Release Details

Smartcard CAC-PIV Plugins	Version
CCID_Terminal_Plug-in	1.0.0
Modernized_CAC_Smartcard_Service_Plugin	1.0.0

Note: These Smartcard plugins are newer than what is available on Xerox.com and requires system firmware version xx.55.51 or later to provide all functionality.

Product Firmware Release xx.54.21 (PL6-R2)

1. Disable XSM Folder

This feature provides for the ability to eliminate the XSM folder when scanning images that produces a single file for each image scanned in a job. When the feature key is enabled the system will store the files in the root folder as opposed to storing the images in an .xsm sub-folder.
The following keys are used to enable or disable the feature.

Product	Enablement Key	Disablement Key
VersaLink C405	*3002476371	*3002476370
VersaLink B405	*3003476371	*3003476370
VersaLink B7025, B7030, B7035	*3004476371	*3004476370

WorkCentre 6515	*3005476371	*3005476370
VersaLink C7020, C7025, C7030	*3014476371	*3014476370
VersaLink C505, C605	*3016476371	*3016476370
VersaLink B605, B615	*3020476371	*3020476370

2. Legacy FIPS 140-2 e-TYPES supported

This feature provides for the ability to perform Scan to Home when FIPS 140-2 is enabled using Legacy e-Types (FIPS Non-Compliant due to older Operating Systems)
The following keys are used to enable or disable the feature

Product	Enablement Key	Disablement Key
Xerox® VersaLink® B400	*5007477581	*5007477580
Xerox® VersaLink® B405	*5003477581	*5003477580
Xerox® VersaLink® B600 / B610	*5021477581	*5021477580
Xerox® VersaLink® B605 / B615	*5020477581	*5020477580
Xerox® VersaLink® B7025/30/35	*5004477581	*5004477580
Xerox® VersaLink® C400	*5006477581	*5006477580
Xerox® VersaLink® C405	*5002477581	*5002477580
Xerox® VersaLink® C500 / C600	*5017477581	*5017477580
Xerox® VersaLink® C505 / C605	*5016477581	*5016477580
Xerox® VersaLink® C7000	*5015477581	*5015477580
Xerox® VersaLink® C7020/25/30/35	*5014477581	*5014477580
Xerox® VersaLink® C8000/C9000	*5023477581	*5023477580
Xerox® VersaLink® C8000W	*5064477581	*5064477580

Note: To enable this feature in C8000W, minimum version required is 72.65.21 (PL7-R2) or higher.

3. Force Kerberos when SMB Scanning

This feature provides for the ability to perform scanning using Kerberos and not fall back to NTLM if it fails. Prior to this change, the device automatically would fall back (fail) and switch to NTLM
The following keys are used to enable or disable the feature

Product	Enablement Key	Disablement Key
Xerox® WorkCentre 6515	*5005477471	*5005477470
Xerox® VersaLink® B405	*5003477471	*5003477470
Xerox® VersaLink® B605 / B615	*5020477471	*5020477470
Xerox® VersaLink® B7025/30/35	*5004477471	*5004477470
Xerox® VersaLink® C405	*5002477471	*5002477470
Xerox® VersaLink® C505 / C605	*5016477471	*5016477470
Xerox® VersaLink® C7020/25/30/35	*5014477471	*5014477470

4. Subject Alternative Name (SAN) and Certificate Signing Request (CSR) file.

This SFR feature provides the ability to include a Subject Alternative Name (SAN) in the device generated Certificate Signing Request (CSR) file. A SAN is now included in the CSR by default. SANs are useful for certificates used in 802.1x network authentication. CSRs including SANs are also important for enabling automated Certificate Management Solutions. The advantage of a device generated CSR is that the private key remains on the device at all times, where an externally generated CSR would need to include the private key. See the table below for SFR keys to disable the feature. The most plausible reason to disable the SAN is if you are using a Commercial/Public CA and experience higher certificate costs with the SAN and you determine the SAN is not required.

Note: Ultimately it is up to Certificate Authority (CA) and its configuration whether or not the final signed certificate based on a CSR with a SAN actually includes the SAN in the final signed certificate. With this SFR enabled, the CA has the SAN available to it.

† Warning: Since the CSR SAN entry is now enabled by default, the SFR Key ending in 1 disables the new CSR SAN Feature. That is, the purpose of the key is to allow for disablement of the CSR SAN entry. This may be opposite many SFR Keys where 1 enables the new feature that in many other cases is off by default. Another way of thinking of it is that the Enablement Key is provided to change the default behavior.

Product	†Enablement Key	†Disablement Key

VersaLink C405	*3002475651	*3002475650
VersaLink C400	*3006475651	*3006475650
VersaLink B405	*3003475651	*3003475650
VersaLink B400	*3007475651	*3007475650
WorkCentre 6515	*3005475651	*3005475650
Phaser 6510	*3008475651	*3008475650
VersaLink B7020/7030/7035	*3004475651	*3004475650
VersaLink C7020/7025/7030	*3014475651	*3014475650
VersaLink C7000	*3015475651	*3015475650
VersaLink C605/C505	*3016475651	*3016475650
VersaLink C600/C500	*3017475651	*3017475650
VersaLink B605/B615	*3020475651	*3020475650
VersaLink B600/B610	*3021475651	*3021475650
VersaLink C8000/C9000	*3023475651	*3023475650
VersaLink C8000W	*3064475651	*3064475650

Note: To enable this feature in C8000W, minimum version required is 72.65.21 (PL7-R2) or higher.

