D7.7.1 Xerox® AltaLink® Product Enhancement Document for Version 119.xxx.023.13000

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

Release Date: June 30,2023   dc23rn4165

Product Model	System Software	Network Controller
AltaLink C8170	119.011.023.13000	119.011.13000
AltaLink C8145/55	119.010.023.13000	119.010.13000
AltaLink C8130/35	119.009.023.13000	119.009.13000
AltaLink B8145/B8155	119.013.023.13000	119.013.13000
Altalink B8170	119.014.023.13000	119.014.13000

Xerox Partner Solutions Compatibility issues on V118.xxx.033.10800 (and newer) (2nd Gen Browser Deprecation)

Caution: **Loading Service Pack (R23-02) version 118.xxx.033.10800 (and newer) could potentially cause compatibility issues with older Xerox Partner Solutions versions.** Issues include (but are not limited to):
- Incomplete information displayed in the device UI
- Problems with solution navigation functions such as scrolling, device lock up when attempting to enter data
- Failure to launch the solution at the device

The Xerox Extensible Interface Platform (EIP) is a software platform inside Xerox® Altalink C81xx/B81xx MFPs that allows Xerox and Partner developers to create solutions. Beginning with software (firmware) version 118.xxx.033.10800 on Altalink C81xx/B81xx devices, the second-generation version of the EIP browser was deprecated, leaving exclusive usage of the third-generation browser. The second-generation browser is being deprecated to advance our EIP technology in terms of security and industry standards.

The following list represents the most common Xerox Partner Solutions that may have compatibility issues with Device Firmware (Software) version V118.xxx.033.10800 (and newer). It is not intended to be a comprehensive list of all Solutions that could experience compatibility issues. You need to upgrade to the compatible version of your solution prior to installing this service pack.

Incompatible Partner Solution Version (and earlier)	Upgrade Path to Compatible Version
Kofax eCopy 5.x	EOL
Kofax Equitrac 5.x	Kofax Control Suite 1.2
Kofax AutoStore 7.6	Kofax Control Suite 1.2
Kofax Output Manager 4.2	Kofax Control Suite 1.2
Kofax eCopy 6.4	Kofax Control Suite 1.2
Kofax SafeCom 10.530	Kofax SafeCom G4 10.6.0 / Device Server 9.13
PaperCut MF 21	PaperCut MF 22
Pharos Beacon 3.70.30 / Beacon 5.3 Update 4	Pharos Beacon 3.76.14 /Beacon 5.3 Update 7
YSoft SAFEQ 6	Ysoft SAFEQ 6.0.77
RSA Qdirect 6.0.1 / Qdirect Scan 2.2.3	RSA Qdirect 6.2.0 / Qdirect Scan 2.2.6

Contact your Partner Solution Provider to update your solution.

The following list of Partner solutions are compatible with the third-generation browser:
- Cleo Stream Server 7.4.3
- Kofax
  - Control Suite 1.2
  - Auto Store 8.2
  - Output Manager 5.2
  - Equitrac 6.2 ECSP
  - E-Copy 6.5 Fix Pack 2
  - Kofax Unified Client for Xerox – Equitrac 6.2, AutoStore 8.2, Output Manager 5.2
  - Kofax Combined Client for Xerox – AutoStore 8.2, Output Manager 5.2
  - Kofax Safecom G4 10.6
- LRS MFPsecure Agent 1.3 / VPSX
- OpenText XM Fax EIP V10
- Pharos Beacon 3.76.14 / Blueprint 5.3 Update
- PaperCut MF 22
- Ysoft SAFEQ 6.0.77
- RSA Qdirect 6.2.0 / Qdirect Scan 2.2.6

Notes:
- The latest versions of Xerox Workplace Cloud and Xerox Workplace Suite support the third-generation browser and, thus, are not affected.
- If you load Service Pack (R23-02) version **118.xxx.033.10800 (and newer)** and experience compatibility issues, you need to upgrade your Partner Solution to a compatible version or downgrade your device's software(firmware) to a version that supports the second-generation browser. Firmware (Software) Version 114.xxx.053.10410 supports the second-generation browser and is available at the following link: **114.xxx.053.10410 Release Notes**
- You should disable automatic software update thru the device's Embedded Web Service to ensure you remain on device firmware(software) version 114.xxx.053.10410 or earlier until you upgrade your solution to a version that is compatible with the third-generation browser. Once you upgrade your solution to a version that is compatible with the third-generation browser, you may re-enable automatic software upgrade.

