Xerox® VersaLink®
Enhancement Read Me

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

Release Date: January 9, 2019

Contents

Products	System Software	Controller ROM
Xerox®VersaLink®B400	37.35.01	1.47.0
Xerox®VersaLink®B405	38.35.01	1.47.0
Xerox®VersaLink®C400	67.35.01	1.47.0
Xerox®VersaLink®C405	68.35.01	1.47.0
Xerox®VersaLink®B600-B610	32.35.01	1.47.0
Xerox®VersaLink®B605-B615	33.35.01	1.47.0
Xerox®VersaLink®C500-C600	61.35.01	1.47.0
Xerox®VersaLink®C505-C605	62.35.01	1.47.0
Phaser6510 Windows Installer Mac Installer	64.35.01	1.47.0
WorkCentre6515 Windows Installer Mac Installer	65.35.01	1.47.0
Xerox®VersaLink®C7000	56.35.01	1.47.0
Xerox®VersaLink®C7020/25/30	57.35.01	1.47.0
Xerox®VersaLink®C8000-C9000	70.35.11	1.47.0

Product Firmware Release xx.35.01

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 an 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

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.34.01

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.33.01

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:
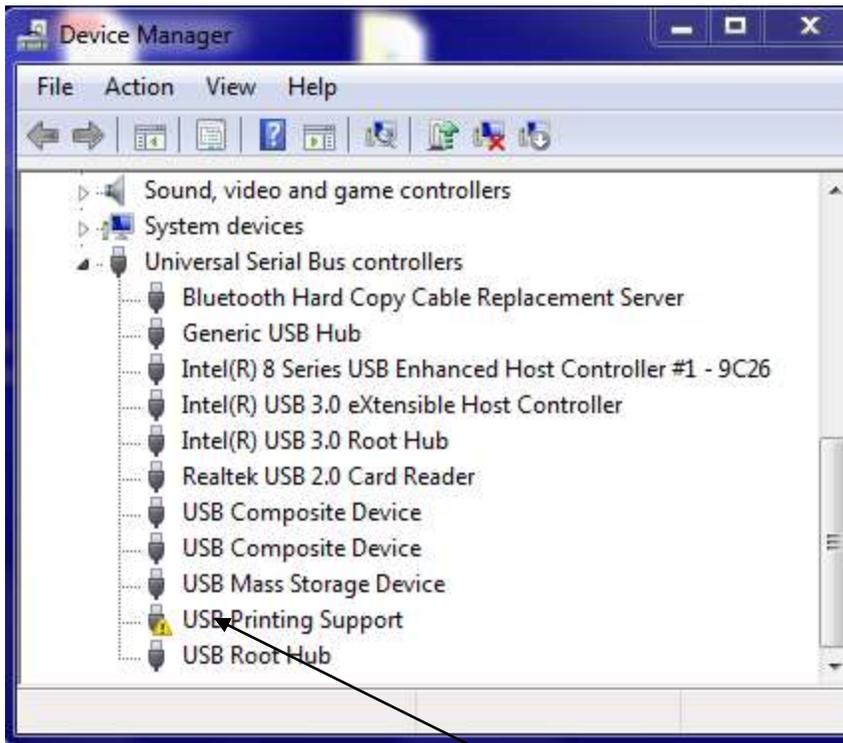
Note: Customers who have a **Yellow Warning!** next to the USB Printing Support will need to Right Click on the USB Printing Support line and select Update Driver Software.