5. Add C5 envelope to media list.

"C5 Envelope" is now included in the tray media pull down list when devices are configured for Metric Units.

6. Various Bug Fixes

- Printer no longer locks up when connected to certain network segments due to malformed DHCPInform packets.
- Device now displays correct IP number on the UI when WI-FI is the primary network.
- Email app displays special characters when language is Spanish or German.
- Email app 'To Address' is displayed correctly when language is set to Russian, Poski, or Croatian.
- Several fixes related to Arabic language:
  - Right to left text display for Arabic within the Web UI.
  - Email addresses in the address book are now displayed correctly when the default language is Arabic.
- Logout and Login security improvements when using SmartCard authentication.

Product Firmware Release xx.52.1 (PL6-R1)

7. Improved ECHDE Ciphers

The ECHDE Ciphers have been improved and resolves an issue that results in failed login with W2K16 or scan to email failures. The problem only occurred when the ECHDE feature was enabled. See section xx.43.x1 item 2 for ECHDE Cipher enablement details.

8. Improvements to fix fault 77-101 jams

Jam and fault 77-101 no longer occurs when copying an odd number of originals via the DADF and using the 1-2 side selection.

9. JBA Data Management Improvements

Improvements have been made to Job Based Accounting to ensure data that has been pulled from the device is correctly cleared and not pulled again.
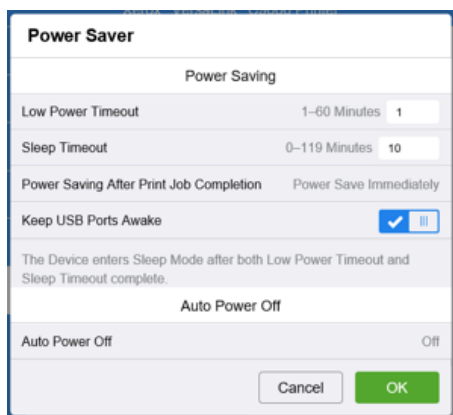
Product Firmware Release xx.50.61 (NW 1.4 PL6)

1. USB Ports Power in Sleep Mode

This release completes the implementation across the remaining VersaLink products that allows the System Administrator the ability to keep the USB Type A ports awake while the device is in Sleep Mode. This allows USB accessories connected to the USB ports to function when the device goes to sleep such as:

- o USB Smart Card readers can access and read the card, wake the device and login the user when a smart card is inserted.
- o USB Proximity Card readers can read the card, wake the device and login the user when a Prox card is swiped.
- o USB flash drive insertion can wake the device and display the "USB Drive detected" screen.

To activate: Login remotely to the device as System Administrator, navigate to System / Power Saver / Power Saving and select "Keep USB Ports Awake", select "OK".

Affected Products:

Model Name:
Xerox® VersaLink® B400 / B405
Xerox® VersaLink® B600 / B605 / B610 / B615
Xerox® VersaLink® B7025 /30/35
Xerox® VersaLink® C400 / C405
Xerox® VersaLink® C500 / C505 / C600 / C605
Xerox® VersaLink® C7000 / C7020 /25/30

2. Updates to comply with 2020 California Password law SB-327

This software release supports the California password law SB-327 effective January 1, 2020.
Upgrading existing devices to this release will have no impact on the default administrator password.
In the event a Reset to Factory Defaults operation is performed on a device after installing this release, the changes incorporated to support SB-327 will become effective, and the default administrator password for the device will be the device serial number. This is a case sensitive password.

3. Additional Language Support (Arabic)

Arabic language is now supported on the Versalink devices.

4. Energy Star 3.0 Support

Energy Star -This software release ensures our products will continue to meet Energy Star. Energy Star 3.0 means more stringent power efficiency and conservation requirements and is going into effect October,2019. This software release provides the necessary updates to meet these new specifications.

Product Firmware Release xx.45.61 (PL5-R2)
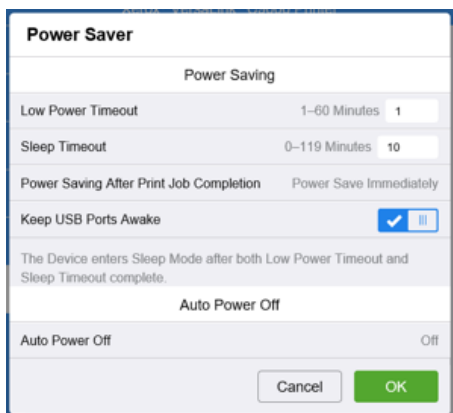
1. Additional Audit Log Events

More events for security and other settings are available in the device's Audit Log.

2. Keep USB Type A ports enabled in Sleep Mode

This release allows the System Administrator the ability to keep the USB Type A ports awake while the device is in Sleep Mode. This allows USB accessories connected to the USB ports to function when the device goes to sleep such as:

- o USB Smart Card readers can access and read the card, wake the device and login the user when a smart card is inserted.
- o USB Proximity Card readers can read the card, wake the device and login the user when a Prox card is swiped.
- o USB flash drive insertion can wake the device and display the "USB Drive detected" screen.

