Xerox® VersaLink® B71xx & C71xx Product Enhancements Document for Version xx.24.71

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

Release Date: March 21, 2024 dc25rn1121

Firmware Release Details

Products SPAR Release xx.24.71 (Click on product name to access software)	System Version	Controller ROM Version	IOT ROM
Xerox® VersaLink® B7125/B7130/B7135	59.24.71	1.100.1	50.18.30
Xerox® VersaLink® C7120/C7125/C7130	69.24.71	1.100.1	60.18.30

Plugin Release Details

VersaLink Card Reader Plug-ins v17	Version
Xerox USB Card Reader	4.2.0
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
Active Tag Plugin	1.0.1
Xerox Cloud Direct Plug-in	1.3.0

Note:

Xerox Cloud Direct Plug-in and Xerox USB Card Reader Plug-in require system firmware version xx.23.41 or later to provide all functionality.

Contents

Latest release information:

Product Firmware Release xx.24.71 (PL1-R9)

1. Various Bug Fixes

- LDAP Passback Vulnerability has been fixed in this version.
- Passback Vulnerability found in user's Address Book Contact of SMB and FTP has been fixed in this version. With this fix, users will not be able to modify the SMB/FTP details (Destination server's IP Address) in the Address book of the VersaLink device using the Security Tools.
- From this version, after logging in select @pbx, the application will open without being prompted to login again irrespective of the parameter "Obtain User Information at time of Login".

Product Firmware Release xx.24.41 (PL1-R8)

1. Allow enablement and disablement of individual USB ports on EWS (introduced in PL1-R7)

These two caveats have been resolved in this SPAR Release:

1. Caveat: Warning – Release not recommended for Cloning
2. Caveat: Smart Card Auth

2. Various Bug Fixes

- With this version, device always exits the power saver mode and displays the "Workplace Kiosk" screen as default wakeup screen instead of home screen.
- New version of Xerox Cloud Direct Plug-in v1.3 addresses several login and configuration related issues with Xerox Workplace Cloud – Direct login.

Product Firmware Release xx.24.11 (PL1-R7)

1. Allow enablement and disablement of individual USB ports on EWS

Note: Below caveats may be resolved in future Software releases.

Caveat: Warning – Release not recommended for Cloning.
If you have Print-From or Scan-To disabled, this SPAR release is not recommended for cloning purposes unless you need the SPAR fix (or other SFR) provided by this release. If you must use this release because you require the SPAR fix and you have Print-From or Scan-To disabled, we recommend you not use cloning. If you need to use this release, for cloning, you will have to manually disable Print-From or Scan-To after the clone operation. That is because those two features will be inadvertently enabled by the cloning operation. See individual caveats below, there are some other issues with visiting the USB Setup page that you should be aware of.

Caveat: Print-From and Scan-To features inadvertently being enabled.
After entering the USB Feature Setup Page, if a reboot is called for because you made a change or mistakenly hit OK instead of Cancel, you must complete the reboot. At this point the system has forcibly enabled Print-From and Scan-To. You will need to go to Apps->USB and reapply your desired selections for those settings.
When configuring a device with USB feature enabled and either PrintFromUSB and/or ScanToUSB disabled as a cloning source, the clone target that the clone operation is done on will have neither feature

disabled. PrintFromUSB and ScanToUSB will have to be manually configured until this issue is addressed in a future release.
Caveats:

Caveat: Cross Model Cloning.
This SFR drove a distinction between a device with a (single) Rear USB-A configuration and a device with a (double) Rear Right USB-A and Rear Left USB-A configuration. The distinction is impactful when cloning, in that the cloning process does not make assumptions about the intentions of the admin. Therefore, cloning from a device with one configuration to a device with the other, will not result in the target's settings being overwritten. If desired, it is recommended that you take the clone from the same model.

Caveat: Smart Card Auth:
The USB feature (including all ports) can be disabled on the UI, even when Smart Card authentication is enabled.

Caveat: Downgrading.
Before downgrading from this release on a B71xx, or C71xx, the admin MUST enable the USB feature AND all USB Ports individually. Otherwise, any ports that were disabled prior to downgrade will remain disabled when the USB feature is then enabled.

2. Support RSASSA-PPS Signature Algorithms in device certificates

Caveat:
Before utilizing the new RSASSA-PSS Signature Algorithm in a certificate, you must manually enable TLS 1.3 on the EWS Page: System->Security->SSL/TLS.

