Xerox® AltaLink®
Product Enhancement Read Me

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

Release Date: January 26, 2018

Contents

Latest release information:

Product Model	System Software	Network Controller
Xerox® AltaLink® C8070	100.003.018.01610	100.003.01610
Xerox® AltaLink® C8045/55	100.002.018.01610	100.002.01610
Xerox® AltaLink® C8030/35	100.001.018.01610	100.001.01610
Xerox® AltaLink® B8045/B8090	100.008.018.01610	100.008.01610

Firmware 100.003.018.01610 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.

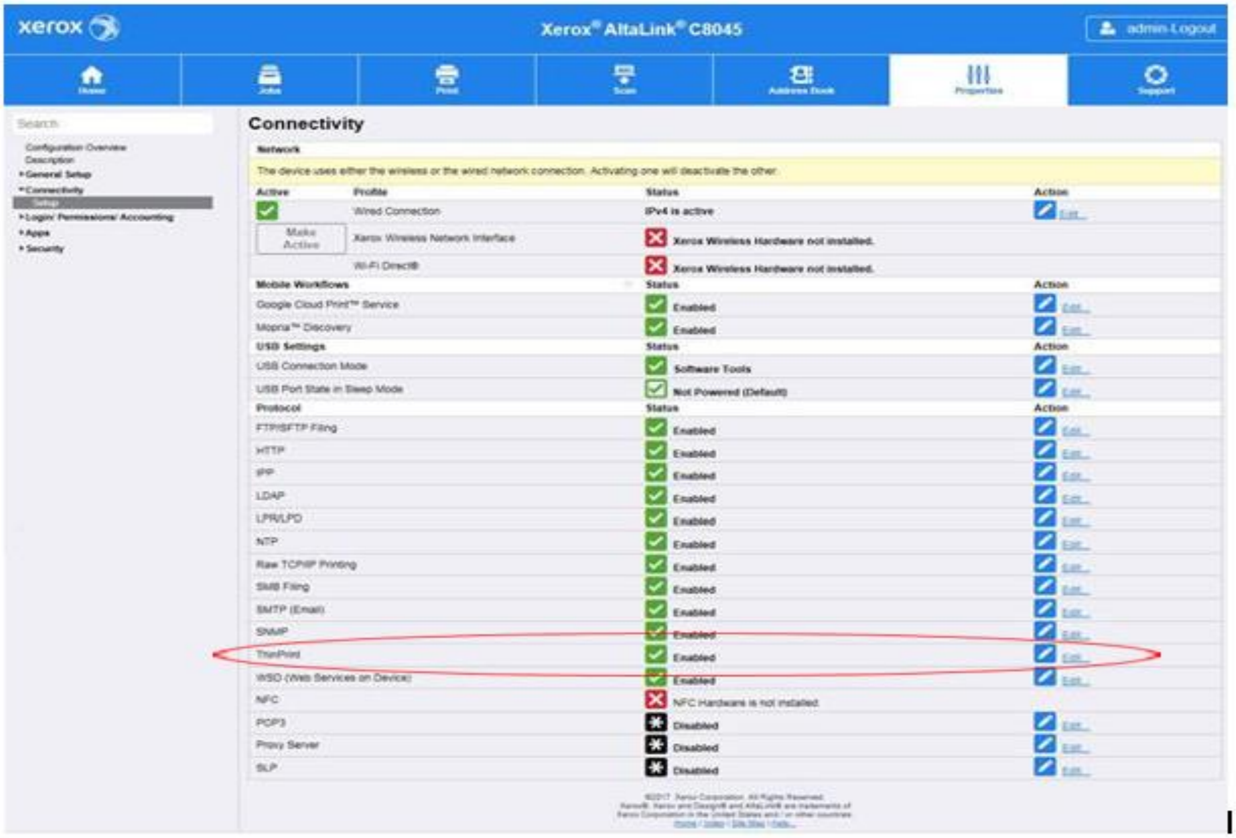
Firmware 100.xxx.107.28600 October 2017

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



Connectivity

Network

The device uses either the wireless or the wired network connection. Activating one will deactivate the other.

Active	Profile	Status	Action
✓	Wired Connection	IPv4 is active	Edit...
Make Active	Xerox Wireless Network Interface	☒ Xerox Wireless Hardware not installed.	
	Wi-Fi Direct®	☒ Xerox Wireless Hardware not installed.	

