Xerox AltaLink Multifunction Printer Product Enhancement Document for Version 122.xxx.025.20910

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

Release Date: Sept 1, 2025 dc25rn1147

Product Model	System Software	Network Controller
AltaLink C8170	122.011.025.20910	122.011.20910
AltaLink C8145/55	122.010.025.20910	122.010.20910
AltaLink C8130/35	122.009.025.20910	122.009.20910
AltaLink B8170	122.013.025.20910	122.013.20910
AltaLink B8145/55	122.014.055.20910	122.014.20910
AltaLink C8270	122.040.025.20910	122.040.20910
AltaLink C8245/55	122.039.025.20910	122.039.20910
AltaLink C8230/35	122.038.025.20910	122.038.20910
AltaLink B8270	122.042.025.20910	122.042.20910
AltaLink B8245/55	122.041.025.20910	122.041.20910

Contents

Firmware 122.xxx.025.20910 (General Release D8.5.1) Sept 2025 3

1. Various Bug Fixes 3

Firmware 122.xxx.005.15400 (General Release D8.5) July 2025 3

1. New Features 3
2. Smartcard Kerberos Authentication supports USB PIV Security tokens such as Yubikey PIV. 4
3. Authentication to Cloud Identify Provider (IdP) supports using Smartcard 5
4. Authentication to Cloud Identify Provider (IdP) supports using USB Security Token 5
5. Discoverable Passkey now supported for Authentication to Cloud Identify Provider (IdP) 5
6. User login steps for Authentication to Cloud Identity Provider (IdP): 5

Firmware 121.xxx.055.12000 (SPAR Release D8.0) R25-04 - May 2025 6

1. Security 6
2. Enable Discoverable Passkey 6

Firmware 121.xxx.004.22726 (General Release) March 2025 6

2. Various Bug Fixes 6
3. Trellix for VersaLink 6
4. Security Made Simple 6
5. Workflow Automation 7
6. Supporting Accessibility with Assistive Technology 7

Firmware 121.xxx.045.03600 (D8.0 SPAR Release) R25-02 - Feb 2025 7

1. Security 7
2. Smartcard Kerberos Authentication now supports USB PIV Security tokens such as Yubikey PIV. 7
3. Authentication to Cloud Identify Provider (IdP) now supports using Smartcard 8
4. Authentication to Cloud Identify Provider (IdP) now supports using USB Security Token 8

Firmware 120.xxx.003.20003 (General Release) July 2024 8

1. Various Bug Fixes 8

Firmware 120.xxx.003.20002 (General Release) April 2024 8

1. Various Bug Fixes 8

Firmware 120.028.003.20001 (General Release) Oct. 2023 8

1. Supports New Components (C415 Model Only) 8

Firmware 120.028.003.20000 (General Release) Sept. 2023 8

1. Supports New Components 8

Firmware 119.028.003.04616 (General Release) June 2023 9

1. Supports New Components 9

Latest release information:

Firmware 122.xxx.025.20910 (General Release D8.5.1) Sept 2025

1. Various Bug Fixes

With this update, the printer can send email using the Device Code Flow (DCF) method of OAuth 2.0. Using the SMTP setup page on the printer's Embedded Web Server, customers can sign-in to the "Xerox® Device Code Flow Email" application using their Microsoft® 365 Exchange Online or Outlook only accounts
and register the printer for sending emails.

The printer will send email as the account that signs-in to the "Xerox® Device Code Flow Email" application.

This note communicates:
1. New feature: Email using OAuth 2.0.
2. Use E-mail setup page on the Embedder Web Server.
3. Sign-in to the Xerox created app.
4. Works only with MS365 and Outlook-only accounts.
5. Email will be sent as the one account that is signed in to the application.