To activate: Login remotely to the device as System Administrator, navigate to System / Power Saver / Power Saving and select "Keep USB Ports Awake", select "OK".

Affected Products:

Model Name:
Xerox® VersaLink® B400 / B405
Xerox® VersaLink® B600 / B605 / B610 / B615
Xerox® VersaLink® B7025 /30/35
Xerox® VersaLink® C400 / C405
Xerox® VersaLink® C500 / C505 / C600 / C605
Xerox® VersaLink® C7000 / C7020 /25/30

Availability in future release (for B600 / B605 / B610 / B615)

Availability in future release (for C500 / C505 / C600 / C605)

3. Ability to query LDAP server for user email address with Smartcard Authentication

Users were not receiving their scan to email because the email address was not valid.
There was a valid email address on the LDAP server, but the device could not be configured to query the server when using smartcard authentication.
The device obtains the user's email address from the Smartcard by default.
The device can now be configured to pull email address from the LDAP server instead of from the smartcard.

When the "Enablement Key" is applied, the device will obtain the user email address from LDAP server. The "Disablement Key" will restore the default condition.

Affected Products: All Xerox® VersaLink® Multifunction Device models.

Feature Enablement Instructions:
1. On the device's Embedded Web Server select System-> Security-> Feature Enablement
2. Enter correct enable/disable code from table below.

Requirements:
- LDAP contains the user's email address and the public key encipherment certificate contains the same email address.
  Or
- LDAP contains the user's email address and the public key encipherment certificate contains a *blank* email address.

If the email address embedded in the public key encipherment certificate does *not match the user's email address on LDAP*; then the following will occur:

- Job will display on UI as complete with error code 027-708.
- The email body is blank.
- The email has no attachment.

The Feature keys are as follows: (include * character when entering)

Product Model	Enablement Key	Disablement Key
Xerox® VersaLink® B405	*3003461861	*3003461860
Xerox® VersaLink® B605 / B615	*3020461861	*3020461860
Xerox® VersaLink® B7025/30/35	*3004461861	*3004461860
Xerox® VersaLink® C405	*3002461861	*3002461860
Xerox® VersaLink® C505 / C605	*3016461861	*3016461860
Xerox® VersaLink® C7020/25/30/35	*3014461861	*3014461860
Xerox® Phaser® 6510 / WorkCentre 6515	*3005461861	*3005461860

4. SNMP / MIB Language

In software releases prior to xx.43.x1, the MIB language matched the language selected on the Local UI. This may cause issues for some remote management utilities when the device's local UI is set to a language other than English. In this release the MIB language setting is now independent of the Local UI language selection. The default language for the MIB is English and remains so regardless of the Local UI language selection.

The MIB language can be set independently if desired to a language other than English via the **prtGeneralCurrentLocalization.1** OID. As with the default setting, the MIB language set via the **prtGeneralCurrentLocalization** OID will remain independent of the Local UI language setting. The prtGeneralCurrentLocalization setting can be cloned when a clone file category "Defaults and Policies" is selected when creating the clone file.

5. Other fixes in this release

- Unable to log into printer webui as admin when connected with Google Chrome version 74.0.3729.131.
- When a DADF jam occurs during Twain scanning, the PC locks up.
- Unable to browse Webpage of VersaLink devices via DNS name if CSRF Protection feature is enabled.

Product Firmware Release xx.43.1 (PL5-R1)

1. SNMP / MIB Language

In prior software releases the MIB language matches the language selected on the Local UI. Some issues have arisen in the field with XDM and XSM (Xerox Device Manager, Xerox Supplies Manager) software when a device's local UI is set to a language other than English. In this release the MIB language setting is independent of the Local UI language selection. The default language for the MIB is English and remains so regardless of the Local UI language selection. The MIB language can be set independently if desired to a language other than English via the **prtGeneralCurrentLocalization.1** OID. As with the default setting, the MIB language setting will remain independent of the Local UI language setting. The prtGeneralCurrentLocalization setting can be cloned when a clone file category "Defaults and Policies" is selected.

2. ECDHE Cipher additions

This release adds support for the following ECDHE ciphers:
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
These ciphers can be used by any TLS communication supported by the device including the embedded web server, EIP and the XCP Plugin server communications.
These ciphers are not available for use by the EWS or EIP until a Feature Enablement Key is entered.

These ciphers are available to the XCP Plugin server as soon as the XCP Plugin server feature is enabled regardless of Feature Enablement Key entry.