If you have mistakenly enabled the cert before enabling TLS 1.3 perform the following:

- Log in as admin on the local UI
- Go to device->Connectivity and disable HTTPS
- Reboot device
- Enter EWS using HTTP
- Return to System->Security->SSL-TLS settings and enable both TLS 1.3 and HTTP - SSL/TLS Communication
- Reboot device

3. Various Bug Fixes

- LDAP Passback Vulnerability has been fixed in this version.
- Passback Vulnerability found in user's Address Book Contact of SMB and FTP has been fixed in this version.
- Xerox USB Card Reader version 4.2.0 fixes an issue where after upgrading printer Software to xx.81.41, iClass OmniKey 5427CK USB Card Readers no longer function (users unable to login with his or her iClass Prox Cards).
- With this firmware version, the border line crop issues for the customer SAP jobs have been fixed. This is applicable only if the option "When specified paper is unavailable" is configured as "Letter/A4 Substitution". The following Feature enablement keys needs to be installed in the device to print the customer SAP jobs without any issues.
  Feature Enablement/Disablement Keys:

Product	Enablement PIN	Disablement PIN
VL B7125/30/35 MFP	*5065203151	*5065203150
VL C7120/25/30 MFP	*5066203151	*5066203150

Product Firmware Release xx.24.11 (PL1-R6)

1. Enable SMB Version Settings on EWS

Caveat: When a cloning file exported from a device with this firmware (NW2.0 PL1-R6) or newer, is imported onto an older NW2.0/NW1.6 firmware or a NW1.5 device, the SMB settings cannot be overwritten with the newer cloning file because the FW level on the target device does not support the SFR. Therefore, we recommend keeping the fleet at the same FW level and taking precaution if there was a need to downgrade. After a downgrade the SMB Port Settings should be evaluated.

2. Enable the inclusion of the OrgID field on product certificates

Enables the import and assignment of PKI certificates that include the Organization Identifier (OrgID, OID 2.5.4.97) field for Device cert, Intermediate cert, and Root CA cert in compliance with European eIDAS regulation.

3. Various bug fixes

- New version of Xerox Cloud Direct Plug-in version 1.2.0 fixes certain timing issues where a failure occurs when attempting to configure VersaLink devices via Xerox Cloud Direct.
- With this version, Email application will be displayed in VersaLink device LUI after configuring the device with XWC direct cloud authentication.
- Fault code "116-324" has been fixed in this version. While submitting the user file with Avenir font installed in PC via Latest GPD PCL driver, print job will be printed successfully without this fault code occurrence.
- Intermittent failure of Badge and keyboard auth has been fixed in this version and the user can authenticate with badge or username/password without any error.
- Fault code 116-331 (Invalid Log Info RAP) is fixed. From this version, user will not experience the random display of the Fault code 116-331 in the device LUI.

Product Firmware Release xx.23.91 (PL1-R5)

1. Various bug fixes

- With this version, Scan to Azure repository over sftp/sslv2 will be successful without the error code 017-526 (Server connection in SFTP Fail).
- After installing a Certificate or Certificate Chain on the printer where the Certificate contains the "Inhibit Any-policy (OID=2.5.29.54)" with the "Critical" attribute set, the printer immediately shows the certificate to be invalid with a "Path Validation Failed" error. This issue has been fixed in this version along with adding a Feature Enablement Key on the printer. Enabling the Feature Enablement Key allows the printer to accept a Certificate that has the “Inhibit Any-policy (OID=2.5.29.54)" with the "Critical" attribute set/configured in the Certificate.

  Feature Enablement/Disablement Keys:

Product	Enablement PIN	Disablement PIN
VL B7125/30/35 MFP	*5065507951	*5065507950
VL C7120/25/30 MFP	*5066507951	*5066507950

- After importing the certificate successfully, the installed certificate will work properly without any errors.
- From this version, VersaLink devices will stay connected to the Network at DHCP expiry and the device will print the jobs properly without rebooting it.

Product Firmware Release xx.23.41 (PL1-R4)

1. Xerox Cloud Direct Support

The Xerox Cloud Direct Plug-in and an updated Xerox USB Card Reader Plug-in enable devices to directly connect to the Xerox Workplace Cloud server without going through an agent server.

