Xerox® AltaLink®
Product Enhancement Read Me

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

Release Date: **August 9, 2019**

Product Model	System Software	Network Controller
Xerox® AltaLink® C8070	101.003.069.20900	101.003.20900
Xerox® AltaLink® C8045/55	101.002.069.20900	101.002.20900
Xerox® AltaLink® C8030/35	101.001.069.20900	101.001.20900
Xerox® AltaLink® B8045/B8090	101.008.069.20900	101.008.20900

Contents

Firmware 101.xxx.069.20900 August 2019 4

1. Low Power Mode 4

Firmware 101.xxx.069.17810 July 2019 4

1. Xerox® Lockdown Security Solution 4
2. Oberthur ID-One PIV V8 Card Supported when using Smart Card Authentication 4
3. Additional Fixes Included in this Version 4

Firmware 101.xxx.059.13300 May 2019 4

1. Card Reader 4

Firmware 101.xxx.059.12100 May 2019 4

1. EIP Peripheral API updates 4
2. EIP ability to request LDAP user attributes to include in user session data 4
3. Translations added for B&W Output Color setting Auto 5
4. Xerox® Lockdown Security Solution 5
5. General Fixes 5

Implemented a fix to include the 1 gigabyte option on the CWIS page. 5

Firmware 101.xxx.029.03810 March 2019 5

1. User Permissions 5
2. Restricted access to print color 5

Firmware 101.xxx.009.00300 January 2019 6

1. B&W saved jobs 6
2. Safenet SC650 v4.0 SIPRNet tokens 6
3. Group Fax Improvements 6

Firmware 101.xxx.028.32100 December 2018 6

1. Color Quality Improvements 6
2. Various bug fixes 6
3. Enablement of SecuraKey ET4-AUS-D-WR8 Proximity Card Reader 6
4. Mixed Size Originals Feature support for Oficio Media (8.5x13.4) 6
5. Support for Croatian and Ukrainian languages. 6
6. Security 6
7. Re-Introduced Support for Gemalto IDPrime MD 3810 and 830b cards 6

Firmware 101.xxx.008.27400 Nov 2018 7

1. PCL Printing Improvement 7
2. Fax Confirmation Sheet 7

Firmware 100.xxx.068.26100 Sept 2018 7

1. Image Quality Improvements 7
2. Support for Gemalto IDPrime MD 3810 and 830b cards 7
3. Secure Print with smartcard user identification 7
4. PKCS12 certificate installation 7

Firmware 100.xxx.058.22800 Aug 2018 7

1. Image Quality Improvements 7
2. General fixes for Authentication and Connectivity. 7
Firmware 100.xxx.048.17300 July 2018 9
1. Enablement for POP3 Over Secured Connection (TLS). 9
3. Image Quality Improvements 9
4. General fixes for Copy, Print and Output functionality. 9
Firmware 100.xxx.038.10200 April 2018 10
1. Hide Network Troubleshooting 10
2. Ability to Edit Device Address Book for Server Fax on the LUI (On The Fly) 11
3. Image Quality Improvements 14
4. Authentication. 14
5. General fixes for Copy, Print and Output functionality. 15
Firmware 100.xxx.028.05200 March 2018 15
1. Image Quality Improvements 15
2. Scanning 15
3. Authentication. 15
4. General fixes for Copy, Print Output, and EIP functionality. 15
Firmware 100.xxx.018.01610 January 2018 15
1. Image Quality Improvements 15
2. SMB Scanning 16
3. Xerox Dropbox App blank screen 16
4. Scanning CAC/PIV/Smartcard Authentication 16
5. General fixes for Accounting, Copy, Print Output and EIP functionality. 16
Firmware 100.xxx.107.34110 December 2017 16
1. Image Quality Improvements 16
2. Xerox Dropbox App blank screen 17
Firmware 100.xxx.107.28600 October 2017 17
1. ThinPrint Protocol Support 17
2. Ability to hide username or IDs for Security 19
3. Xerox® Lockdown Security Solution / Healthcare Lockdown Solution 20
Firmware 100.xxx.077.17900 & (.17010 for B8045/B8090) July 2017 21
5. Custom Administrator Solution 21
2. Cloning Webservice 22
3. EIP Authentication 23
4. Disable Print Submission of Clone Files 23
5. Disable SNMP Sets 23
6. XML Configuration Report 23
7. Support Log Tab 23
8. Network Troubleshooting Log Feature 23

Firmware 101.xxx.069.20900 August 2019

1. Low Power Mode

This release fixes as issue found in version 101.xxx.069.17810 where the device would not wake up when in Low Power mode even though the user pressed the Power Saver button. Print jobs would wake the device successfully.

Firmware 101.xxx.069.17810 July 2019

1. Xerox® Lockdown Security Solution

This release introduces other languages in support for this feature.

2. Oberthur ID-One PIV V8 Card Supported when using Smart Card Authentication

Oberthur ID-One PIV cards are now supported when using smart card authentication.

3. Additional Fixes Included in this Version

- Applying the clone file to a machine using a customer certificate no longer causes the device to revert to the self-signed certificate.
- Improvements made during the boot process to eliminate DHCP error when connecting to an 802.1x network
- Machine will now reliably exit from power saver mode and no longer need to be unplugged to become active.
- If Remote Services is disabled, the audit log will no longer display “remote Service.sh crash” messages.
- Additional improvements made to prevent the message “Card Reader Detected” from appearing.

Firmware 101.xxx.059.13300 May 2019

1. Card Reader

This release fixes an issue reintroduced in AltaLink software versions 101.xxx.008.27400 – 101.xxx.059.12100 where a “Card Reader Detected” Pop Up message appears on the device local user interface after wake up from sleep mode. This issue is fixed whether the card reader is plugged into the front or back USB port and whether the card reader is directly connected to the device or is connected using a USB splitter cable.

Firmware 101.xxx.059.12100 May 2019

1. EIP Peripheral API updates

The EIP Peripheral API has been updated to provide more information on TWN 4 card readers attached to an AltaLink device. The EIP Peripheral API previously communicated the card reader Vendor ID, Product ID, and Interface Type (keyboard). The new capability also provides Serial Number, Firmware version, Interface protocol and interface class. This information can be retrieved by Xerox Device Manager and used by Xerox Service Manager and PLM for asset tracking of the card readers.
Refer to the latest version of EIP DDK or SDK for more information on the EIP Peripheral API.

2. EIP ability to request LDAP user attributes to include in user session data

Added the EIP ability to request sAMAccountName & userPrincipalName from LDAP as part of the xrxSessionGetSessionInfo() call in the Session Web service to include in the user session data.

This method allows a client to retrieve information about the currently logged in user. It returns a block of XML data that is defined by the SessionInfoSchema.xsd. An optional parameter can be passed in to request a list of LDAP attributes from the MFD.

Note: Other LDAP values may become available in the future, but for now only sAMAccountName & userPrincipalName are available.

Note: For the GetSessionInformation request to return info for sAMAccountName & userPrincipalName the following must be true on the MFD being used:

- The EIP version must be 4.1.4+ or 3.5.7+ (EIP 3.7.X not supported)
- LDAP must be configured on the MFD
- LDAP Personalization must be completed successfully for the user logged in at the MFD Local UI

Refer to the latest version of EIP DDK or SDK for more information on the EIP Peripheral API.

3. Translations added for B&W Output Color setting Auto

Language Translations have been provided for the B&W Saved Jobs feature provided in a previous release (101.xxx.009.00300). Full translations for "Auto" are now available in the Print From app.

4. Xerox® Lockdown Security Solution

This release introduces the Xerox® Lockdown Security Solution previously known as Xerox® Healthcare Lockdown Solution, initially introduced with Firmware 073.xxx.197.2850 October 2017. (This release includes English language only. Other language translations will be added in a future release.)