Additional Information:
https://www.xerox.com/en-us/office/insights/exchange-online-authentication

Firmware 122.xxx.005.15400 (General Release D8.5) July 2025

1. New Features

Intuitive User Experience

- Quick Access Button
  - The Atlantis platform supports a Quick Access button that provides a way to jump to specific information screens without having to navigate through the Device App or other locations. The initial implementation provides quick access to:
    - Supplies
    - Paper Trays
    - Notifications
    - Accessibility
    - About
- Adaptive Learning - Notifications
  - The Adaptive Learning history log has been enhanced to include more detail regarding Adaptive Learning changes.
  -
- Accessibility Improvements
  - Speech output for the remote user interface and EIP
  - Private listening support utilizing headphones

- Print Support Application (PSA) by Xerox
  - We have created the Xerox® Print and Scan Experience App that acts as the Print Support App (PSA) for clients with Microsoft IPP Class driver queues connected to their Xerox® Devices, or Universal Print (UP) Class driver queues connected to cloud printers.
  - This app customizes IPP or UP printers, provides access to all our features, and gives our printers an enhanced and coherent user experience across all devices–making print job setup fast, simple, and efficient.
- Supports splitting large scan jobs into multiple files based on image count.

- Redesigned VersaLink® B&C415 soft keyboard to properly display on a 5" screen.
  - Soft keyboards were resized to use more of the Touchscreen area
  - Update ".com" custom key to function like accented characters

Comprehensive Security

- This firmware release is certified compliant with the EU Radio Equipment Directive (RED) which is required for wireless enabled devices in Europe from August 1st 2025.

- Meets the latest Common Criteria Certification (CCC) collaborative Protection Profile (cPP) for Hardcopy Devices v1.0e
    - The newest firmware has been submitted for certification under the updated CCC requirements. Certification is expected by January 2026.
- Customers may disable the USB Type-B port on the back of the printer. (AltaLink specific feature)
- System administrators can disable FTP client capabilities.
- IdP Authentication via PIV Card, MS Authenticator & Yubikey
    - YubiKey provides multi-factor protection against phishing and account takeovers, with easy, password-less login.
- Mobile phone authentication using Xerox Easy Assist App
    - Tap your phone on the NFC chip to securely authenticate your identity.
- Cloud SIEM Support – Natively supports Cloud SIEM Tools like Microsoft® Sentinel*
- This release delivers extensive security enhancements across IPsec, logging, EIP Web Services, access control, authorization, accounting, FIPS, TLS, cipher hardening, and certificate management. It also mitigates multiple CVEs, including path traversal, privilege escalation, remote code execution, and cross-site scripting.

PDF Printing Enhancements

- Supports the use of the
- Adobe Embedded Print Engine (AEPE) for PDF printing
    - PDF files are no longer converted to PostScript before printing
    - AEPE directly rasterizes PDF files, enhancing processing efficiency
    - This change results in improved performance and, in some cases, better image quality

Sustainability

- Toner Cartridge Recycling Initiative
    - Xerox devices now display a QR code with recycling info after toner replacement.
    - Upon replacing a depleted toner cartridge, the printer displays a QR code and a message detailing the correct recycling procedure for empty cartridges.

Versalink Archival Mode

- The VersaLink® B&C 625/620/415 products now support both Swedish Archive and German PTS archival modes. These modes are selectable but are off by default as they increase toner usage.

Support for an additional 550-Sheet Tray on Versalink C415

- Up to 2 optional 550-Sheet Trays are now supported in addition to the 550+100 Sheet Tray (consistent with the C410.)
- 550-Sheet Tray can now be installed as the first optional tray, with support for up to a total of (3) 550-Sheet Trays.

2. Smartcard Kerberos Authentication supports USB PIV Security tokens such as Yubikey PIV.

Users can now login using either a smartcard or a USB PIV Security token, such as Yubikey PIV, when the device is configured for on-premise Smartcard (Kerberos) Authentication and does not require any unique configuration settings.
Selecting the “Smartcard” option in the Login Methods / Control Panel Login pulldown list also enables use of PIV USB security tokens.
Note: User interface messaging is updated to reflect “Authentication Tokens” to be consistent with the industry. “Authentication tokens” include Smartcards and USB security tokens which are also commonly referred to as a security token, security key or passkey.
Note: Use of USB Security tokens which plug into the front USB port (such as Yubikey) REQUIRE the installation of the USB Token Hub kit. Contact Xerox Sales for obtaining these kits.