Contents

Latest release information:

Firmware 119.xxx.023.13000 (D7.7.1 General Release) July 2023

1. Features

- **Embedded Web Server and Touchscreen Style Updates:** The Next Generation User Interface style continues to advance. These advancements address customer and design concerns, as well as improvements to intuitiveness and simplification. In this Atlantis release, advancements have been made to the Embedded Web Server and the Touchscreen styles, thus improving the overall user experience.

- **Deprecate Internet Fax:** The Internet Fax feature has been deprecated. Through analysis of data pushes and overall feedback from the field, Internet Fax is rarely used, thus, maintaining the feature costs Xerox® money and resources. Hence, deprecation makes economic sense.

- **Xerox® PSA for Microsoft® Universal Print:** Microsoft® has added support for Printer Support Apps (PSA) to their Universal Print offering. The PSA offers the ability to expose advanced print settings for Universal Print users. Thus, when the user selects "Print Properties" on a Universal Print job, the Xerox® PSA loads and offers the same enhanced, fully featured, Xerox® branded user experience as the Xerox® v4 print driver. This new functionality solves complaints where customers cannot access advanced print features with Universal Print

- **Xerox® Easy Assist App:** The Xerox® Easy Assist mobile app helps customers install, configure, and maintain supported Xerox® devices. The latest Atlantis firmware fully support the Xerox® Easy Assist app, thus simplifying the overall installation of a new Xerox® device. For more information on the Xerox® Easy Assist app, search for "Xerox® Easy Assist" in the Apple and Google Play stores.

Firmware 118.xxx.033.10800(R23-02 D7.6 SPAR Release) April 2023

1. Features

- **Embedded Web Server and Touchscreen Style Updates:** The Next Generation User Interface style continues to advance. These advancements address customer and design concerns, as well as improvements to intuitiveness and simplification. In this Atlantis release, advancements have been made to the Embedded Web Server and the Touchscreen styles, thus improving the overall user experience.

- **Deprecate Internet Fax:** The Internet Fax feature has been deprecated. Through analysis of data pushes and overall feedback from the field, Internet Fax is rarely used, thus, maintaining the feature costs Xerox® money and resources. Hence, deprecation makes economic sense.

- Xerox® PSA for Microsoft® Universal Print: Microsoft® has added support for Printer Support Apps (PSA) to their Universal Print offering. The PSA offers the ability to expose advanced print settings for Universal Print users. Thus, when the user selects "Print Properties" on a Universal Print job, the Xerox® PSA loads and offers the same enhanced, fully featured, Xerox® branded user experience as the Xerox® v4 print driver. This new functionality solves complaints where customers cannot access advanced print features with Universal Print

- Xerox® Easy Assist App: The Xerox® Easy Assist mobile app helps customers install, configure, and maintain supported Xerox® devices. The latest Atlantis firmware fully support the Xerox® Easy Assist app, thus simplifying the overall installation of a new Xerox® device. For more information on the Xerox® Easy Assist app, search for "Xerox® Easy Assist" in the Apple and Google Play stores.

2. Security

- Internal diagnostic page removed
- Standard access mode enhancement to mitigate potential information disclosure.
- Security Improvements
  - **FIPS 140-3:** As security standards evolve, Atlantis based Xerox® MFPs also evolve to meet the new standards. The latest Atlantis firmware now meets the new FIPS 140-3 standard.
  - **WPA3 Wireless Security:** As wireless protocols continue to advance, Xerox® MFPs must also advance to stay current and maintain benchmark security. The Atlantis firmware now supports WPA3 wireless security.