Note: The Xerox® Lockdown Security Solution kit part number 301K33790 can be ordered by contacting your Xerox® account representative.

Installation of this release enables a device Administrator to install the purchasable Xerox® Lockdown Security Solution on a device. While the Solution content is contained in this release, the feature is hidden until it is activated by purchase of the kit and installation of a Feature Installation Key (FIK).

The Xerox® Lockdown Security Solution permanently enhances certain security aspects of the Xerox® WorkCentre® Devices by encrypting the hard drive, overwriting hard drive data immediately after use, preventing jobs from being stored on or printed from USB devices, recording who has used the device and how they used it and providing additional controls designed to protect specific Xerox® networked and non-networked devices against malicious attacks.

Refer to description in Firmware 100.xxx.107.28600 October 2017 for more details.

5. General Fixes

Implemented a fix to include the 1 gigabyte option on the CWIS page.

Firmware 101.xxx.029.03810 March 2019

1. User Permissions

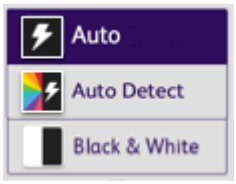
User permissions of Allow Only Secure Print is now working.

2. Restricted access to print color

Restricted access to print color for non-logged in users is no longer printing in color instead of black and white.

Firmware 101.xxx.009.00300 January 2019

1. B&W saved jobs



After installing this release: in the ”Print From” app, the default ”Output Color” for saved jobs will be “Auto,” meaning saved jobs will print as defined by their submitted color attributes. If they were saved as a B/W image, they will print as a B/W image. If they were saved as color images, they will print as color images. The previous default “Auto Detect” is still available. “Auto Detect” will print jobs according to their image composition. If color pixels are detected in the image, it will print in color. (Note: USA English only. Other languages will be delivered in a future release.)

2. Safenet SC650 v4.0 SIPRNet tokens

Added support for the SafeNet SC650 v4.0 SIPRNet card to this release.

3. Group Fax Improvements

The group fax application can now send to a large number of faxes successfully. It will no longer fail and lockup.

Firmware 101.xxx.028.32100 December 2018

1. Color Quality Improvements

Many color quality improvements for Scan, Copy, and Print are included in this release above and beyond previous releases. After installing this release, ensure a copy and print calibration have been performed. If quality is still not acceptable, contact Xerox Customer Technical Support.

2. Various bug fixes

- When opening and closing the envelope tray, the message will be correctly cleared.
- Sending tabloid size PDF documents using IPP protocol no longer results in job shrinking to fit on Letter size paper.
- Fax Forward fields can now be cleared and reset to default.

3. Enablement of SecuraKey ET4-AUS-D-WR8 Proximity Card Reader

SecuraKey card reader model: ET4-AUS-D-WR8 is supported in this release.

4. Mixed Size Originals Feature support for Oficio Media (8.5x13.4)

When the setting under WebUI General Setup > Paper Management > Required Paper Policies / Default Legal Size is set to default size as “8.5 x 13.4” (Mexican Legal – Oficio), then the Mixed Size Original Feature will allow scanning of “8.5 x 13.4” size paper with 8.5x11 documents.

5. Support for Croatian and Ukrainian languages.

Support has been added for Croatian and Ukrainian languages. This includes the user interface language as well as help screens and embedded web pages.

6. Security

- Various cross scripting vulnerabilities (XSS) have been addressed.
- Vulnerabilities found in OpenSSL (CVE-2016-2109 CVE-2016-2105 CVE-2016-2106 CVE-2016-2176 CVE-2016-2107)

7. Re-Introduced Support for Gemalto IDPrime MD 3810 and 830b cards

Support for Gemalto IDPrime MD 3810 and 830b cards are being reintroduced because the General Release 101.xxx.008.27400 did not include support for these cards.

Gemalto has discontinued the Gemalto IDPrime .Net 510 cards and replaced them with the new Gemalto IDPrime MD 3810 and MD830b cards. These new cards are now supported in the 101 firmware release.

Note: A Caveat for this release: Email signing feature with FIPS 140-2 mode enabled will not function. If both Email signing and FIPS 140-2 are required please contact Xerox customer support.

Firmware 101.xxx.008.27400 Nov 2018

1. PCL Printing Improvement

The device now uses 8 Bit PCL for all standard PCL printing, which delivers the best image quality for PCL mode.

2. Fax Confirmation Sheet

The fax confirmation sheet will no longer stop working intermittently.

Firmware 100.xxx.068.26100 Sept 2018

1. Image Quality Improvements

Implemented functionality to improve PCL print quality in default Standard mode. To enable these improvements, the patch 1284222v4 is included in the 100.xxx.068.26100 software installation zip file and must be installed using the instructions provided.

2. Support for Gemalto IDPrime MD 3810 and 830b cards

Gemalto has discontinued the Gemalto .Net 510 cards and replaced them with the new Gemalto IDPrime MD 3810 and MD830b cards. These new cards are supported in this release.

Note: A Caveat for this release: Email signing feature with FIPS 140-2 mode enabled will not function. If both Email signing and FIPS 140-2 are required please contact Xerox customer support.

3. Secure Print with smartcard user identification

Implemented Fix that applies the correct user's username for secure print job release.

4. PKCS12 certificate installation

Implemented a fix that corrects incomplete installation of PKCS12 formatted private key and chain of trust certificates.

Firmware 100.xxx.058.22800 Aug 2018

1. Image Quality Improvements

Implemented functionality to improve PCL print quality in default Standard mode. To enable these improvements, the patch 1284222v3 is included in the 100.xxx.058.22800 software installation zip file and must be installed using the instructions provided.

2. General fixes for Authentication and Connectivity.

Implemented a fix to eliminate a case where, after logging in with a Smartcard, a Network Address Book search resulted in an error message that read "The device cannot process results from Network Address Book, device decoding error (e.g. out of memory).

Fixed a CAC card Login failure with "KRB5KDC_ERR_POLICY NT Status: Unknown error code 0xc00002fa".

Corrected a defect where the device was placing a dot (.) character at the end of the domain name resulting in the DNS Server's inability to resolve the Printer's Host Name.

Placing a dot (.) at the end of the domain name is now an optional setting that is settable by the System Administrator. When the 'Complete domain name(s) with dot character' option is selected, the device will automatically append a dot (.) to the end of domain names. This setting ensures that domain names are interpreted as absolute domain names, which can improve DNS resolution.
In order to change the setting:

1. Navigate to the printer's WebUI
2. Select Properties
3. Select Connectivity
4. Select Setup
5. Select the "Edit" link to edit the "Wired Connection" setting
6. Select the "Edit" link to edit the "Internet Protocol" setting
7. Select the "Show DNS Settings" button
8. Select/de-select the "Complete domain name(s) with dot character" as desired
9. Select the "Apply" button at the bottom of the page
10. Select the "OK" button on the change confirmation pop-up window
11. Select the "Close" button on the "Updating IP Settings" page
12. Select the "Close" button on the "Wired Profile" page to return to the <Properties/Connectivity/Setup> page
13. Close the Browser or continue configuring the device as required.

Firmware 100.xxx.048.17300 July 2018

1. Enablement for POP3 Over Secured Connection (TLS).

Office 365 Servers require TLS encryption for POP3 traffic over Port 995. To support receiving emails from Office 365 POP3 Over Secure Connection (TLS) has been added.

To Enable POP3 Over Secure Connection (TLS) simply do the following:

a. Using the device IP address, log onto the CWIS as Admin.

b. Go to **Properties>Connectivity>Setup**

c. Select **Edit** for POP3.

d. Check the **Pop3 Over Secure Connection (TLS)** checkbox and notice that the **Validate Server Certificate** checkbox is automatically checked, and the POP3 Server port value has defaulted to Port 995.