The key codes below enable these ciphers. When the "Enablement Key" is applied, the ciphers are available. The "Disablement Key" will restore the default condition, i.e. ciphers are not available.
Feature Key Instructions:
1. On the device's Embedded Web Server select System-> Security-> Feature Enablement
2. Enter correct enable/disable code (include the * character)

The Feature keys are as follows:

Product Model	Enablement Key	Disablement Key
Xerox® VersaLink™ C405	*3002452891	*3002452890
Xerox® VersaLink™ C400	*3006452891	*3006452890
Xerox® VersaLink™ B405	*3003452891	*3003452890
Xerox® VersaLink™ B400	*3007452891	*3007452890
Xerox® VersaLink™ C7020/C7025/C7030	*3014452891	*3014452890
Xerox® VersaLink C7000	*3015452891	*3015452890
Xerox® VersaLink C505/C605	*3016452891	*3016452890
Xerox® VersaLink C500/ C600	*3017452891	*3017452890
Xerox® VersaLink™ B605/B615	*3020452891	*3020452890
Xerox® VersaLink™ B600/B610	*3021452891	*3021452890
Xerox® WorkCentre 6515	*3005452891	*3005452890
Xerox® Phaser 6510	*3008452891	*3008452890
Xerox® VersaLink™ B7025 / B7030 / B7035	*3004452891	*3004452890
Xerox® C8000 / C9000	*3023452891	*3023452890
Xerox® C8000W	*3064452891	*3064452890

Note: To enable this feature in C8000W, minimum version required is 72.65.21 (PL7-R2) or higher.

3. Scan to email (Gmail)
Addressed a scan to email (GMAIL) issue that could result in error 027-773 or 016-781 when the scan job consisted of multiple pages.

4. Faxing of 8.5X11 LEF
Fax send size detection issue where a LEF 8.5X11 sheet may be detected as 11X17 has been resolved.

5. IPsec enabled in Windows 10 Client
When IPsec is enabled, a Windows 10 client is now able to upgrade the printer.

Product Firmware Release xx.42.1 (NW 1.3 PL5)
This is a General Release. For more information on other features, refer to the User Manuals and the System Administration Guides on Xerox.com.

1. Improved existing Audit Log Events
Information about security settings in the device's Audit Log have been improved to include the name of the logged in user who changed the setting, identify when a security setting has been enabled or disabled, and identify what the final setting of the feature is.

2. Remote Control Panel

The Remote Control Panel feature is a way to gain access remotely into the device's Local UI. This feature can help the administrator troubleshoot the device from their PC. The Remote Control Panel can also be used to train users or simply walk them through a workflow. The Remote Control Panel feature is accessed from the Embedded Web Services (EWS). Simply open the Embedded Web Services for the device on your computer by entering the device IP address in the address bar of your web browser and select [Enter]. By default, this feature is disabled.
Please refer to the System Administrator Guide located on Xerox.com for instructions on how to enable the feature.
If the Remote Control Panel icon is not immediately visible after upgrade, perform a browser hard refresh (refer to instructions for your specific browser)

Note: This feature is available on all products except Phaser 6510. More information can be found in the System Administrator Guide located on Xerox.com.

3. Additional Language Support (Ukrainian and Croatian)

Additional language support for Ukrainian and Croatian in the Walk-up UI and the WebUI

4. Server Fax

Server Fax is now supported. Server fax allows you to send a fax over a network to a fax server. The fax server sends the fax to a fax machine over a phone line. Server fax supports FTP, SFTP, SMB, SMTP for transport types.

5. Secure Scanning Workflows

Secure scanning and browsing is added using the Secure FTP (SFTP) protocol (also referred to as SSH (Secure Socket Shell) File Transfer Protocol). SFTP ensures that data is encrypted and transferred securely over the network. SFTP support is added to the Scan To App for Browsing, Scan using Address Book Contacts, Server Fax, and EIP Scan Templates/Tickets, Scan Template Pool Repository, and Scan File Repositories.

6. Show Supported Media Sizes

This release adds the ability to show and select from the available media sizes from tray 1, improved from the existing state of only allowing for Auto Select or Custom sizes.

7. Device Alert Sounds

This release adds support for remotely configuring and managing the device Alert sounds. This includes granular controls for enable/disable of sounds as well as various audible functions in the device such as mobile connections, job completion, UI touches, logins, errors, and fax processing and ring tones. Additional details can be found in the System Administrator Guide located on Xerox.com.

8. System Alert Notifications for Firmware Updates

This release improves the software update notification system in place on VersaLink devices, adding top level UI notifications when the device detects that a firmware update is available.

9. Displaying the IPv4 Address on the Home Screen

This release adds support for displaying the device's IPv4 address on the home screen of the local UI. Additional details can be found in the System Administrator Guide located on Xerox.com.

Product Firmware Release xx.35.32

1. Enablement of Server Name Indication (SNI) on Versalink

Enablement of Server Name Indication (SNI) on Versalink as required by connector applications (DropBox, OneDrive, Office365, Blackboard, @PBX APP, @PrintByXerox).
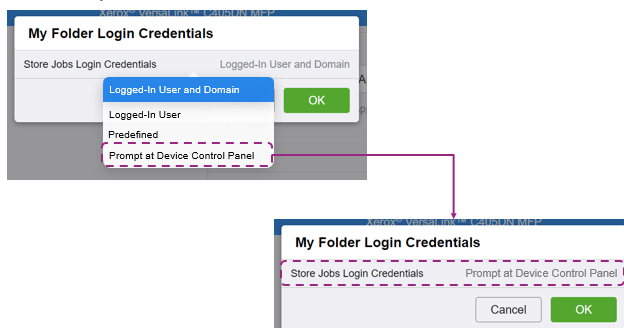**Note:** Enabled by default, no user interface to enable/disable.