3. Various Bug Fixes

- Altalink B8155 - SNMPTimeOutFault response for SNMP walk request <timeout>0.000001</timeout>
- Vulnerability, Local file inclusion

Firmware 118.xxx.023.02500(R23-01 D7.6 SPAR Release) Feb 2023

1. Enable Local System User Login for Apps

For Smartcard or Convenience Authentication, the SA will be able to configure apps that the Local System User can access.

From the Login Methods page:
1. Set the Control Panel Login to either Smartcards or Convenience Authentication.
2. Edit On-Device Authentication and slide to enable.
3. When using Smartcards, set the Alternate Control Panel Login to Local System User Login.

Xerox AltaLink® C8170

Home | Jobs | Print | Scan | Addres... | | | | | | admin 👤

On-Device Authentication

On-Device Authentication ✓ ‖

Cancel | OK

Search

- Security Dashboard
- Fleet Orchestrator
- Adaptive Learning
- Configuration Overview
- Description
- Configuration Report
- General Setup
- Connectivity
- Login/ Permissions/ Accounting
  - Login Methods
  - User Permissions
  - Accounting Methods
  - Device User Accounts
- Apps
- Security
- Configuration Watchdog

Login Methods

Control Panel & W... Edit...

🖨 → 🗎 **Control Panel Login**
Smart Cards

🖨 **Website Login**
User Name / Password
Validate on the Device

Alternate Control Panel Login
Disabled

Configuration Settings	Method	Status	Action
Domain Controllers	Control Panel	❌ Required; Not Configured	✎ Edit...
Certificate Validation	Control Panel	✱ Optional; Not Configured	✎ Edit...
Smart Card Inactivity Timer	Control Panel	☑ Optional; Configured	✎ Edit...
Acquiring Logged in User's Email Address	Control Panel	✅ Optional; Configured	✎ Edit...
Customize Blocking Screen	Control Panel	✅ Optional; Configured	✎ Edit...
Device User Accounts	Device Website	✅ Required; Configured	✎ Edit...
Device Account Requirements	Control Panel & Website	☑ Optional; Configured	✎ Edit...
Personalization	Control Panel	☑ Default; Configured	✎ Edit...
Personalization Profiles	Control Panel	✅ No Profiles Saved	✎ Edit...
LDAP Servers	Personalized User Profile	✅ Required; Configured	✎ Edit...
Log Out Confirmation	Control Panel (Alternate)	☑ Optional; Configured	✎ Edit...
EIP Authentication	Control Panel	✱ Optional; Not Configured	✎ Edit...
Single Sign On Identity Provider	Touch UI	✱ Optional; Not Configured	✎ Edit...
Kerberos Setup	Touch UI	✅ Optional; Configured	✎ Edit...
USB Reset Policy	Touch UI	☑ Optional; Configured	✎ Edit...
On-Device Authentication	Touch UI	✱ Optional; Not Configured	✎ Edit...

Graphic Key

Xerox AltaLink® C8155

Home | Jobs | Print | Scan | Address Book | Properties | Support | admin 👤

🖥 / Login Methods

Search

- Security Dashboard
- Fleet Orchestrator
- Adaptive Learning
- Configuration Overview
- Description
- Configuration Report
- General Setup
- Connectivity
- Login/ Permissions/ Accounting
  - Login Methods
  - User Permissions
  - Accounting Methods
  - Device User Accounts
- Apps
- Security
- Configuration Watchdog

**Edit Login Methods**

Control Panel & Website Login Methods

🖨 → 🗎 **Control Panel Login**
Smart Cards ▼

Smart Card Type
All Supported Smart Cards ▼
Supported Smart Cards List: Default Smart Card List