3. Authentication to Cloud Identify Provider (IdP) supports using Smartcard

Authentication to Cloud Identify Provider (IdP) now supports using Smartcard via certificate-based authentication (CBA).
Users can now login to an IdP using their smartcard by selecting certificate-based authentication (CBA) when prompted on the IdP login screen.
This can be configured by setting "Control Panel Login" to "Identity Provider (IdP) – Validate on Cloud". Corresponding enablement is required on the Customer IdP to enable CBA.

4. Authentication to Cloud Identify Provider (IdP) supports using USB Security Token

Authentication to Cloud Identify Provider (IdP) supports using USB Security Token via FIDO2 interface.
Users can login to an IdP using their FIDO2 USB security token, such as Yubikey, by selecting FIDO2 when prompted on the IdP login screen.
This can be configured by setting "Control Panel Login" to "Identity Provider (IdP) – Validate on Cloud". Corresponding enablement is also required on the Customer IdP to enable FIDO2.
Note: User interface messaging is updated to reflect "Authentication Tokens" to be consistent with the industry. "Authentication tokens" include Smartcards and USB security tokens which are also commonly referred to as security token, security key or passkey.
Note: Use of FIDO2 USB Security tokens which plug into the front USB port (such as Yubikey) REQUIRE the installation of the USB Token Hub kit on all devices. Contact Xerox Sales for obtaining these kits.

5. Discoverable Passkey now supported for Authentication to Cloud Identify Provider (IdP)

Enable Discoverable Passkey when using USB security token for FIDO2 Authentication to Cloud Identify Provider (IdP).
Users can login to an IdP using their FIDO2 USB security token, such as Yubikey, without having to enter their username by selecting Discoverable Passkey / PIN sign-in option on the IdP login screen. Then select "Face, fingerprint, PIV or Security key" option and when prompted, enter Security Key PIN" and select "submit".

Note: Use of FIDO2 USB Security tokens which plug into the front USB port (such as Yubikey) REQUIRE the installation of the USB Token Hub kit on all devices. Contact Xerox Sales for obtaining these kits.

6. User login steps for Authentication to Cloud Identity Provider (IdP):

- Smartcard CBA login: insert smartcard in smartcard reader, enter "user Passcode" when prompted at the user interface. Select "Submit". Device communicates with the IdP and user will be logged-in when successful.

- FIDO2 USB Security Token login: (USB Token Hub is installed): Insert FIDO2 USB Security Token into the USB Token Hub. The IdP "Sign in" screen is displayed. The user may login using either:
    - Username / PIN login: user enters their username and selects "Next".
    - Discoverable Passkey / PIN login: user selects "sign-in options". The Microsoft Sign-in options screen is displayed, user selects "Face, fingerprint, PIB or Security key" option.
    -

  The "Log in" screen is displayed prompting user to "enter Security Key PIN". User enters their Security Key PIN and selects "submit". The Login screen prompts the user to "Touch your Security Key to continue" (user presence challenge). User touches the USB Security Key. Device communicates with the IdP and user is logged-in when successful. The Microsoft "Stay signed-in?" screen is displayed, the user may select "don't show this again" and answer "Yes" or "No".

- Microsoft Authenticator App login: select "Alt Login" (keyboard) icon in the top header of the Custom Blocking Screen. The IdP "Sign in" screen is displayed prompting for username, enter "username", select "Next." Enter "username" and press "skip" when presented with "insert your Smart Card or other authentication token" Screen. Choose "other ways to sign in" and select "Approve a request on my Microsoft Authenticator app." The IdP will present the "Approve Sign in" screen displaying the number to enter into the Authenticator app, user enters the number on the Authenticator App on their phone. User will be logged-in when successful.

- Username & Password login: select "Keyboard/Alt Login" icon in the top header of the Blocking Screen, enter "username" and press "skip" if presented with "insert your Smart Card or other authentication token." Screen. Choose "other ways to sign in" and "Use my password." Enter "password" when prompted on IDP login page, select "Enter". User will be logged-in when successful.