Product Firmware Release xx.31.81

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

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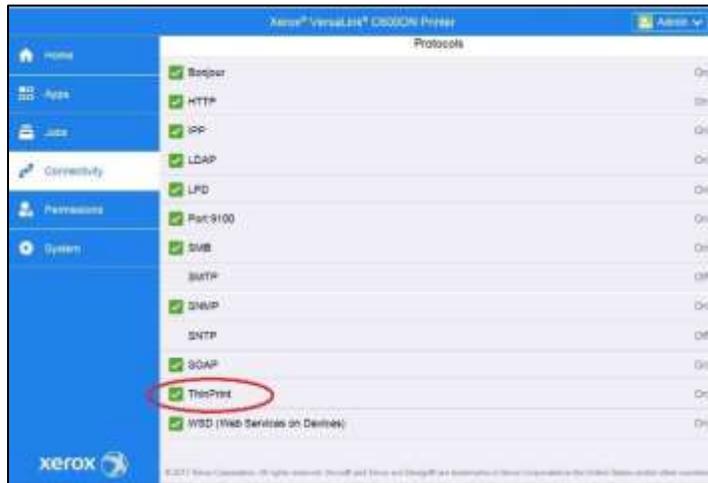
Once the ThinPrint Protocol is enabled, the Admin has access to the settings below. The port must be enabled. The default port number for ThinPrint communication is 4000.

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
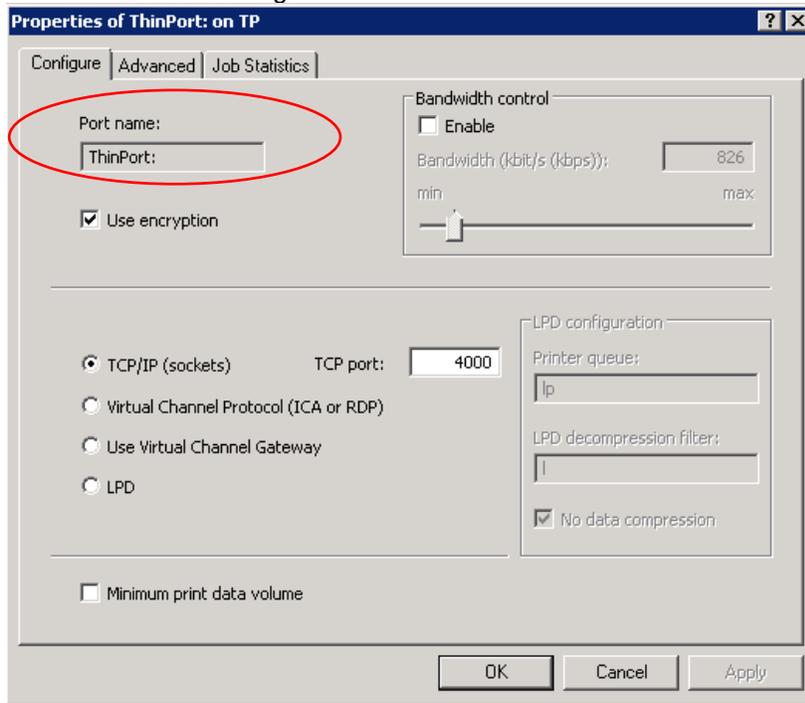
ThinPrint Device Settings

SSL/TLS Settings

- [✓] TLS 1.0
- [✓] TLS 1.1
- [✓] TLS 1.2

Select at least one protocol.

Device Certificate - Server	CN=XC-60EB8B
HTTP - SSL/TLS Communication	[✓ III]
HTTP - SSL/TLS Port Number	1–65535 443
LDAP - SSL/TLS Communication	[✓ III]
SMTP - SSL/TLS Communication	SSL/TLS
ThinPrint - SSL/TLS Communication	[✓ III]
Device Certificate - Client	CN=tp.cactest.lab,O=Xerox,L=Rochester,ST=NY,C=US
Verify Remote Server Certificate	[III]

Cancel   OK

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	*3014333081	*3014333080
Xerox® VersaLink® C7020/25/30/35	*3014333081	*3014333080
Xerox® WorkCentre® 6515	*3005333081	*3005333080

3. 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.