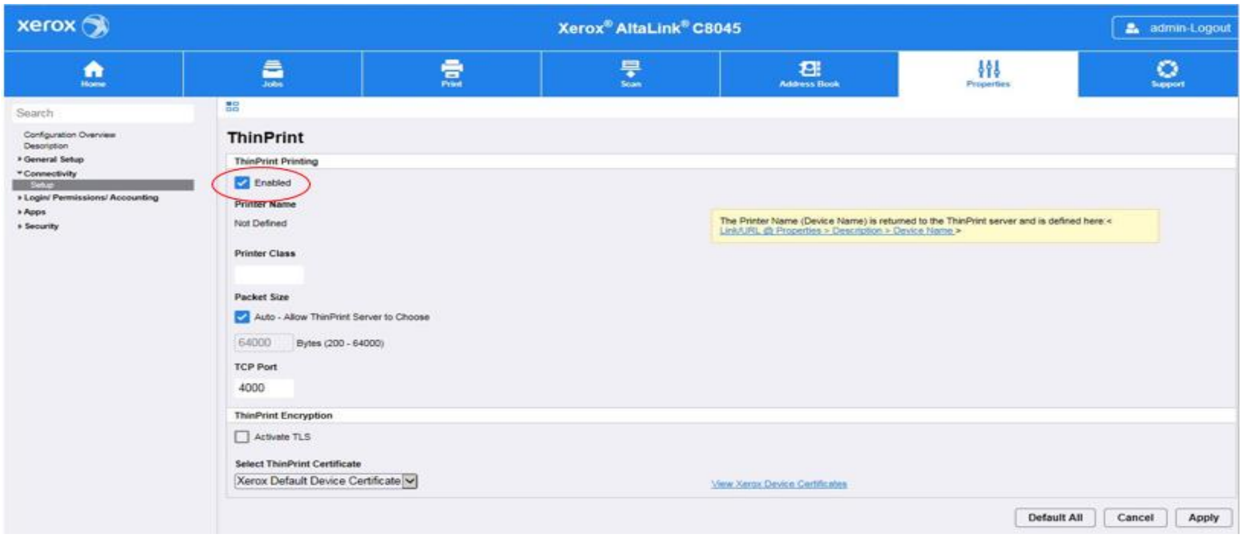
Mobile Workflows	Status	Action
Google Cloud Print™ Service	✓ Enabled	Edit...
Mopria™ Discovery	✓ Enabled	Edit...

USB Settings	Status	Action
USB Connection Mode	✓ Software Tools	Edit...
USB Port State in Sleep Mode	✓ Not Powered (Default)	Edit...

Protocol	Status	Action
FTP/SFTP Filing	✓ Enabled	Edit...
HTTP	✓ Enabled	Edit...
IPP	✓ Enabled	Edit...
LDAP	✓ Enabled	Edit...
LPR/LPD	✓ Enabled	Edit...
NTP	✓ Enabled	Edit...
Raw TCP/IP Printing	✓ Enabled	Edit...
SMB Filing	✓ Enabled	Edit...
SMTP (Email)	✓ Enabled	Edit...
SNMP	✓ Enabled	Edit...
ThinPrint	✓ Enabled	Edit...
WSD (Web Services on Device)	✓ Enabled	Edit...
NFC	☒ NFC Hardware is not installed	
POP3	✱ Disabled	Edit...
Proxy Server	✱ Disabled	Edit...
SLP	✱ Disabled	Edit...

©2017 Xerox Corporation. All Rights Reserved.
Xerox®, Xerox and Design® and AltaLink® are trademarks of
Xerox Corporation in the United States and / or other countries
Home | Index | Site Map | Help...

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.



ThinPrint

ThinPrint Printing

☑ Enabled

Printer Name

Not Defined

The Printer Name (Device Name) is returned to the ThinPrint server and is defined here:< Link/URL @ Properties > Description > Device Name >

Printer Class

Packet Size

☑ Auto - Allow ThinPrint Server to Choose

64000 Bytes (200 - 64000)

TCP Port

4000

ThinPrint Encryption

☐ Activate TLS

Select ThinPrint Certificate

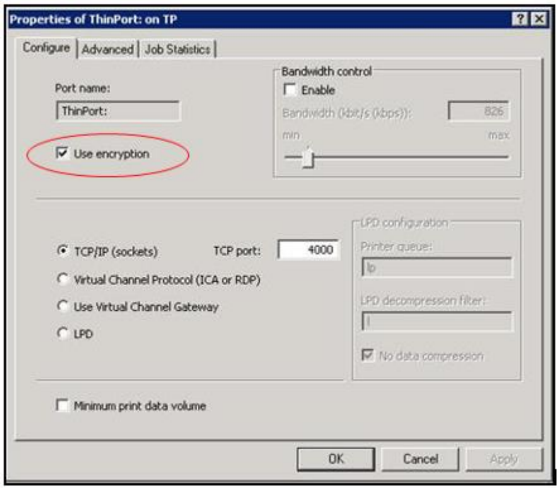
Xerox Default Device Certificate

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



Port name: ThinPort:

☑ Use encryption

Bandwidth control

☐ Enable

Bandwidth (kbit/s (kbps)): 826

min max

● TCP/IP (sockets) TCP port: 4000

○ Virtual Channel Protocol (ICA or RDP)

○ Use Virtual Channel Gateway

○ LPD

LPD configuration

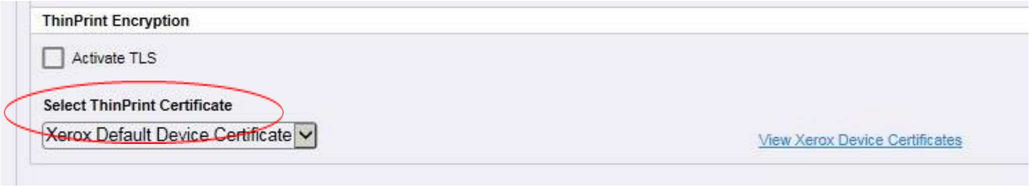
Printer queue: lp

LPD decompression filter:

☑ No data compression

☐ Minimum print data volume

ThinPrint Device Settings (see entire web page above)


ThinPrint Encryption

☐ Activate TLS

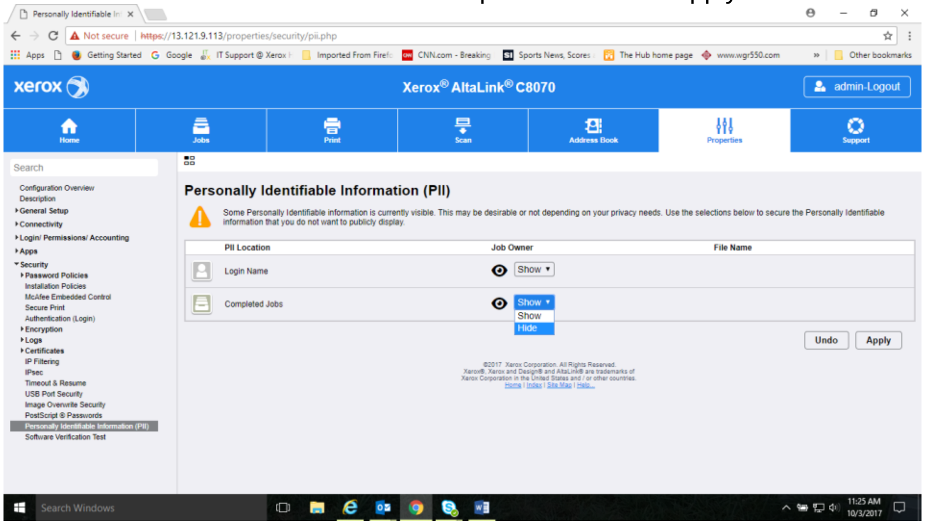
Select ThinPrint Certificate

Xerox Default Device Certificate

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



Personally Identifiable Information (PII)

Some Personally Identifiable information is currently visible. This may be desirable or not depending on your privacy needs. Use the selections below to secure the Personally Identifiable information that you do not want to publicly display.

PII Location	Job Owner	File Name
Login Name	Show ▾	
Completed Jobs	Show ▾ Show Hide	