Note: A port value of 995 is not permitted with an unsecure connection. It is recommended to upload Trusted Root /Intermediate certificates to the device for certificate validation.

e. Enter your POP3 Server I**Pv4 Address** or **Host Name**.

f. Enter **Login Name** and P**assword**.

g. Enter password again under **Retype password** and check the **Select to save new password** checkbox.

h. Select **Save**

3. Image Quality Improvements

Implemented a fix to Copy and SCAN in B&W mode for better reproduction of yellow colors..

Implemented fixes in Copy B&W mode. Light and dark Grey halftones are reproduced correctly.

4. General fixes for Copy, Print and Output functionality.

Implemented a fix to eliminate a case where colored lines appeared in the process direction and a fault was declared when printing or copying on plain, glossy or cardstock paper, or when the bypass tray empties while in use.

.

Fixed a device reboot during workflow scanning with single touch scan + meta data when pressing X to close the metadata prompt window.

Fixed incorrect stacking on the 2KLCSS finisher when printing multiple consecutive single-page documents

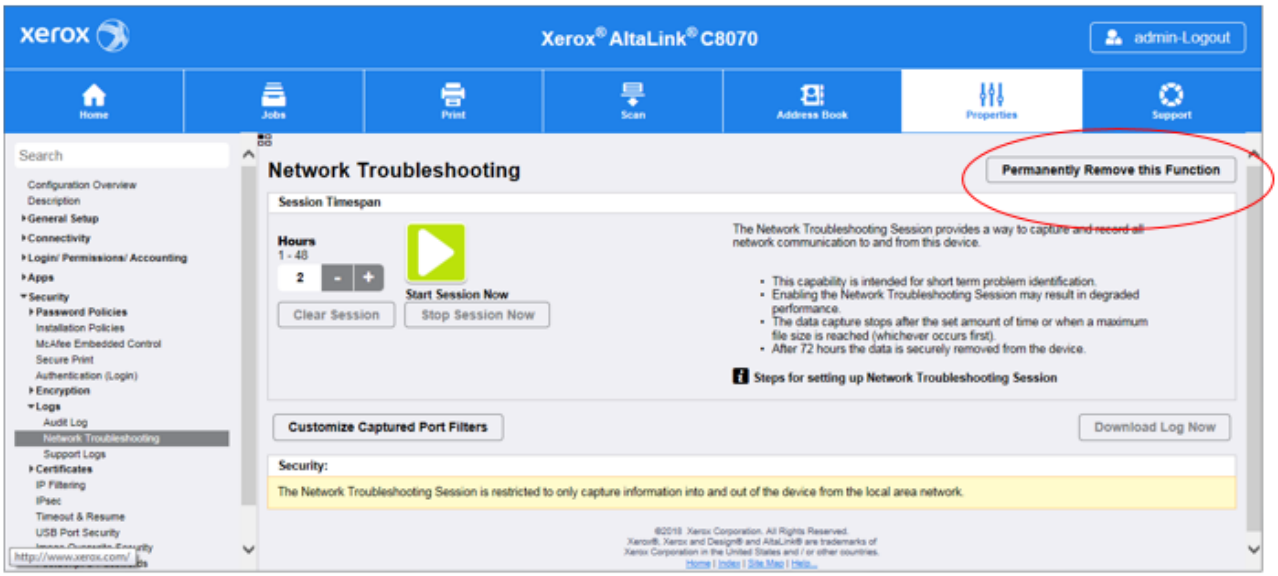
Fixed an issue where the permission roles to control user access to Web UI were not functioning as expected

Firmware 100.xxx.038.10200 April 2018

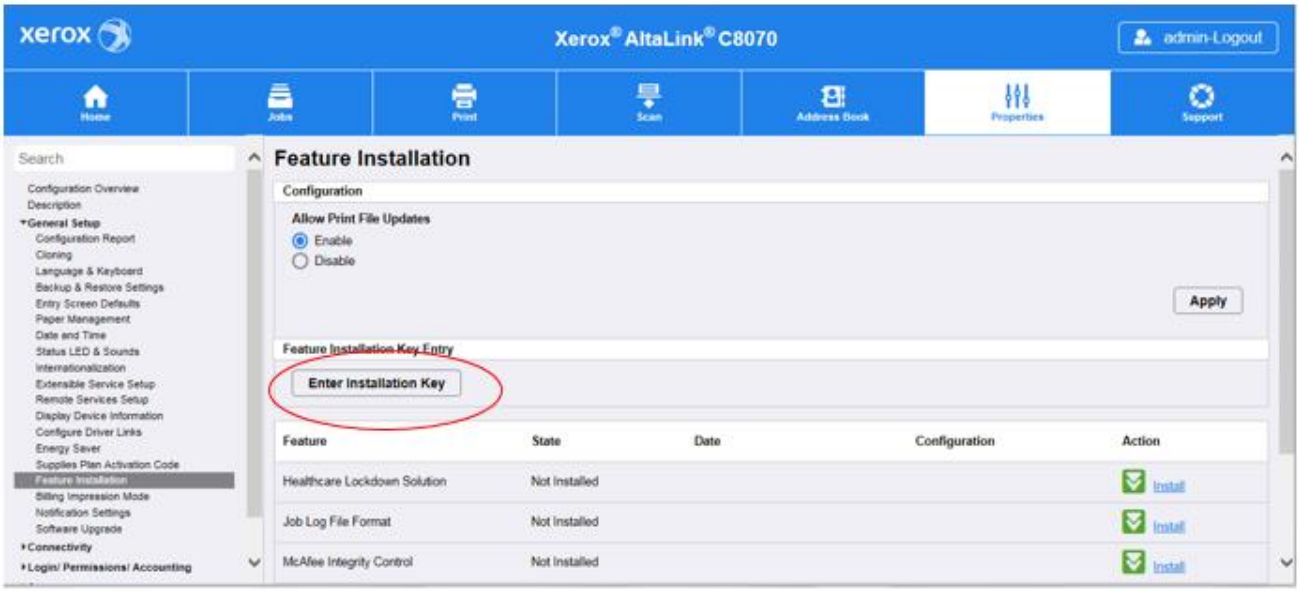
1. Hide Network Troubleshooting

Overview: Altalink Devices have added the ability to permanently remove the Network Troubleshooting feature.
Note: The will permanently remove the Network Troubleshooting feature from the device.

There are two methods to remove the feature from the device.
There is a button called permanently remove Network Troubleshooting page that will allow an Administrator to "hide" the feature. The button is on the Properties, Security, Log, Network Troubleshooting page. Below is an image of the button.



The second method is to install a FIK Key on Properties, General Setup, Feature Installation page by selecting Enter Installation Key.
The FIK key to permanently remove the Network Troubleshooting feature is **468854198391**



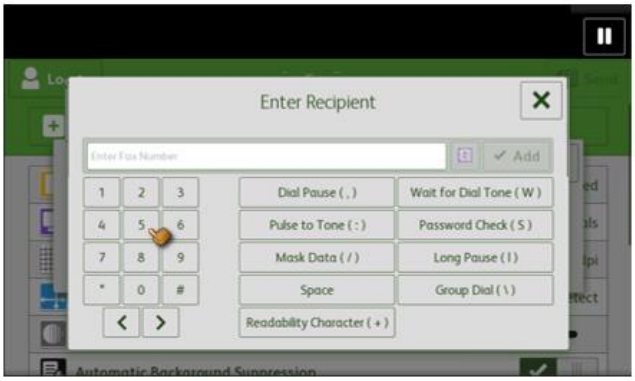
Permanently removing the Network Troubleshooting feature can be cloned.
There is also support of a MIB to Hide and Unhide the Network troubleshooting feature (using FIK OID).
The Network troubleshooting Feature will be available by default.
Only a user with Administrator privileges can remove the Network troubleshooting feature.