2. Prompt at Device Control Panel

Prompt at Device Control Panel feature is now available for a User to enter when scanning to their Home Folder (My Folder).

o Prompt at Device Control Panel Setup

Go to **Apps**, **Scan To**, **My Folder Login Credentials**
Select Prompt at Device Control Panel as shown below. Select OK.

o When a User now performs a **Scan To Home or My Folder** job they will be prompted for login credentials as shown below. Password must be input for every scan.

Note: All translations of the Prompt at Device Control panel feature are not 100% correct. However the Prompt at Device Control panel selection will always be the bottom selection in the My Folder Login Credentials pulldown menu as shown below.
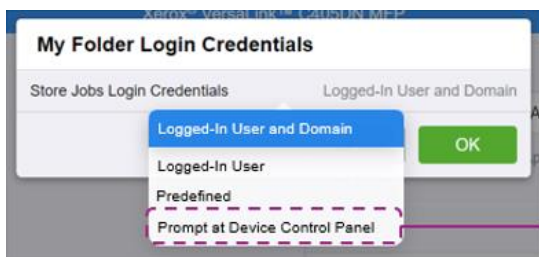
3. **Print Configuration reports as Admin Under Smart Card Authentication**

From the VersaLink front panel, "admin" users are now able to print Information and Support reports even when smart card Authentication is enabled.

Product Firmware Release xx.35.1 (PL4-R3)

1. Email addresses containing apostrophe in name

Fixed the issue to populate the email address in the 'To' field of users with an apostrophe in their name while using LDAP search at the printer control panel.

2. Fault 018-505 SMB-DOS Protocol error with Scan to Home & CAC

Scan to Home no longer fails with a 018-505 SMB-DOS Protocol Error when a DNS PTR Record does not exist for the destination Server that houses the CAC/Smartcard User's Home Directories.

Product Firmware Release xx.34.1 (PL4-R2)

1. Error message 016-404 displayed after 802.1x authentication renewal

The problem causing this customers occurrence of fault 016-404 after 802.1x authentication renewal has been fixed.

2. XML Configuration Report translate into international languages.

When the device Local UI language is changed, the XML Configuration Report will mirror the Local UI language. The XML Configuration Report is accessible to System Administrators at the bottom of the Web UI Home screen page. The Configuration Report is in XML format that can be easily viewed using any XML viewer such as Microsoft XML Notepad, a direct Microsoft download at https://www.microsoft.com/en-us/download/confirmation.aspx?id=7973.

3. Changed Fax Forward setting when convenience authentication enabled.

When convenience authentication is enabled, Fax Forwarding settings can now be set and saved properly from the local user interface.

4. Logged in user unable to delete their own jobs from LUI

A user logged with a convenience authentication system can now delete their own jobs own jobs from LUI. Once the user logs in, navigates to the applications print screen and releases their job to the printer job queue, the delete button is now operational.

Product Firmware Release xx.33.1 (PL4-R1)

1. Google Cloud Print does not require a restart to freshen the jobs queue

Once Google Cloud Print is installed and registered, printer remains online. Machine will print jobs as they are queued on the printer. No restart is required to continue refreshing the printer queue on device.

2. Display performance on Local UI when searching the Address Book

Address book will no longer display "search failed" as letters are entered when the device receives a large number of results.

3. Caveat: USB may not be recognized on Win7.x/8.x after upgrade

A device connected to a PC running Windows 7 or 8 with a USB cable may experience an issue of the device not being recognized by the PC. This issue is not expected to occur on PCs running Windows 10.
After upgrading to the release, the PC may need to update the USB driver and reassigned it to the USB Composite Device driver.
Customers may check if this issue is being seen on their Windows7.x/8.x workstations by following these steps:
1. Open [Control Panel] on the Windows 7.x/8.x Workstation
2. Customers can determine if their PC has this issue by checking the Universal Serial Bus controllers section of Device Manager
3. Depending on your version of Windows, Control Panel is usually available from the [Start Menu] or [Apps] Screen· Otherwise, follow the notes below depending upon the operating system used.

Note #1: Windows 8.x → In Windows 8, tap or click on the **Hardware and Sound** link. You could also jump right to Device Manager through the Power User Menu and not have to go through Control Panel.
Note #2: Windows 7.x → In Windows 7, look under [*System*]
4. Select the [**Hardware**] tab, and then click the [**Device Manager**] button.

With Device Manager now open, you can now view the list and select [Universal Serial Bus controllers] to identify if the problem is being seen on the Windows Workstation.
Please reference sheet shot below:
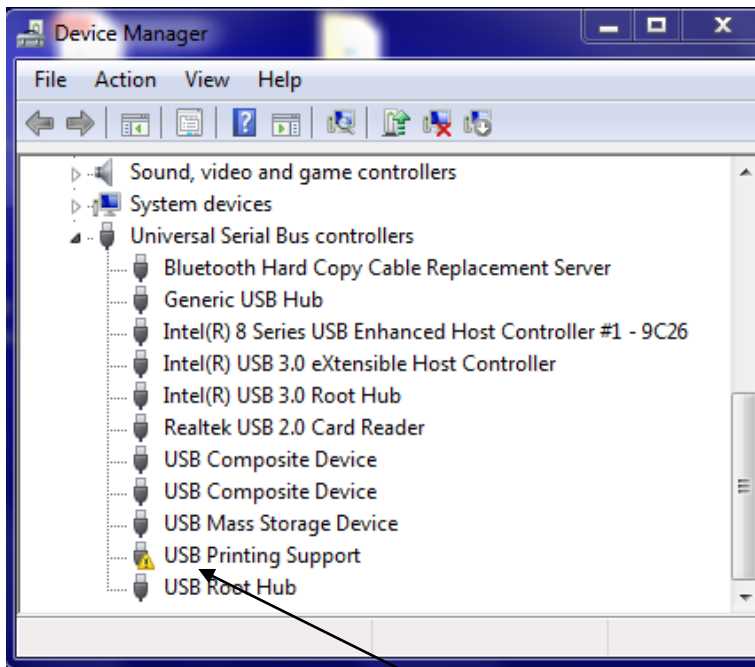
Note: Customers who have a **Yellow Warning!** next to the USB Printing Support will need to Right Click on the USB Printing Support line and select Update Driver Software.