Undo Apply

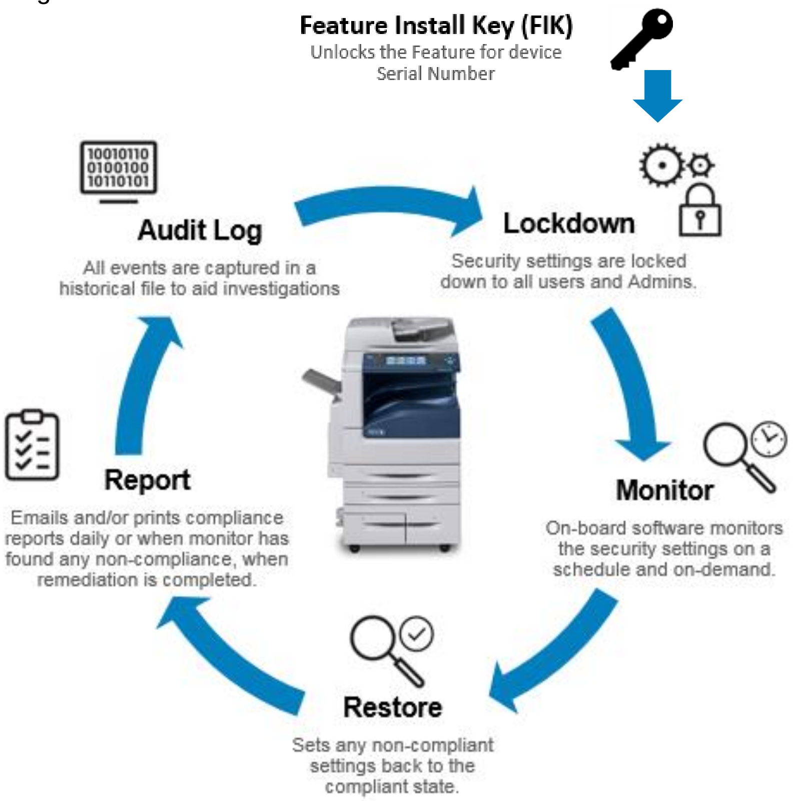
©2017 Xerox Corporation. All Rights Reserved.
Xerox®, Xerox and Design® and AltaLink® are trademarks of Xerox Corporation in the United States and / or other countries.
Home | Index | Site Map | Help...

3. Xerox® Healthcare Lockdown Solution

Note: The Xerox® Healthcare Lockdown 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® Healthcare Lockdown 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® Healthcare Lockdown 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.



Feature Install Key (FIK)
Unlocks the Feature for device Serial Number
10010110
0100100
10110101
Audit Log
All events are captured in a historical file to aid investigations
Lockdown
Security settings are locked down to all users and Admins.
Report
Emails and/or prints compliance reports daily or when monitor has found any non-compliance, when remediation is completed.
Monitor
On-board software monitors the security settings on a schedule and on-demand.
Restore
Sets any non-compliant settings back to the compliant state.

As the name imp ıem unchangeable to
anyone including ıecurity settings that
Xerox® Healthca

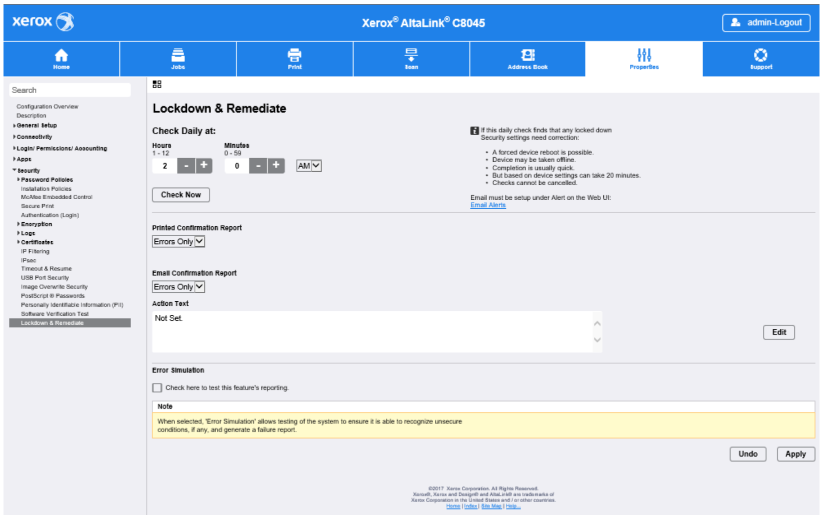
- User Data Eı e that may contain
customer da
- Immediate J at temporarily
contained el ev1.
- Scheduled D This deletes and
overwrites e ımer data.
- McAfee® Em ıtrol™ if this option has
been purcha ting technology that
allows only approved files to run.

- 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.
- 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.
- 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:
- At the scheduled time on a daily basis.
- When the Monitor function has found any non-compliance.
- When Restore has been completed.
- 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.



Lockdown & Remediate

Check Daily at:

Hours 1 - 12: 2

Minutes 0 - 59: 0

AM

If this daily check finds that any locked down Security settings need correction:

- A forced device reboot is possible.
- Device may be taken offline.
- Completion is usually quick.
- But based on device settings can take 20 minutes.
- Checks cannot be cancelled.

