Xerox® VersaLink® B71xx & C71xx Product Enhancements Document for Version xx.14.31

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

Release Date: June 17, 2022 **dc22rn4104**

Firmware Release Details

Products SPAR Release xx.14.31 (Click on product name to access software)	System Version	Controller ROM Version	IOT ROM
Xerox® VersaLink® B7125/B7130/B7135	59.14.31	1.2.1	50.17.00
Xerox® VersaLink® C7120/C7125/C7130	69.14.31	1.2.1	60.18.00

Plugin Release Details

VersaLink Card Reader Plug-ins v12	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	1.2.0
TWN4 Card Reader Service	1.0.0

Contents

Latest release information:

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)

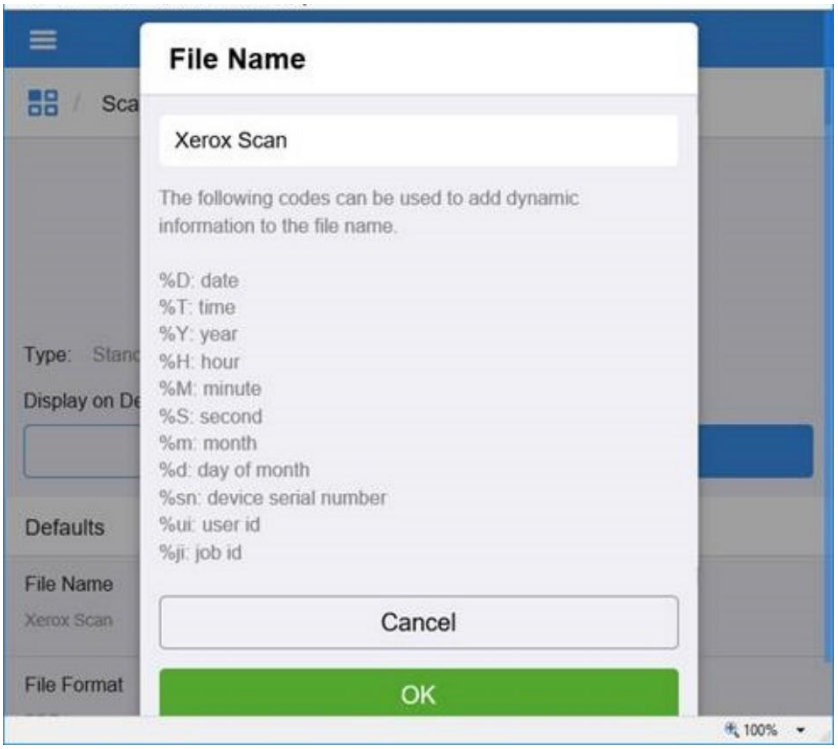
This release adds support for SMBv3 with the 3.0.0 dialect. Also supports scan to encrypted SMBv3 shares.

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

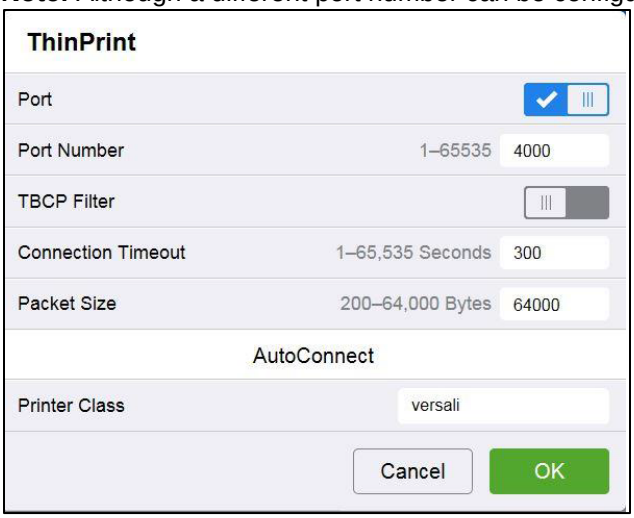
ThinPrint is a Third-Party solution that saves network bandwidth by allowing print data to be compressed at the server and decompressed at the Print device before being printed out on a printer. The ThinPrint solution also supports print data encryption prior to sending to the print device. Xerox has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

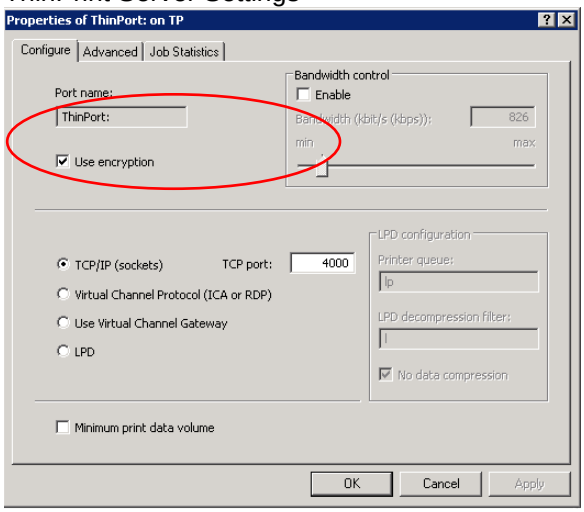
Note: Although a different port number can be configured. It is important not enter a port number that is already in use.



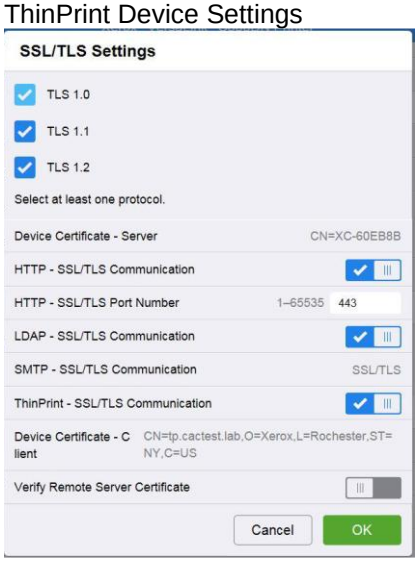
ThinPrint requires a certificate to be loaded on the device when running with TLS encryption.
This is in System Security SSL/TLS Settings.

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.

Document Version: 1.0