Product Firmware Release xx.31.81 (NW 1.2 PL4)

1. USB Scanning added for Versalink A4 MFP devices

This change allows users the ability to scan directly to a PC or Mac when connected to the device via USB cable. It requires the new scan drivers that are currently available here:
Windows Scan driver
Mac Scan Driver

2. Cloning Webservice

VersaLink devices will now accept clone files from CentreWare Web via a Cloning WebService with Administrator credentials. This CWW functionality is available in the CWW release 6.0.6 or higher which can be downloaded from Xerox.com.
NOTE: This functionality should be used with CentreWare Web Release 6.0.6 or higher.

3. XML Configuration Report

VersaLink device Administrators will be able to download the Configuration Report in XML format. This capability is on the WebUI under Home, Download Configuration Report. NOTE: XML Notepad can be used for viewing the XML Configuration Report. A direct Microsoft download link is below:

https://www.microsoft.com/en-us/download/confirmation.aspx?id=7973

4. WPA2 - KRACK Vulnerability Addressed

The serious weaknesses in WPA2-suppliment, a protocol that secures all modern protected Wi-Fi networks, has been identified and fixed in this release. No longer can an attacker exploit these weaknesses using key reinstallation attacks (KRACKs) to the Xerox Printers.

Product Firmware Release xx.21.41 (NW 1.1 PL3)

1. ThinPrint

ThinPrint is a Third Party solution that saves network bandwidth by allowing print data to be compressed at the server and decompressed at the Print device before being printed out on a printer. The ThinPrint solution also supports print

data encryption prior to sending to the print device. Xerox has added the ability to accept this compressed (and encrypted if configured) print data, process the Thin Print data, and print.

Note: Xerox devices must be equipped with a hard drive or solid-state drive to utilize the ThinPrint feature.

ThinPrint WebUI
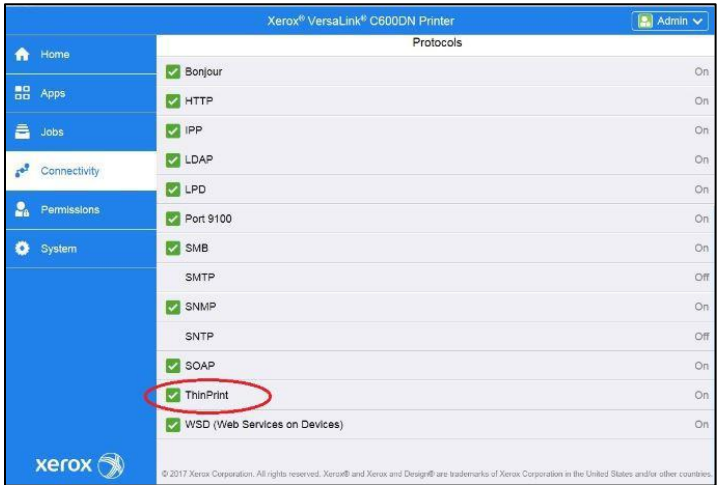
Once the ThinPrint Protocol is enabled, the Admin has access to the settings below. The port must be enabled. The default port number for ThinPrint communication is 4000.

Note: Although a different port number can be configured. It is important not enter a port number that is already in use.
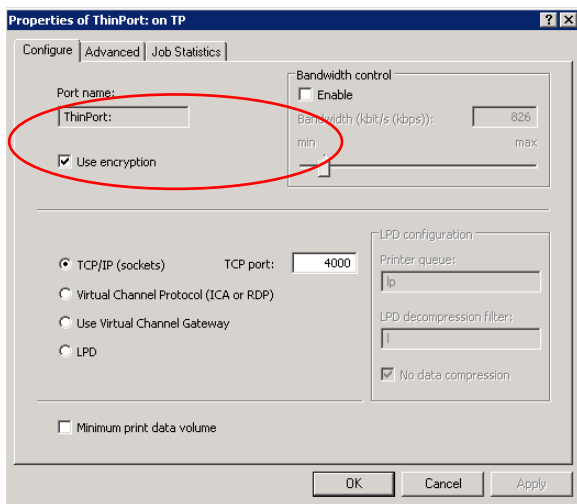

ThinPrint requires a certificate to be loaded on the device when running with TLS encryption.
This is located in System Security SSL/TLS Settings

Note: The ThinPrint Engine/Server output queue and the Xerox device ThinPrint settings must both be set to TLS encryption for print jobs to be encrypted (see more below).