4. 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.
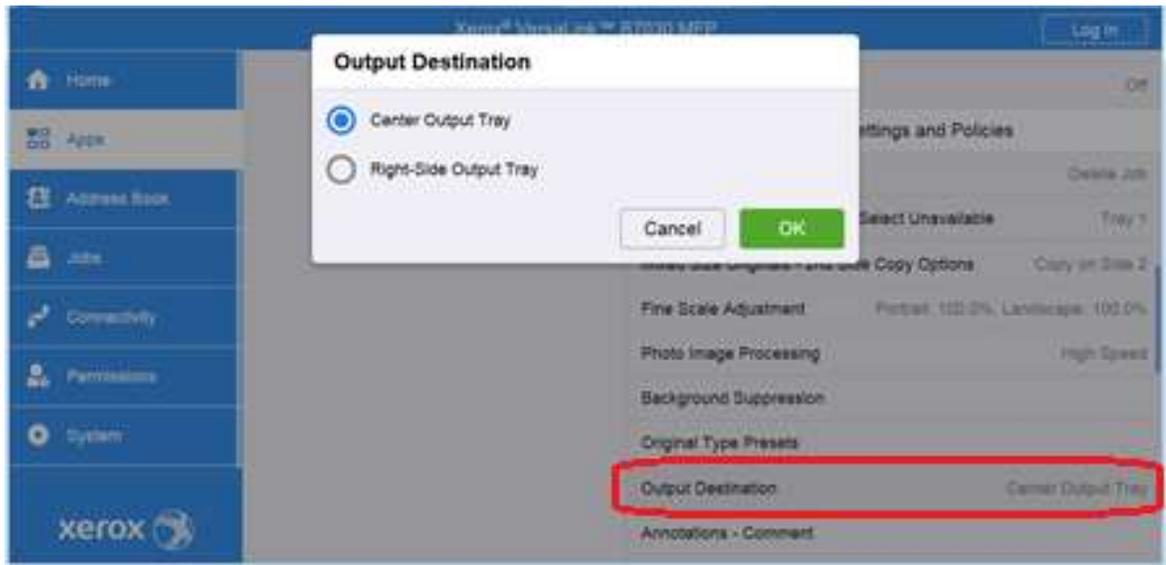
Figure 2: Output Destination shown when optional *Office Finisher LX* is not installed.
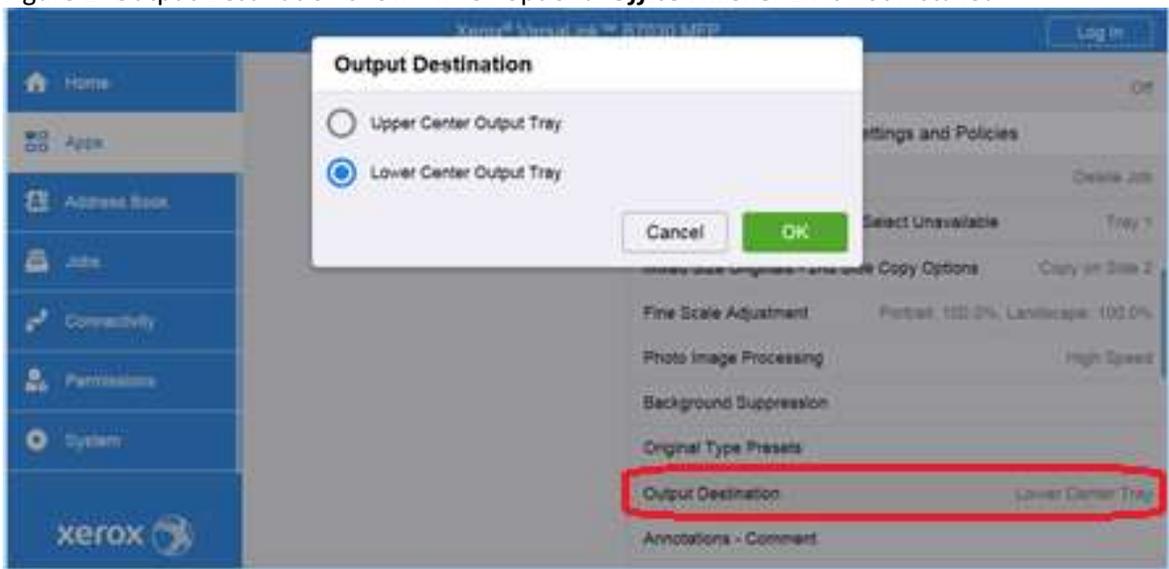
Not applicable to Xerox® Phaser® 6510, Xerox® WorkCentre® 6515

5. 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

6. 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

7. 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

8. 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.

xerox