🖨 → 🗎 **Alternate Control Panel Login**
User Name / Password - Validate on the Network ▼ Why would I use this feature?
Disabled
User Name / Password - Validate on the Network
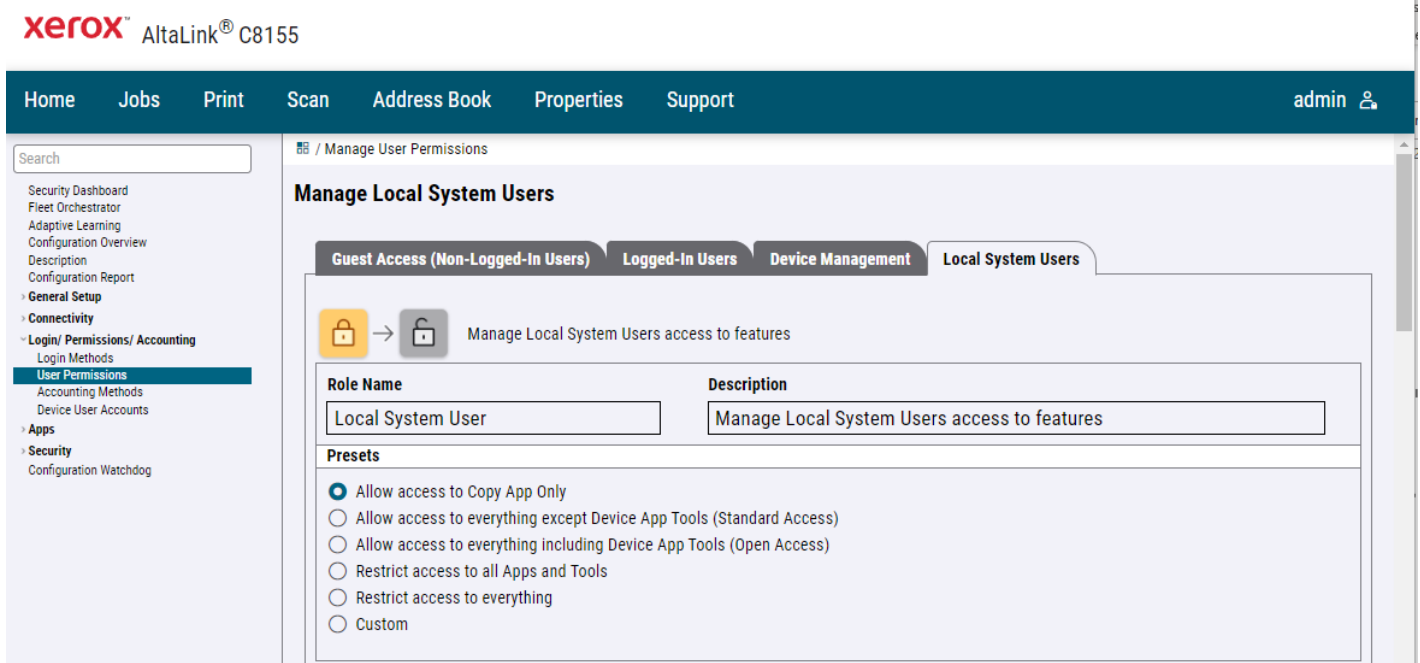**Local System User Login**

🖨 **Website Login**
User Name / Password - Validate on the Device ▼

Customize Supported Smart Card List | Cancel | Save
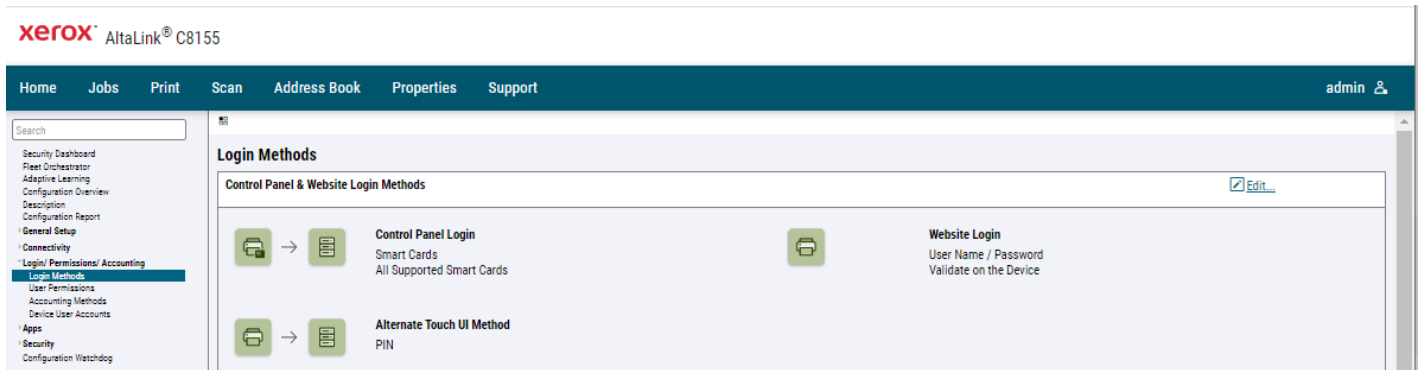
On the User Permissions page, Local System Users tab set the app permission for the Local System User using the presets or individually to customize.