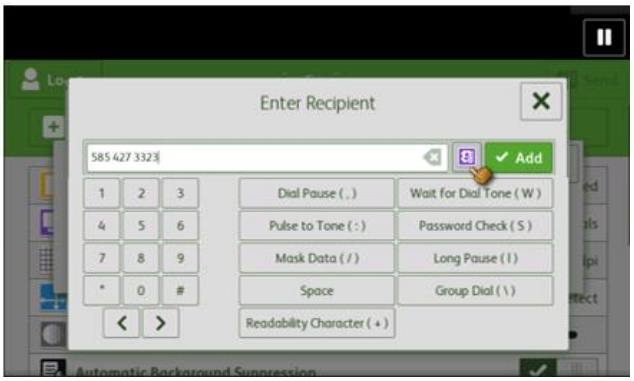
2. Ability to Edit Device Address Book for Server Fax on the LUI (On The Fly)

Overview: On The Fly is a feature which allows the user to create a new contact or add to an existing contact to the Device Address Book for Server Fax right from the LUI.

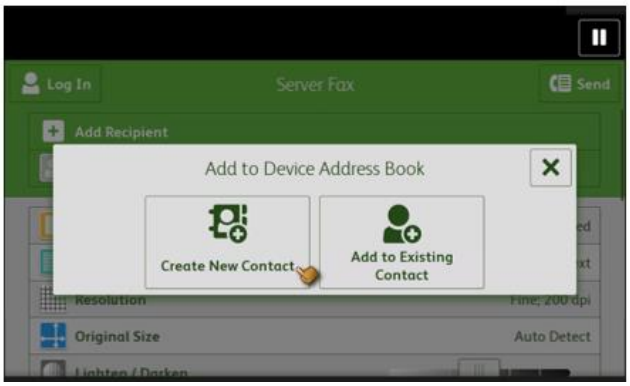
Creating From Server Fax 'Enter Recipient' Screen:
When creating a New or Existing Contact to Add to the Device Address book from the Server Fax App, simply select 'Manual Entry'.

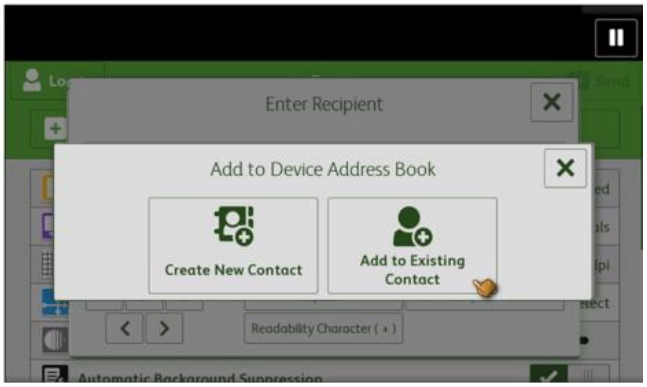
Enter recipient fax number and then select the 'On The Fly' icon to add to address book.





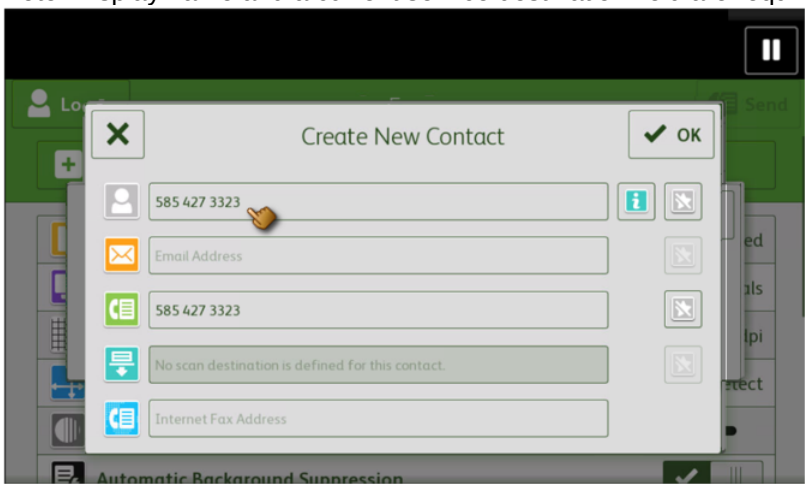
Select 'Create New Contact' if new or select 'Add to Existing Contact' if contact already exists.





When Creating New Contact:
Edit ‘Display Name’ and select ‘OK’.
Edit ‘Email Address’ and select ‘OK’.
On the ‘New Contact Card’ pop up select ‘OK’.

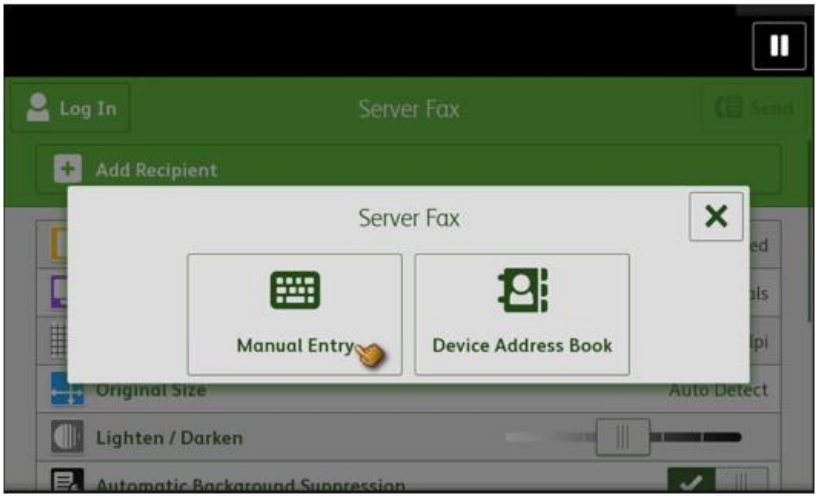
Note: Display name and a current service destination field are required and cannot be empty..



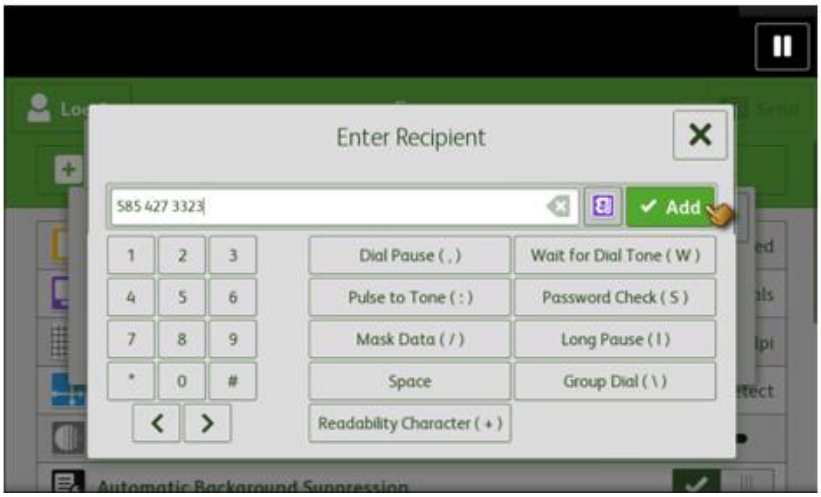
When Adding from Existing Contact Select the desired contact to add and select ‘OK’

Contact is now added to the address book and recipient list.