Note: USB Security Tokens can support multiple interfaces (OTP, FIDO, CCID, etc…) and are typically shipped with all interfaces active. Since the login process is different for each interface, it is recommended to disable all interfaces that are not being used in order to avoid user login confusion.

When multiple interfaces are active on a USB Security Token, the PIV interface is given first priority. If the users' USB Security Token PIV is active but not completely configured, when the user attempts to login, it will fail. In this case, when the user is prompted to "enter passcode" for PIV login, user should select "skip" to get to the FIDO2 login prompt to "Enter Security Key PIN" to login.

Firmware 121.xxx.055.12000 (SPAR Release D8.0) R25-04 - May 2025

1. Security

This is a SPAR release that includes multiple security enhancements for the AltaLink products and includes fixes for XSS (Cross Sight Scripting), Denial of service (DoS), Remote Code Execution, LDAP Pass Back, SQL Injection, and Broken Access Control.

2. Enable Discoverable Passkey

Enable Discoverable Passkey when using USB security token for FIDO2 Authentication to Cloud Identify Provider (IdP).
Note: Use of USB Security tokens which plug into the front USB port (such as Yubikey) REQUIRE the installation of the USB Token Hub kit and is software enforced. See the Additional Details section for ordering information.

Firmware 121.xxx.004.22726 (General Release) March 2025

2. Various Bug Fixes

- Performance and supplies reporting improvements have been made in this release.
- A crash that could occur when using LAN Fax, faxing from the PCL print driver, has been fixed in the printer version.
- Improves PCL IQ problems introduced in the previous release.
- This software fixes an intermittent issue where login using Convenience Authentication, Xerox Secure Access, or Xerox Workplace Cloud results in failure to log in with one of the following messages:
    - "The Remote Server has not responded."
    - "Authentication Error. Access Denied."
    - "Login to register card."
    - "Associate Card."

- For customers using this device for embedded fax, see link to super patch readme. Install this post-upgrade patch to improve fax reliability.

3. Trellix for VersaLink

- Trellix is now supported on the entire Atlantis based VersaLink® product line.

4. Security Made Simple

- **Server-less card authentication** where customers can utilize cards and card readers without the need for a solution and a server.

- **EIP Authentication** allows EIP developers to create a ConnectKey app that can be configured as the blocking screen for the device. Once configured, the ConnectKey app fully assumes the responsibility of authenticating and authorizing users, or it can leverage device authentication / authorization configuration.

- **Security Templates** are available to simplify the security configuration process. A template can be selected during the installation process or modified later through the Embedded Web Server (ESW). The templates available are Default, Elevated and High.

- **Secure Print with Microsoft Universal Print** Universal Print now supports the option to send jobs with a Secure Print PIN that is encrypted with the job. These jobs align with the Device Policies and Defaults settings that the device administrator can set in the "Secure Print" section of the Embedded Web Server (EWS).

- **Secure Release with Microsoft Universal Print** where the walk-up user authenticates with the device and their secure print jobs are available to print without entering a pin.

5. Workflow Automation

- **Metadata for Scan To** enables the 'Scan To' app the ability to apply metadata as part of the scan job.

- **Scan To Print** within the 'Scan To' app, now allows you to select "Print Scanned Document" as a destination for a multi-destination scan.

6. Supporting Accessibility with Assistive Technology

- **Updated Touchscreen Interface** supports zoom and pan to allow the user to zoom via pinch/zoom gestures.

- **Touchscreen keyboard navigation** which allows users to navigate and operate the touchscreen via an attached USB keyboard.

- **Speech output** that works in conjunction with the keyboard to enable the user to navigate through the touchscreen and in return receive audible sounds for the information displayed on screen (i.e., Print, Copy, Scan To).

- **Updated Embedded Web Server guest pages** that meet Web Content Accessibility Guidelines (WCAG) success criteria.

Firmware 121.xxx.045.03600 (D8.0 SPAR Release) R25-02 - Feb 2025

1. Security

This is a Service Pack release that includes a security enhancement for the AltaLink and VersaLink products to mitigate Cross Site Scripting (XSS), Remote Code Execution (RCE), Broken Access Control, and Local Privilege Escalation.