ThinPrint Server Settings

ThinPrint Device Settings
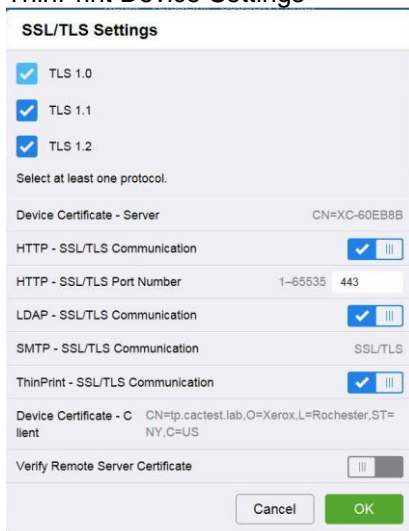
Caveats:

- Unencrypted print jobs from the server will not be accepted by ThinPrint protocol when TLS encryption is enabled on the print device.
- Cloning of the ThinPrint settings is not supported.
- Use of MIBS / OID string commands for ThinPrint settings is not supported.
- Audit Logging of the ThinPrint enablement / configuration is not supported.
- Thin Print may require the use of TLS 1.0 for encrypted job communication.
- Not applicable to Xerox® Phaser® 6510, Xerox® WorkCentre® 6515

2. Auto-populate the realm on walk-up UI

This release will automatically populate the default realm for walk-up users authenticating with Kerberos or SMB, allowing other pre-configured realms to be selected from a menu on the local user interface. The preconfigured menu will hold up to 50 Kerberos realm names or 5 SMB realm names which can be populated through the Authentication setup menu in the Embedded Web Server.

Note: An error message will appear on the walk-up UI if a user enters their fully qualified (username@realm) instead of just their username.
Not applicable to Xerox® Phaser® 6510, Xerox® WorkCentre® 6515

3. Eliminate thumbnail on fax confirmation sheet

The key codes below provide the ability to turn on/off the fax image that is printed on the fax confirmation sheet. The fax image is printed on the confirmation sheet by default. When the "Enablement Key" is applied, the faxed image will be suppressed. The "Disablement Key" will restore the default condition, displaying the fax image.

Feature Key Instructions:

1. On the device's Embedded Web Server select System-> Security-> Feature Enablement
2. Enter correct enable/disable code (include the * character)

The Feature keys are as follows:

Product Model	Enablement Key	Disablement Key
Xerox® VersaLink® B405	*3002333081	*3002333080
Xerox® VersaLink® C405	*3003333081	*3003333080
Xerox® VersaLink® B7025/30/35	*3004333081	*3004333080
Xerox® VersaLink® C7020/25/30/35	*3014333081	*3014333080
Xerox® WorkCentre® 6515	*3005333081	*3005333080

4. Remove embedded web server support for 3DES cipher suite (Sweet32)

Sweet32 is the name of an attack that takes advantage of design weaknesses in a cipher known as 3DES, or Triple-DES. Fortunately, successfully carrying out the TLS variant of the Sweet32 attack requires a very particular set of capabilities on the part of the attacker. The attacker needs to keep the victim on the web page for days, in order to execute a practical attack; researchers found that up to 785 GB of data transfer is required.
Xerox has removed this cipher from the web server components of these products, removing the possibility of an attack via the embedded web interface.

5. Default output tray setting for copy job

This feature addresses an issue for devices with the optional Office Finisher LX installed. Copy jobs without finishing options selected were limited to output the job to the Center Output Tray where offsetting cannot be performed. A new Admin accessible setting is available on the Embedded Web Server (EWS) to default copy job output to the finisher tray. This provides the ability to offset the sets with or without finishing options selected.
To change the setting:
Open EWS of the device and log in as admin.
Select Apps > Copy
Select General Settings and Policies
Select Output Destination
Selections are "Center Output Tray" (default) or "Right-Side Output Tray" (finisher).

Figure 1: Output Destination shown when optional *Office Finisher LX* is installed.