2. Various bug fixes

- With this version, Network Scan/Scan to Home will be successful when scanning to a resource in an Active Directory Trusted domain.
- While resetting Maintenance Kit via LUI, Chain-link values (950-800, 950-804, and 950-824) of the Maintenance Kit can be successfully reset to “0” via Reset Option.
- With this version, the word “Accounting” will be spelled correctly in the software configuration chart which is downloaded from the device.
- Fault code 117-372 has been fixed in this version.

Product Firmware Release xx.23.11 (PL1-R3)

1. Various bug fixes

- Fault Code 132-311 has been fixed in this version.
- With this version, in device app, lengthy Logged-in username (ex: ThisIsALongUserLoginNameItIs) is getting truncated correctly instead of displaying the complete username.
- Fax Enablement/Disablement settings are applied properly when installing a Clone file.
- Plugins that were deactivated prior to upgrade no longer have status of Restart to Activate after upgrade, status is Deactivated.
- Plugin status gets cloned when XWC remote management is enabled/disabled on the device.

Product Firmware Release xx.22.82 (PL1-R2)

1. Plug-ins and Added Cloning features

Firmware releases will now contain the 5 card and card reader plug-ins listed below and will be automatically installed. If the plugins versions on the device is older than the version contained with the firmware release, the newer version plugins will be installed and will retain the older plug-in activation status after firmware install and restart.

1) CCID_Terminal_Plug-in_
2) Modernized_CAC_Smartcard_Service_DPV_Plug-in
3) Xerox_USB_Card Reader
4) GemNetSmartCardService
5) Active Tag

On the Create Clone File webpage, the following additional settings are now selectable:

- Plug-ins activated/not activated “Status” are now included in the Clone file when Defaults and Policies is selected in Cloning.
- Remote Services Upload
- Connections (Ethernet, WiFi, USB, WiFi direct, NFC) are now independently selectable.
- FIPS 140-2 settings are cloneable when the SFR key is installed (see table below)

NW 2.0 Models	Activate	Deactivate
C7120/C7125/C7130 MFP	*5066506581	*5066506580
B7125/B7130/B7135 MFP	*5065506581	*5065506580

Notes:
If after firmware with plugins is installed and any of these 5 plug-ins has been deleted, the deleted plug-ins will not be reinstalled until a later firmware version that contains newer plug-in versions is available.
If a plug-in has been deleted but needs to be activated, manually download the latest plug-ins from Xerox.com and upload the desired plug-in to the device and activate.

SP-49642: When a plug-in that was either “Deactivated” or not installed on the device prior to firmware update with plug-ins upload, these “Deactivated” plug-ins incorrectly display status of “Restart to Activate”. Upon the next device restart, their status is correctly displayed as “Deactivated”.

Caveats:

SP-49634: plug-in status doesn't get cloned when XWC Remote Management is enabled on the device.

Workaround: If XWC Remote Management is required, the Plug-in's Activated/Deactivated status must be manually set.

If the Plugin feature is disabled on the target device, and a clone file with the Plugin feature enabled and plugin statuses set is submitted to the target device, the clone file must be submitted twice. The first time enables the plugin feature, and the second time applies the Plugins activated/deactivated statuses.

2. 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.

3. Various bug fixes

- With this version, Xerox Standard accounts will not disappear after rebooting the device.
- 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.
- 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.

Product Firmware Release xx.21.91 (PL1-R1)

1. 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.

2. LDAP Proximity Card Registration & Login

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

3. 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

4. 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.

5. 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.
- 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.21.21 (PL1)

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. 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”.

3. SIPRNet Plug-ins Upgrade/downgrade

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.

4. 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.

5. 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

6. 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).

7. 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.

8. Support Printing of Encrypted File(s) via EIP Pull Print Model

Add the ability for an external EIP solution to detect that the device supports encrypted print files for the EIP Pull Print API.”

9. Bluetooth (AirPrint Discovery)

Added support for BLE (Bluetooth Low Energy) for iBeacon communication with iOS devices as defined in Apple's iBeaconForPrintersSpecification-1.0 spec. Support includes BLE On/Off setting whose default is ON and iBeacon On/Off setting whose default is On within the Web UI. The settings are configurable and cloneable by the system administrator. The iBeacon setting is independent of the BLE setting. Both iBeacon and BLE must be enabled for iBeacon to function.