Email must be setup under Alert on the Web UI:
Email Alerts

Printed Confirmation Report: Errors Only

Email Confirmation Report: Errors Only

Action Text: Not Set.

Error Simulation

□ Check here to test this feature's reporting.

Note

When selected, 'Error Simulation' allows testing of the system to ensure it is able to recognize unsecure conditions, if any, and generate a failure report.

©2017 Xerox Corporation. All Rights Reserved.
Xerox®, Xerox and Design® and AltaLink® are trademarks of Xerox Corporation in the United States and / or other countries.

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

1. 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. Network Troubleshooting

Xerox® AltaLink® devices will deliver a means for Network Troubleshooting by capturing and allowing download of a network trace (tcdump) file. The Network Troubleshooting Session shall only be configurable by a Systems Administrator or a user with System Administrator privileges. This Feature can be accessed through the Embedded Web Services by selecting the Properties tab> Security> Logs> Network Troubleshooting or by selecting the Support Tab>Troubleshooting> Network Troubleshooting Log.

6. 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> Connectivit> Setup> SNMP.

7. 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.

8. 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.

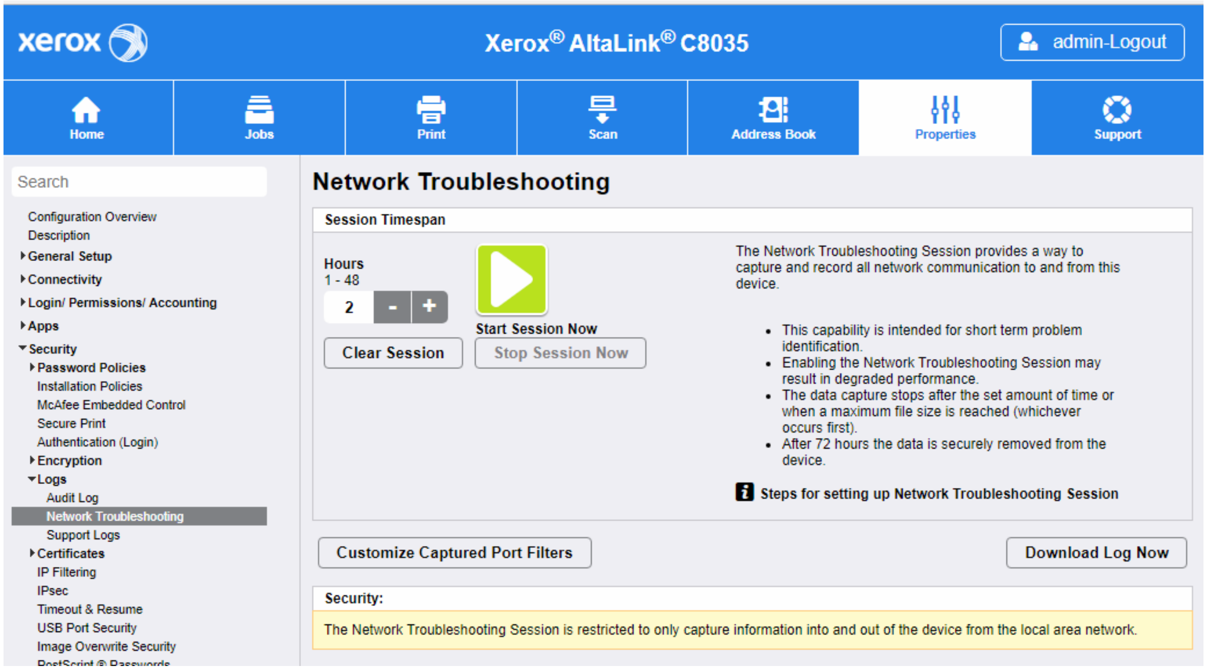
9. Network Troubleshooting Log Feature

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.



Network Troubleshooting

Session Timespan

Hours
1 - 48

2 - +

Start Session Now

Clear Session | Stop Session Now

The Network Troubleshooting Session provides a way to capture and record all network communication to and from this device.

- This capability is intended for short term problem identification.
- Enabling the Network Troubleshooting Session may result in degraded performance.
- The data capture stops after the set amount of time or when a maximum file size is reached (whichever occurs first).
- After 72 hours the data is securely removed from the device.