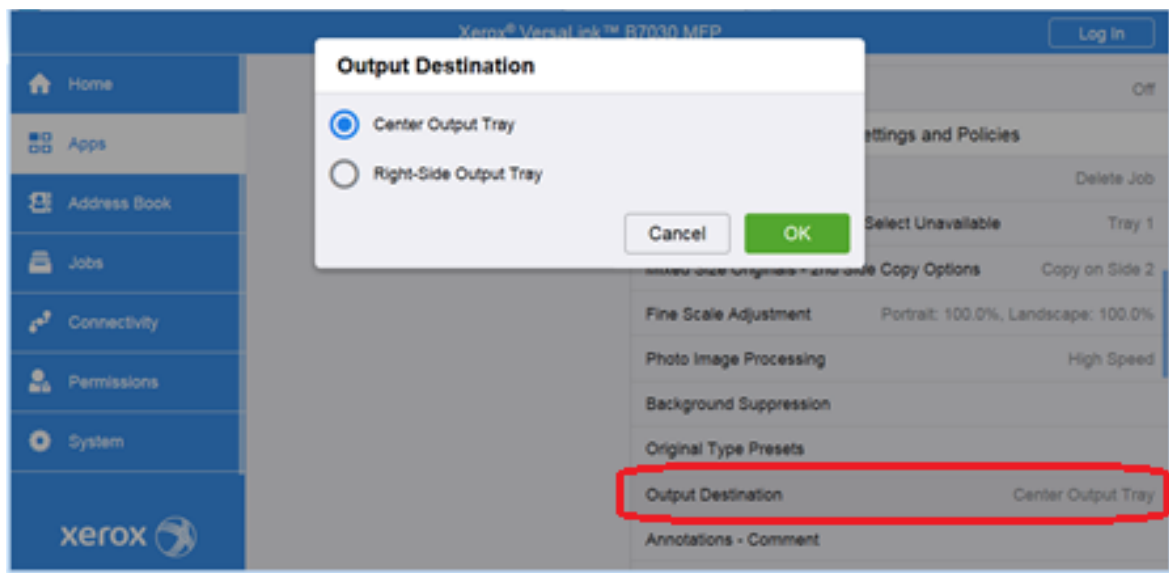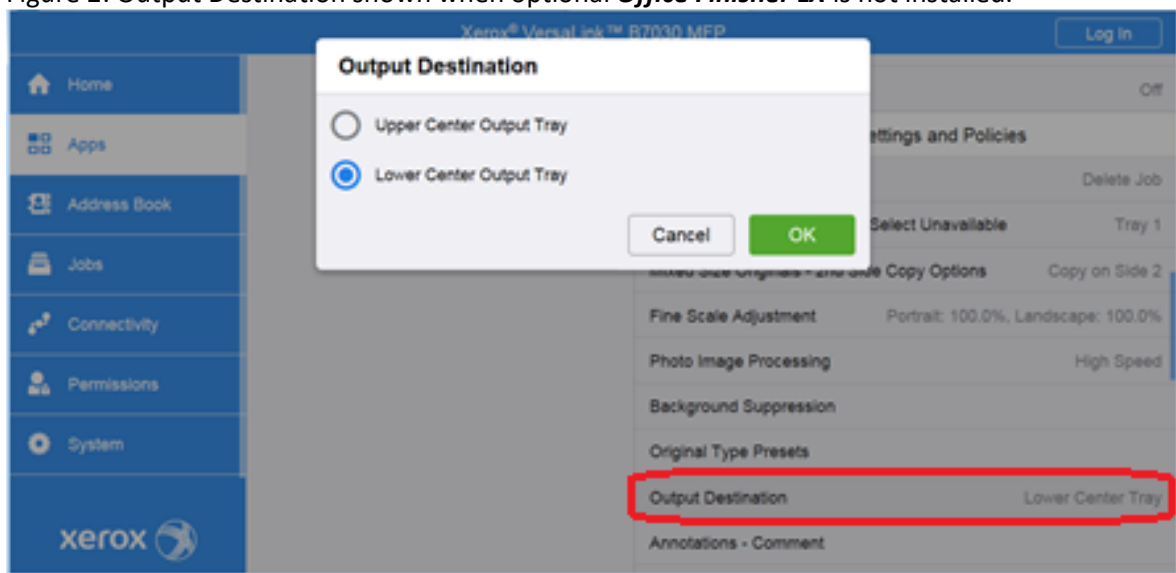Figure 2: Output Destination shown when optional *Office Finisher LX* is not installed.

Not applicable to Xerox® Phaser® 6510, Xerox® WorkCentre® 6515

6. One-Touch Feature Enhancement

This update expands the capabilities of One Touch features, allowing users to create, edit, and share one-touch "apps" that save and simplify complicated or lengthy workflows that customers may need to do frequently. Once created this app will appear and behave similarly to native device apps and functions. Creation of one-touch apps is simple, with a new option presented within app menus that allow for settings and control for a function to be saved. Once saved, the new one-touch app appears at the LUI like other native functions, and can be edited later if desired. One-touch apps can be shown for all users, user groups, or just the creator of the one touch app. This app can be cloned and shared, and supports personalization and customization.
Not applicable to Xerox® Phaser® 6510, Xerox® WorkCentre® 6515

7. Personal Favorites

This update adds enhancements to the personalization and customization functions that allow users to customize and save individual application settings and contacts to individual user accounts. This allows users to streamline and customize their user experience by saving frequently used options, hiding unused featured and functions, and providing an overall more efficient streamlined user experience. Frequently used contacts and destinations can be prioritized and saved, specific to the individual user. With the addition of one touches, and the already present UI customization and personalization options, this provides a best in class user experience for these devices.

Not applicable to Xerox® Phaser® 6510, Xerox® WorkCentre® 6515

8. SNMPv3 FIPS 140-2 mode support

FIPS 140-2 approved security protocols have been added to SNMPv3 enabling its use in in FIPS 140-2 mode without an exception. This enhancement provides an overall improvement to device security and management compatibility within secure environments.
Not applicable to Xerox® Phaser® 6510, Xerox® WorkCentre® 6515

9. Simultaneous HTTP and HTTPS Support

HTTPS connectivity is now available, using default, self signed certificates without a user having to enable and configure HTTPS, similar to operation of AtlaLink devices. This will allow HTTPS connections, as well as services and functions that depend on and require HTTPS functionality to work seamlessly without the extra step of enabling HTTPS and configuring certificates. Devices will still have the ability to enforce HTTPS ONLY connections by disabling insecure HTTP.