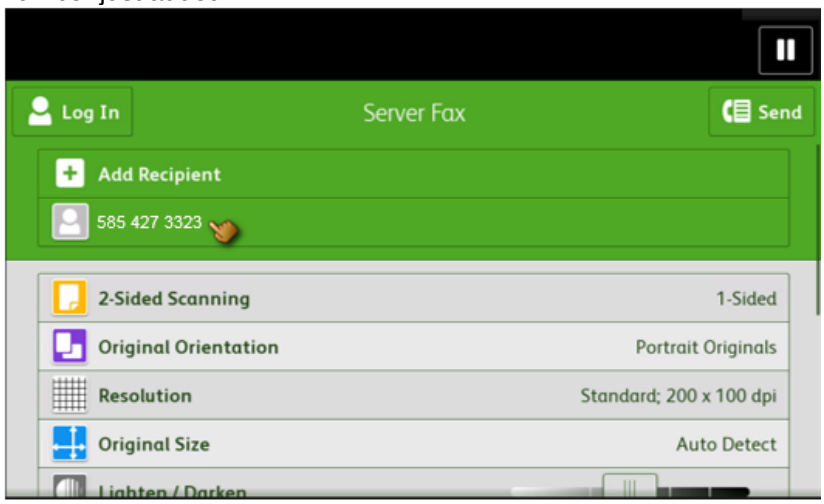
Creating From Server Fax Recipient List:
When creating a New Contact to Add to the Device Address book from the Server Fax App, simply select ‘Manual Entry’.



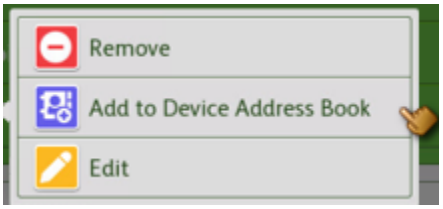
Enter recipient fax number and select ‘Add’.



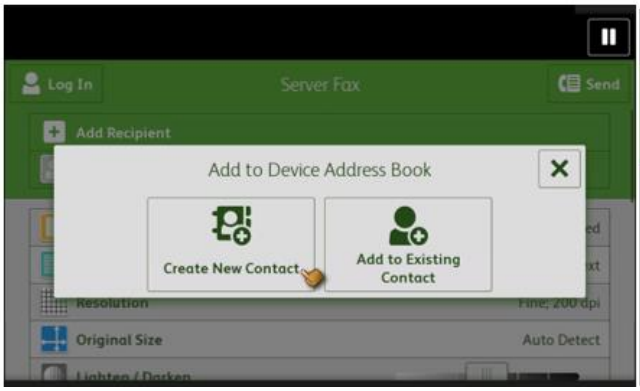
Add ‘Display Name’ and ‘Email Address’ to the Device Address Book by selecting the field with the Fax number just added.

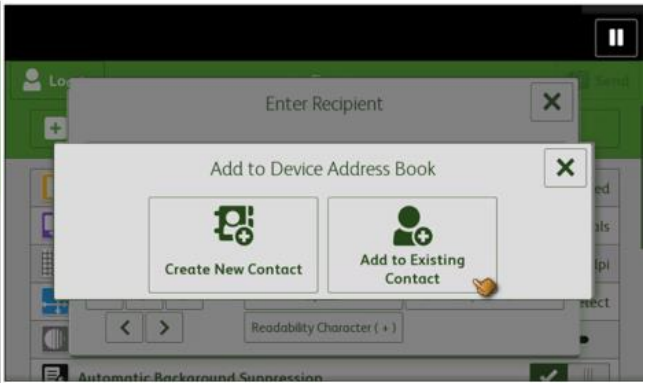


Then Select ‘Add to Device Address Book’



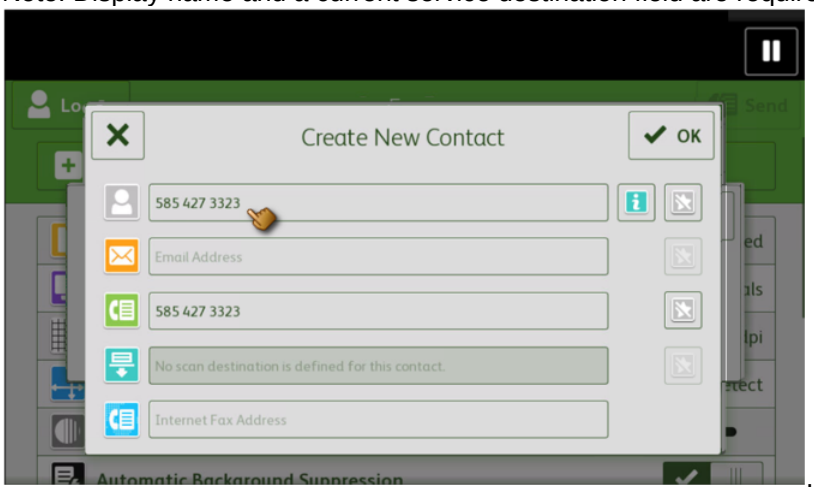
Select ‘Create New Contact’ if new or select ‘Add to Existing Contact’ if contact already exists.





When Creating New Contact:
Edit ‘Display Name’ and select ‘OK’.
Edit ‘Email Address’ and select ‘OK’.
On the ‘New Contact Card’ pop up select ‘OK’.

Note: Display name and a current service destination field are required and cannot be empty.



When Adding from Existing Contact Select the desired contact to add and select ‘OK’

Contact is now added to the address book and recipient list.
.

3. Image Quality Improvements

Implemented a fix to eliminate faded print output in PostScript mode.

Eliminated intermittent yellow bands, appearing in the inboard to outboard direction of output after reloading an empty bypass tray.

If color output is still not acceptable after upgrading to this release, ensure that Print Calibration and Copy Calibration routines have been run. If quality is still not acceptable contact Xerox Customer Technical Support.

4. Authentication.

Fixed an authentication failure where the printer used the wrong certificate ID when attempting to authenticate with CAC authentication.

Fixed an email failure where the device sent the incorrect domain component during an SMTP authentication.

Email authentication no longer fails when a single quote (‘) is in the user name.

5. General fixes for Copy, Print and Output functionality.

The Altalink device no longer interprets some postscript grayscale pages as color.

Several fixes were implemented for better keyboard functionality and some special characters not being available on the keyboard.

A fix was implemented where the printer would reset after accessing the list of multiple secure print jobs on the local user interface.

Machine no longer crashes when performing Booklets with the BR finisher

Machine no longer can switch to copy mode only when installing the C/Z trifold finisher module

Fixed an issue where the permission roles to control user access to Web UI were not functioning as expected

Firmware 100.xxx.028.05200 March 2018

1. Image Quality Improvements

A fix was implemented for the symptom of lines and stripes across the output page and fault codes 319-409 and 319-410.03 are displayed when copying or scanning.

If color output is still not acceptable after upgrading to this release, ensure that Print Calibration and Copy Calibration routines have been run. If quality is still not acceptable contact Xerox Customer Technical Support.

2. Scanning

A fix was implemented to prevent the incorrect image size output on the last two segments when using the build job feature for Scan to file.

A fix was implemented to eliminate incorrect file naming when using the '1 file per page' setting along with a custom naming convention in a scan workflow.

3. Authentication.

Fixed an issue of a "Server login error" displayed on the MFD LUI after an open user session is already started.

4. General fixes for Copy, Print Output, and EIP functionality.

A problem was fixed in a scenario where a secure job is sent to an Altalink device, a user is not able to release it using the Job Management Client API, even when they correctly supply a pin code.

Fixed an MFD reboot during a copy job, when the user selects the legal size tray, places a legal document on the platen, selects Reduce/Enlarge>More>Independent with Y set to 97% and X to 99%. After pressing start, the display indicates "Scanning your job" but the start button is grayed out and the document is never scanned and MFD eventually reboots.

Firmware 100.xxx.018.01610 January 2018

1. Image Quality Improvements

This software update includes image quality improvements for the C80xx devices.

Text Original Type image quality parameters have been improved for all speeds and walkup mode parameters have been improved for the C8070.

PostScript Standard IQ improvements have been made. This change improves color reproduction consistency and coherency between the different models.

The “rainbow” or color banding effect that could be seen when making many rapid successive copies or scans has been fixed.

Improvements have been made to provide more stable color rendition after software upgrade and over time as the environment changes.