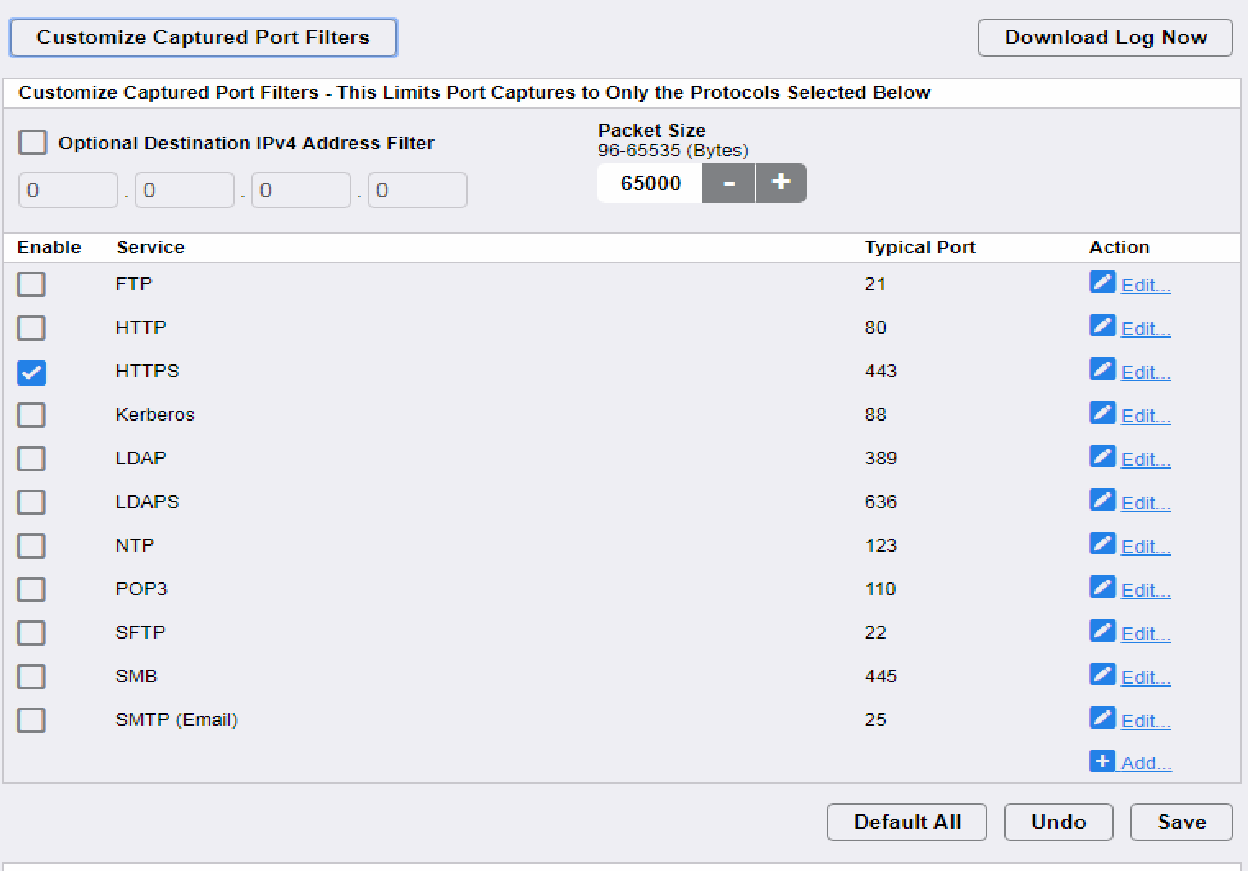
Steps for setting up Network Troubleshooting Session

Customize Captured Port Filters | Download Log Now

Security:

The Network Troubleshooting Session is restricted to only capture information into and out of the device from the local area network.

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


Customize Captured Port Filters | Download Log Now

Customize Captured Port Filters - This Limits Port Captures to Only the Protocols Selected Below

□ Optional Destination IPv4 Address Filter

0 . 0 . 0 . 0

Packet Size
96-65535 (Bytes)

65000 - +

Enable	Service	Typical Port	Action
□	FTP	21	Edit...
□	HTTP	80	Edit...
☑	HTTPS	443	Edit...
□	Kerberos	88	Edit...
□	LDAP	389	Edit...
□	LDAPS	636	Edit...
□	NTP	123	Edit...
□	POP3	110	Edit...
□	SFTP	22	Edit...
□	SMB	445	Edit...
□	SMTP (Email)	25	Edit...
			Add...

Default All | Undo | Save

©

Document Version: 1.0 (January 2017).