2. Smartcard Kerberos Authentication now supports USB PIV Security tokens such as Yubikey PIV.

Users can now login using either a smartcard or a USB PIV Security token, such as Yubikey PIV, when the device is configured for on-premise Smartcard (Kerberos) Authentication and does not require any unique configuration settings.

The “Smartcard” option in the Login Methods / Control Panel Login pulldown list has been changed to “Authentication Tokens” to reflect the use of Smartcards and USB security tokens.

Note: User interface messaging is updated to reflect “Authentication Tokens” to be consistent with the industry. “Authentication tokens” include Smartcards and USB security tokens which are also commonly referred to as a security token, security key or passkey.

Note: Use of USB Security tokens which plug into the front USB port (such as Yubikey) REQUIRE the installation of the USB Token Hub kit. Contact Xerox Sales for obtaining these kits.

3. Authentication to Cloud Identify Provider (IdP) now supports using Smartcard

Authentication to Cloud Identify Provider (IdP) now supports using Smartcard via certificate-based authentication (CBA).
Users can now login to an IdP using their smartcard by selecting certificate-based authentication (CBA) when prompted on the IdP login screen.

This can be configured by setting "Control Panel Login" to "Identity Provider (IdP) – Validate on Cloud". Corresponding enablement is required on the Customer IdP to enable CBA.

4. Authentication to Cloud Identify Provider (IdP) now supports using USB Security Token

Authentication to Cloud Identify Provider (IdP) now supports using USB Security Token via FIDO2 interface.

Users can now login to an IdP using their FIDO2 USB security token, such as Yubikey, by selecting FIDO2 when prompted on the IdP login screen.
This can be configured by setting "Control Panel Login" to "Identity Provider (IdP) – Validate on Cloud". Corresponding enablement is also required on the Customer IdP to enable FIDO2.

Note: User interface messaging is updated to reflect "Authentication Tokens" to be consistent with the industry. "Authentication tokens" include Smartcards and USB security tokens which are also commonly referred to as security token, security key or passkey.
Note: Use of FIDO2 USB Security tokens which plug into the front USB port (such as Yubikey) REQUIRE the installation of the USB Token Hub kit on all devices. Contact Xerox Sales for obtaining these kits.

Firmware 120.xxx.003.20003 (General Release) July 2024

1. Various Bug Fixes

- Reliability Improvements

Firmware 120.xxx.003.20002 (General Release) April 2024

1. Various Bug Fixes

- Resolved Remote Services Communication Issue
- Service and Reliability Improvements

Firmware 120.028.003.20001 (General Release) Oct. 2023

1. Supports New Components (C415 Model Only)

- Intermittent black page issue seen on Copy / Print jobs has been fixed.

Firmware 120.028.003.20000 (General Release) Sept. 2023

1. Supports New Components

- OCR -- Support scanning to searchable PDF
- Light sleep mode enables a faster recovery from power saver to a ready to print state, thus improving performance from sleep to printing.
- Fax Remote Configuration - Support full remote configuration for fax features via Xerox® Easy Assist app,
- Xerox Device Managed Services.
- Includes support for Thales SafeNet IDPrime 930 Smartcards

- The User Guide for Smart Cards Enablement including the IDPrime driver implementation and support for VersaLink products is available at this link: https://s3s.smartcentre.xerox.com/products-and-supplies/production/customization/customization/office-customization-xcis/xcis-solutions/
- Reliability Improvements
- Performance Improvements

Firmware 119.028.003.04616 (General Release) June 2023

1. Supports New Components

- Accessibility to inverting Display Color
- Cloud & Mobile Ready
- Remove DocuShare Go In-Box App
- Security Improvements, Certificate Management TLS
- SIPRNet Support
- Auto-Configure Low Toner Messaging
- Reliability and Robustness
- Memory Footprint Reduction
- Enablement of a customer installable Productivity Kit (HDD)

2025 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. BR22626
Other company trademarks are also acknowledged.
Document Version: 1.0 (January 2020).