Product Firmware Release xx.14.31 (IL-R1)

1. Various bug fixes

- With this version, VersaLink device will print the barcode along with human readable text correctly using installed fonts "LibreBarcode39Text-Regular.ttf and LibreBarcode128Text-Regular.ttf".
- When language is set to French, AZERTY layout keyboard will be shown in Email - To, Cc, BCC Fields.
- 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.
- PDF files with Xerox Sans font will be printed correctly
- Out of memory error when trying to do OKTA authentication with @PrintByXerox app on Versalink devices has been resolved.
- Fault code (18-505) no longer occurs while scanning to the Isilon server.
- Email address for the “From” field can be configured for the users without any issues in case of enabling the Xerox Standard Accounting
- Massive jobs from invoicing system will be printed in the device without any problem.

- 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.14.01 (Launch)

1. 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 C7120/25/30	*5066482911	*5066482910
VersaLink B7125/30/35	*5065482911	*5065482910

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

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:

Product	Enablement Key	Disablement Key
VersaLink C7120/25/30	*3066420751	*3066420750
VersaLink B7125/30/35	*3065420751	*3065420750

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. 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.

4. SMBv3 support for encryption and signing (only)

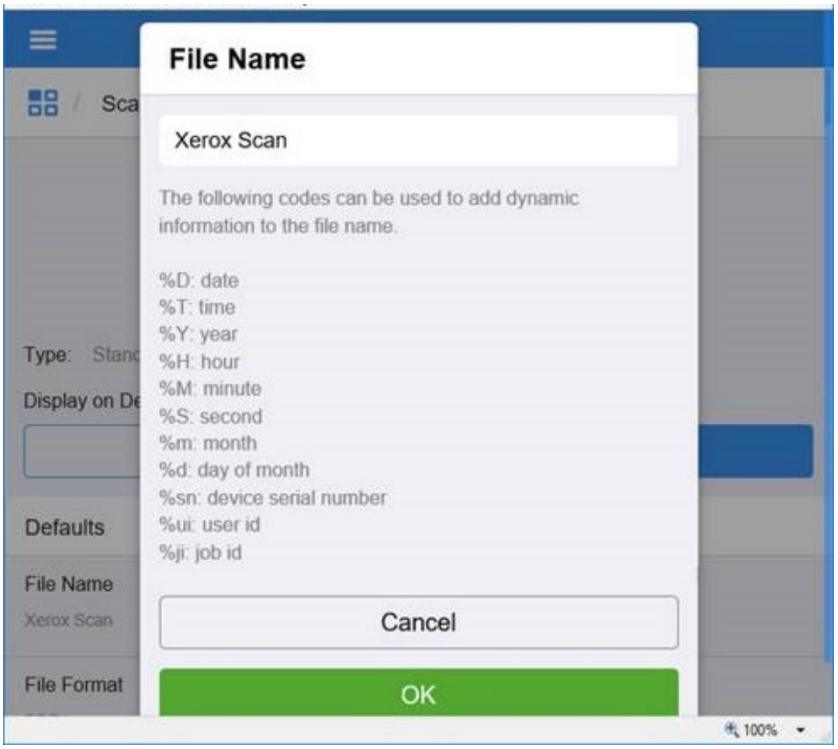
This release adds support for SMBv3 with the 3.0.0 dialect. Also supports scan to encrypted SMBv3 shares.

5. 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



6. Enable Full UPN when authenticating using a Smartcard

This feature enables the Full UPN as defined in a User's LDAP directory entry 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:

Product	Enablement Key	Disablement Key
VersaLink C7120/25/30	*5066484521	*5066484520
VersaLink B7125/30/35	*5065484521	*5065484520

7. 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 C7120/25/30	*3066476371	*3066476370
VersaLink B7125/30/35	*3065476371	*3065476370

8. 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
VersaLink C7120/25/30	*5066477581	*5066477580
VersaLink B7125/30/35	*5065477581	*5065477580

9. 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 C7120/25/30	*3066475651	*3066475650
VersaLink B7125/30/35	*3065475651	*3065475650

10. 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	Enablement Key	Disablement Key
VersaLink C7120/25/30	*3066461861	*3066461860
VersaLink B7125/30/35	*3065461861	*3065461860

11. SNMP / MIB Language

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.