If color output is still not acceptable after upgrading to this release, ensure that Print Calibration and Copy Calibration routines have been run. If quality is still not acceptable contact Xerox Customer Technical Support.

2. SMB Scanning

A fix has been implemented to prevent a login failure when scanning to Netapp Filer(NAS) over SMB
Special Instructions
The customer administrator should log into the upgraded printer and then:
Select Properties > Connectivity > SMB Filing, then select Edit and de-select SMB2 and SMB3 then check SMB1. Apply the selection change.

3. Xerox Dropbox App blank screen

The functionality for the patch file that was included in the 100.xxx.107.34110 software installation zip file, which corrected a malfunction when initiating the Xerox Dropbox, has been implemented in this release. The patch is no longer required when upgrading to this release.

4. Scanning CAC/PIV/Smartcard Authentication

Fixes have been implemented to prevent Scan to Home failures when CAC/PIV/Smartcard is used for Authentication

5. General fixes for Accounting, Copy, Print Output and EIP functionality.

Firmware 100.xxx.107.34110 December 2017

1. Image Quality Improvements

This software update improves the image quality of copied pages primarily for the C8070 devices. Improvements have been made for Photo mode and Text mode when copies are made. Fine lines have been improved as well when using Postscript printing.

When installing updated software, a print calibration process for PCL will not be performed unless required by other component changes. This will provide more consistent PCL print quality through the software upgrade process. Additionally, print quality has been made more consistent for all speeds within the Color AltaLink product line

If color output is still not acceptable after upgrading to this release, ensure that Print Calibration and Copy Calibration routines have been performed. If quality is still not acceptable, contact Xerox Customer Technical Support.

2. Xerox Dropbox App blank screen

There is an additional patch file included in the software installation zip file. This patch corrects a malfunction when initiating the Xerox Dropbox App.

Firmware 100.xxx.107.28600 October 2017

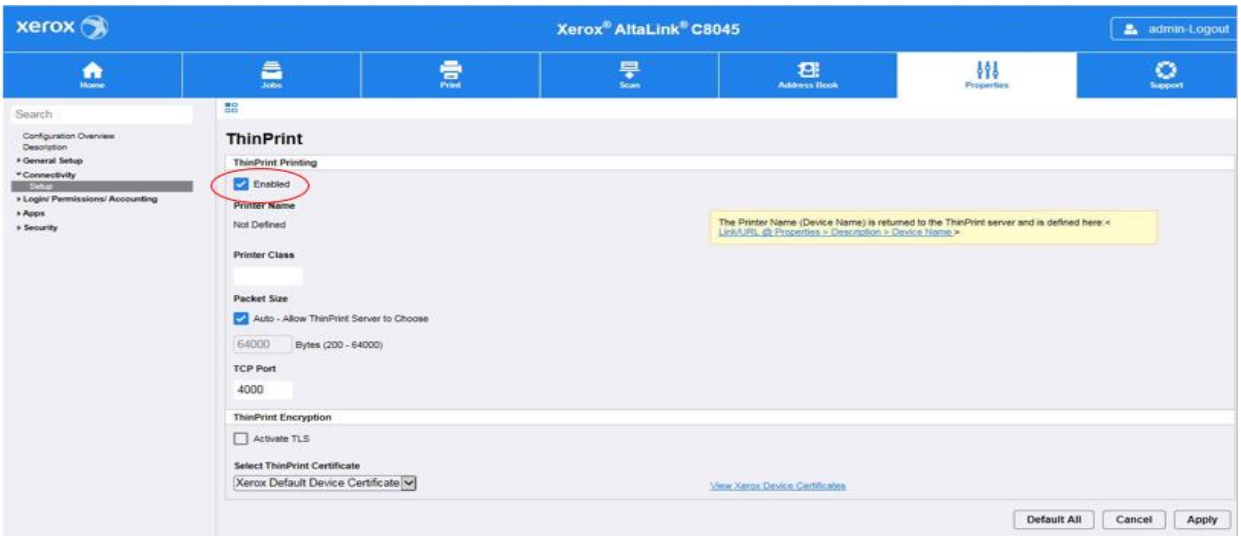
1. ThinPrint Protocol Support

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 ThinPrint data, and print on the Xerox® AltaLink® products.

Note: The ThinPrint Engine/Server output queue and the Xerox® AltaLink® device ThinPrint settings must both be set to TLS encryption for print jobs to be encrypted (see more on next page).

ThinPrint Embedded Web Server

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.

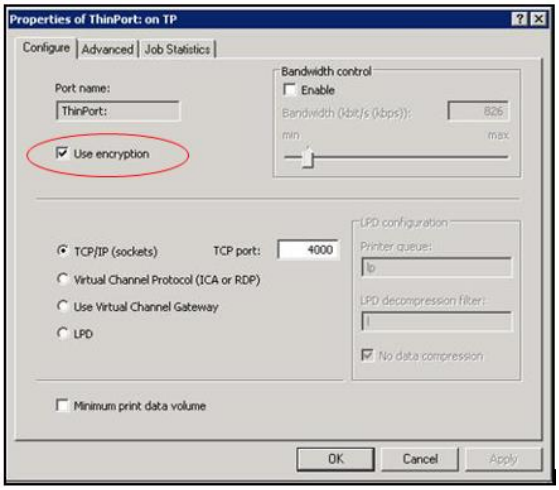


Note: Although a different port number can be configured, it is important not enter a port number that is already in use.

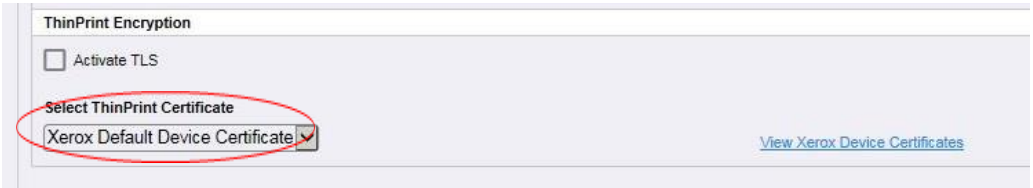
ThinPrint requires a certificate to be loaded on the device when running with TLS encryption. This is located in Properties > Connectivity> ThinPrint Settings.

Note: The ThinPrint Engine/Server output queue and the Xerox® AltaLink® device ThinPrint settings must both be set to TLS encryption for print jobs to be encrypted (see more on next page).

ThinPrint Server Setting for Encryption



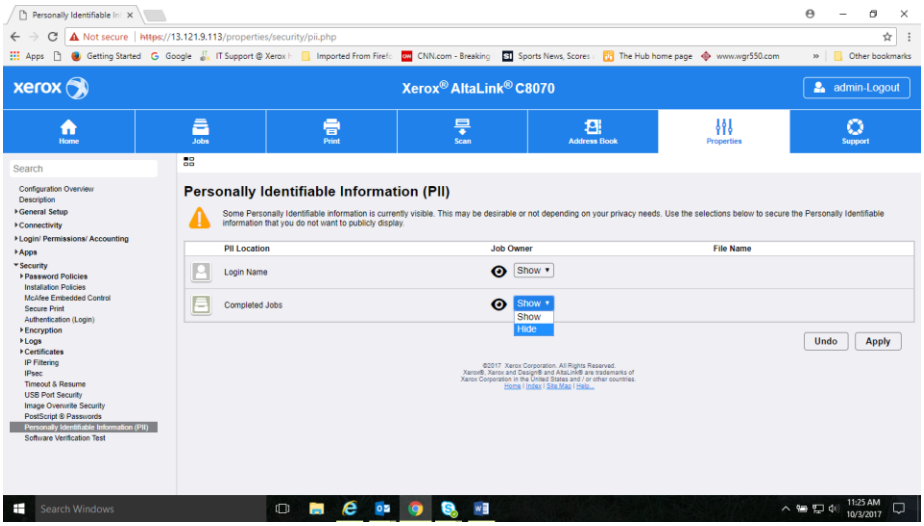
ThinPrint Device Settings (see entire web page above)



Note: Unencrypted print jobs from the server will not be accepted by ThinPrint protocol when TLS encryption is enabled on the print device.