Firmware 114.xxx.053.10410 (R22-12 D5.6 General Release) Feb 2023

1. Various Bug Fixes

- Domain Name Not Configured"/ "Email is Not Configured". This could be caused either by an issue with the device's ability to automatically acquire Domain Name settings from the network or as result of an error after a Software Upgrade.

Firmware 118.xxx.052.32600 (R22-10-D7.6 SPAR Release) Dec. 2022

1. Require User Confirmation to Auto-Release Secure Print Jobs Upon Login Policy

A new Secure Print Job Release policy has been added to the Properties / Apps / Printing / Secure Print / Device Policies Web UI webpage. The new policy: "Require User Confirmation to Auto-Release Secure Print Jobs Upon Login" is selectable if "Release Jobs Without Prompting for Passcode" has been enabled <factory default>.

When this 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".

2. LDAP User Mapping Properties Access

The behavior of the LDAP user mapping webpage has been changed to enable the logged-in Device Administrator to see/change LDAP User Mappings without first having to login to the LDAP server and perform an LDAP query. This is helpful for making user LDAP changes for accounts that no longer provide Xerox Service personnel with LDAP Server username and password (system credentials).

3. ID Card Copy and EWS Apps configuration

The local device user interface will display the ID Card Copy app to the user at factory defaults.
The EWS interface will allow the Admin user to configure apps on the Enablement screen (Properties / Apps / Enablement). Apps can be changed to "Available" / "Unavailable" (ie. enable/disable) on the device LUI. Apps can be changed to "Visible" / "Invisible" (ie. hide/show) on the LUI.

4. Embedded Fax EIP API

The EIP Scan API has been extended to now include support for embedded fax. EIP apps can now be written that can use this new API to send a fax using the onboard fax option.

5. AltaLink Cloning Configuration

The AltaLink Cloning Configuration feature allows a device administrator to clone the full set of cloneable system attributes, including FIPS. FIPS Enablement is now a cloneable attribute, and when cloning from a source device with FIPS Enabled, the FIPS Acknowledgements will also be cloned on the target device. A FIPS Enabled device must use full cloning, meaning all fields will be cloned, no partial cloning can be done.

Additionally, two formerly hidden web pages have been made available to the device administrator on the WUI:
1. A checkbox on the Web UI for setting Resolve Hostname: **Apps > Scan To Home > General**
2. A policy toggle on the Web UI for setting the Lock Files policy: **Apps > Scan To > Setup > Scanning Lock Files Policy**

6. Security
- Addressed pages vulnerable to XSS attack.
- Addressed unauthenticated Denial of Service

Firmware 114.xxx.002.21400 (D5.6General Release) October 2022

1. Supports New Components

Due to the world-wide issue of part shortages, alternate electronic components were required for the Single Board Controller. This new software release is needed to support additional component changes

Firmware 114.xxx.001.31515 (D5.6) July 2022

1. Supports New Components

Due to the world-wide issue of part shortages, alternate electronic components were required for the Single Board Controller. This new software release is needed to support additional component changes.

Firmware 114.xxx.001.31514 (D5.6) May 2022

1. Install Wizard Fixes
2. Bug Fixes with certain Diagnostic Routines
3. Prevention of SW Downgrade with certain versions of Single Board Controllers
4. Support for the new Single Board Controller (SBC) components.

- Due to the world-wide issue of part shortages, alternate electronic components were required for the single board controller. From the beginning of year 2022, newly manufactured devices will have this new SBC and it will be introduced into spares inventory. The SBC will have Tag 3 checked on its tag matrix to the left of the board.