12. Thin Print

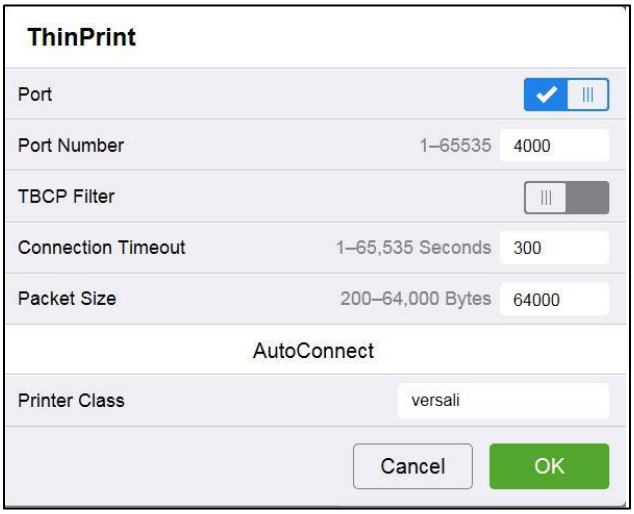
ThinPrint is a Third-Party solution that saves network bandwidth by allowing print data to be compressed at the server and decompressed at the Print device before being printed out on a printer. The ThinPrint solution also supports print data encryption prior to sending to the print device. Xerox has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

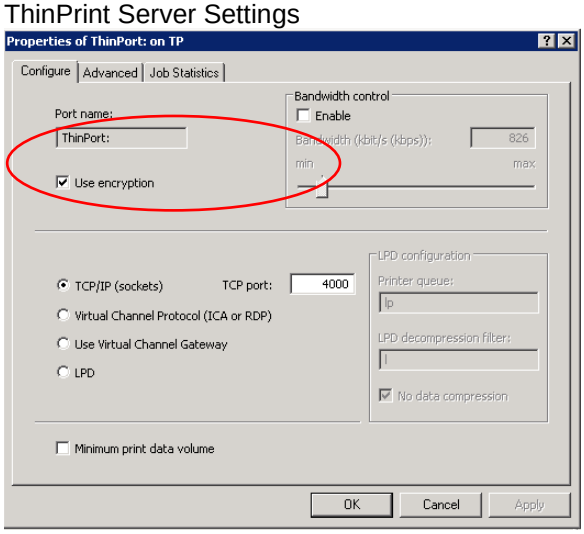
Note: Although a different port number can be configured. It is important not enter a port number that is already in use.



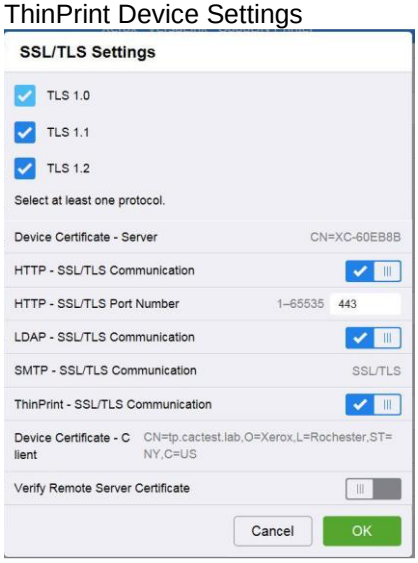
ThinPrint requires a certificate to be loaded on the device when running with TLS encryption.
This is in System Security SSL/TLS Settings.

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.

13. 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.

14. 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

15. 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

Above ciphers are enabled by default.

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.

16. 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
VersaLink C7120/25/30	*5066477471	*5066477470
VersaLink B7125/30/35	*5065477471	*5065477470

17. 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.

18. 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.

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

A user logged with a convenience authentication system can 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.

20. 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.

21. 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.

22. 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.

23. Various bug fixes

- Fixed an intermittent fuser error while printing large volumes of paper whose width is less than 148mm.
- With this version, Scanning the printer with NMAP will show TCP port 3000 as closed
- In this release, device pulls correct hostname from DHCP server
- Some Hungarian characters are no longer missing.
- Reduction of 024-747 faults when printing Comm10 Envelopes.
- Remote command injection is not possible to perform using the clone file
- 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
- Ability to receive the email notifications, has been improved
- 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.

© 2022 Xerox Corporation. All rights reserved. Xerox® and Xerox and Design® and VersaLink® are trademarks of Xerox Corporation in the United States and/or other countries. BR22773
Other company trademarks are also acknowledged.
Document Version: 1.0