2. Ability to hide username or IDs for Security

Xerox® AltaLink® device Admins will be able hide the Job Owner on the completed Jobs tab of the LUI for security reasons. This can be accomplished by browsing to the following web page on the device Embedded Web Server. Then select “Hide” for Completed Jobs and apply



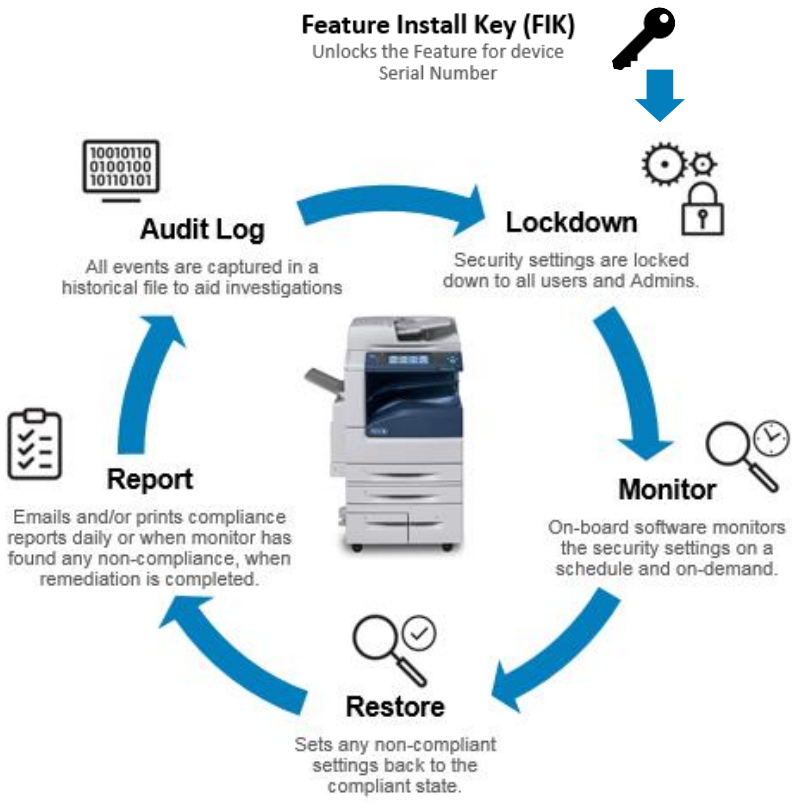
3. Xerox® Lockdown Security Solution / Healthcare Lockdown Solution

The Xerox® Lockdown Security Solution was previously known as Xerox® Healthcare Lockdown Solution, initially introduced with Firmware 100.xxx.107.28600 October 2017.

Note: The Xerox® Lockdown Security Solution kit part number 301K33790 can be ordered by contacting your Xerox® account representative.

Installation of this release enables a device Administrator to install the purchasable Xerox® Lockdown Security Solution on a device. While the Solution content is contained in this release, the feature is hidden until it is activated by purchase of the kit and installation of a Feature Installation Key (FIK).

The Xerox® Lockdown Security Solution permanently enhances certain security aspects of the Xerox® WorkCentre® Devices by encrypting the hard drive, overwriting hard drive data immediately after use, preventing jobs from being stored on or printed from USB devices, recording who has used the device and how they used it and providing additional controls designed to protect specific Xerox® networked and non-networked devices against malicious attacks.



As the name implies, it “Locks down” a set of security settings on the printer, making them unchangeable to anyone including the system administrator and raises the bar on printer security. The security settings that Xerox® Lockdown Security Solution permanently controls:

a) User Data Encryption is enabled which AES encrypts all partitions of the hard drive that may contain customer data.
b) Immediate Job Overwrite is enabled which deletes and overwrites disk sectors that temporarily contained electronic image data conforming to NIST Special Publication 800-88 Rev1.
c) Scheduled Disk Overwrite is enabled on a daily basis at a time that is selectable. This deletes and overwrites every sector of any partitions of the hard drive that may contain customer data.
d) McAfee® Embedded Control is set to Enhanced Security (or McAfee® Integrity Control™ if this option has been purchased) to protect against threats to confidential data by use of whitelisting technology that allows only approved files to run.

e) Audit Log is set to record information about who has used the device and how they have used it, as well as the chronology to help track the events that have occurred.
f) Print from USB is disabled preventing the printing of any files that are stored on a USB Flash Drive from the USB port on the printer control panel.
g) Scan to USB is disabled preventing scanning of a document and storing the scanned file on a USB drive.

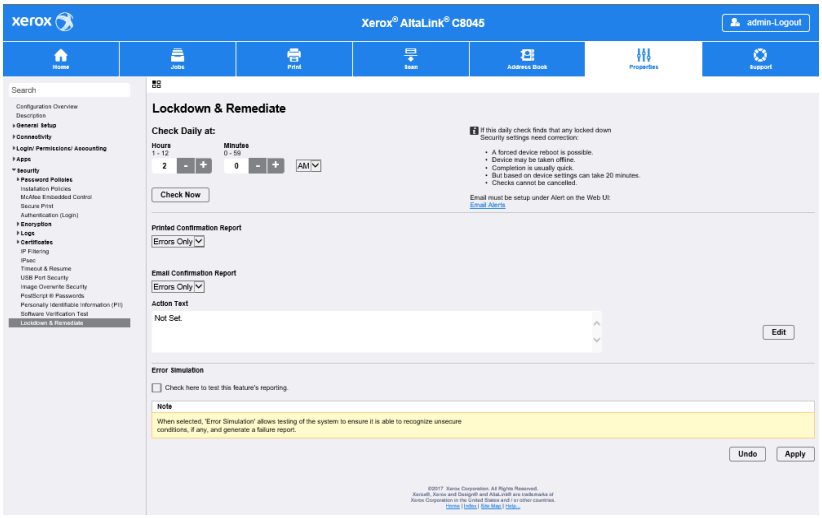
Note: Front USB Port is no longer disabled in this version.

In addition, the solution:

- Monitors these security settings on a daily basis to ensure that they have not been changed maliciously.
- Restores any of these settings automatically back to the compliant state if the Monitor found any to be non-compliant.
- Reports the compliance state of the machine via email and/or printed reports:
    a. At the scheduled time on a daily basis.
    b. When the Monitor function has found any non-compliance.
    c. When Restore has been completed.
    d. When "check now" is selected.
- Records all of these activities in the Printer Audit Log.

Once the Feature Installation Key is installed, a Lockdown control panel is made available and added to the list of Security functions for the MFP via both Embedded Web Server and Local UI.

The Administrator can determine the time of day the Monitor will run, the frequency of printed and emailed confirmation reports, set the action text that appears on the printed confirmation reports that directs the user where to deliver the printed reports and perform Monitor "Check Now" and Error Simulation" to test the operation.



Firmware 100.xxx.077.17900 & (.17010 for B8045/B8090) July 2017

5. Custom Administrator Solution

Custom Administrator Solution provides a new level of device Administrator. The Administrator can create a Custom Administrator role, assign users to the role and select from a list of 21 permissible features that the Custom Admin has permission to modify.

Custom Administrators rights are determined by the Admin. The Custom Admin is allowed to create/manage logged-in user roles, but they cannot create/modify roles with Admin permissions or device management roles. If you are enabling the Healthcare Lockdown Solution then you will want this feature enabled as well.

Note

- Custom Administrators permissions are determined by the Admin.
- Administration of the Custom Admin role can only be performed via the Embedded Web Server.
- A Custom Admin is allowed to create/manage logged-in user roles, but they cannot create/modify roles with Admin permissions or device management roles.
- Creating a Custom Admin role will delete the default "Logged-in user" Role if no other custom roles have been previously created. See section 4 below to re-create the default "Logged-in user" Role

Note: The Custom Admin role Administration can only be performed via the Embedded Web Server.
Note: Creating a Custom Admin role will delete the default "Logged-in user" Role if no other custom roles have been previously created. See section 4 below.

- Create a new Custom Administrator role
- Login to the device Embedded Web Server as Admin
- Select Properties > Login / Permissions / Accounting > User Permissions
- On User Permission Roles row, select **Edit**
- On User Permission Roles page, select **Device Management** tab
- On Device Management tab, select **Add New Role**
  - Type in **Role Name** (e.g. Custom Admin Role) and **Description** (e.g. Some settings are Read Only)
  - Select **Create**
- Assign permissions to the Custom Administrator role
- On Add Management Role page, select Properties tab
- If **Forbid All** is selected, this role will not have rights to change any of these settings.
  - To give users in this role the rights to change a particular setting, set the pulldown in the status column to **Allowed**.
- Assign users to the Custom Administrator role
- On Add Management Role page, select Assign Users to Role tab
- Select Add New User
- On **Add New User** page, define the corporate wide **user** and **password**
  - Type in **User Name** (e.g. HealthAdmin) and **Friendly Name** (e.g. HealthAdmin)
  - Type in **New Password** and **Retype password** (e.g.1234 or other unique password)
  - Select **Save**
- On Add Management Role page, Assign Users to Role tab
- Select the **check box** in front of the new user (e.g. HealthAdmin)
- Select **Apply**
- Creating a logged-in user role (optional)
- Login to the machine as Admin or Custom Admin
- Select Properties > Login > Permissions > Accounting > User Permissions
- On User Permission Roles row, select Edit
- On User Permission Roles page, select Logged-in Users tab
- On Device Management tab, select Add New Role
  - Type in **Role Name** – "Logged-in user" and **Description** – "Allow logged-in users unrestricted access to all features except Tools"
  -

2. Cloning Webservice

Xerox® AltaLink® devices will accept clone files from Centreware Web via a Cloning WebService with a Network User ID and password. This CWW functionality will be released in the next CWW release slated for summer 2017.

Centreware Web will deliver compatible software for this Xerox® AltaLink® solution that will Import, export and manage clone files. CWW and Xerox® AltaLink® devices will authenticate Network Users and verify User is in appropriate Active Directory Group for device administration. CWW will schedule and push clone files to individual and multiple Xerox devices with the user's Network User ID and clone file description.

3. EIP Authentication

For EIP web service calls requiring administrator credentials, the Xerox® AltaLink® devices will now add the ability to authenticate the credentials against the Device Configuration for Network Authentication and for the Device Administrator privileges. The authentication could be network (LDAP, Kerberos or SMB), or the device user database, or 'admin'.

4. Disable Print Submission of Clone Files

Xerox® AltaLink® devices will be able to disable the delivery of Clone files through the Print Submission path. This setting is located on the Embedded Web Server under Properties> Security> Installation Policies

5. Disable SNMP Sets

The Xerox® AltaLink® devices will also allow System Admins the ability to disable SNMP Sets (Writes) while still allowing SNMP Gets (Reads) on the device. This setting is located on the Embedded Web Server under Properties> Connectivity > Setup> SNMP.

6. XML Configuration Report

Xerox® AltaLink® device Admins will be able to download the Configuration Report in XML format. This capability is on the Embedded Web Server, under Properties> General Setup> Configuration Report.

7. Support Log Tab

The previous Network Log functionality on the Embedded Web Services will now be called Support Logs. Support Logs are located under the Embedded Web Services under the Support tab> Troubleshooting> Support Logs and can be found under the Properties tab> Security> Logs> Support Logs.

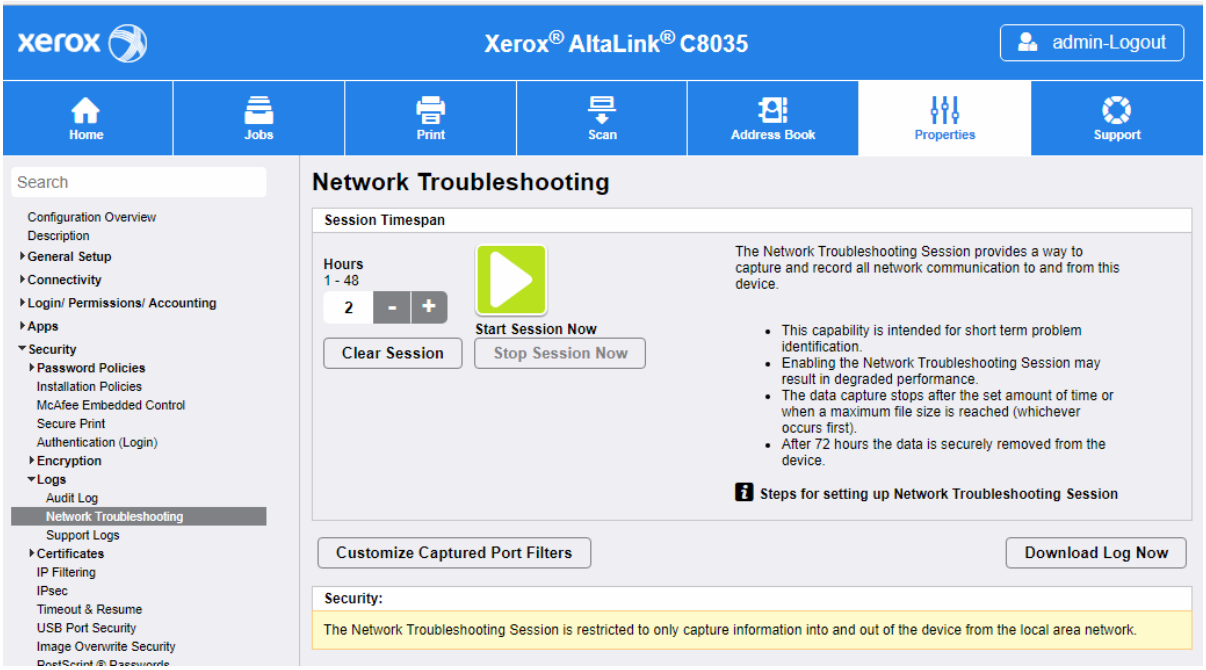
8. Network Troubleshooting Log Feature

This new feature allows a device administrator to capture network communications directed to the device. This feature is disabled by default, and only captures communications between the device and another network node. It does not capture broadcast information or communications between other devices. Additionally, it can be limited to specific protocols. Note this data may contain authentication credentials or other sensitive information. The feature enables administrators to analyze network traffic which can help diagnose communications problems.

The Capability can be accessed through the Properties> Security> Logs> Network Troubleshooting OR under Support> Troubleshooting> Network Troubleshooting tabs as shown below.
Note: File size of the Network Trace capture is limited to 10 MB.

Settings:

1. Settings shown above include setting the number of hours of capturing the trace from 1 to 48 hours.
2. Start Session Now begins the process of capturing network packet data.
3. Clear Session can be selected to clear the trace data and start a trace over.
4. Stop Session can be selected to stop a trace at a point in time but save the existing trace data.
5. Download Log Now can be selected to download the existing log file.
6. Maximum packet size can be customized, default is 1514 bytes
7. Customize Captured Port Filters can be selected to limit the trace selection to select Protocol, Ports or limit to a specific Destination IP Address as shown below.
8. Be sure to select Save before beginning data capture.
9. Encrypted communications will not be decrypted in the log.
10. Downloaded file has .pcap extension,
11. Default All can be selected to return the Customize Capture Port Filters to their Default values.



Each Protocol can be edited to customize protocol name or select a specific port.
Additional custom protocols can be added.