D5.6 Xerox® AltaLink® Product Enhancement Document for Version 114.xxx.011.28800

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

Release Date: November 10, 2021 dc21rn4061

Product Model	System Software	Network Controller
AltaLink C8170	114.011.011.28800	114.011.28800
AltaLink C8145/55	114.010.011.28800	114.010.28800
AltaLink C8130/35	114.009.011.28800	114.009.28800
AltaLink B8145/B8155	114.013.011.28800	114.013.28800
Altalink B8170	114.014.011.28800	114.014.28800

Contents

Latest release information:

Firmware 114.xxx.011.28800 (R21-10) November 2021

1. Various Security Improvements

- SECURITY: Addresses CVE-2020-25710

2. Various Bug Fixes

- Custom blocking screen text can now be configured when configured for Xerox Workplace Cloud.
- Resolved issue with “Only Send to Self” when device is installed in a multi-domain network.

Firmware 114.xxx.001.27300 (D5.6) November 2021

3. Various Security Improvements

- Audit Log improvements
- CVE-2020-24588 CVE-2020-24587

4. Various Bug Fixes

- Fax card reliability improvements
- Mixed sized printing output improvements.
- Fix for WSD print queues losing connection after printer upgrade
- Advancements in Adaptive Learning
- Improvements to Editable 1-Touch apps
- Improvements to Imaging Security
- Improvements to Multi-Feed Detection for Copy/Scan

Firmware 113.xxx.021.20610 (R21-07) August 2021

1. SMTP password length increase to 256 characters

Introduces ability to support SMTP password length longer than 60 Characters for Outgoing SMTP Authentication. SMTP password length max supported is 256 characters.

Many mail server applications now begin enforcing MFA on all User accounts and starting to use API key (essentially a 69 Character password) for SMTP Authentication.

2. Enhanced Preview Capabilities

Introduces new preview capabilities to the native preview feature for Scan To and Scan to Email. Preview now supports the ability to delete images, re-order images and to change scan settings between scan segments.

The Scan API has been updated to allow EIP apps to take advantage of the native preview feature.

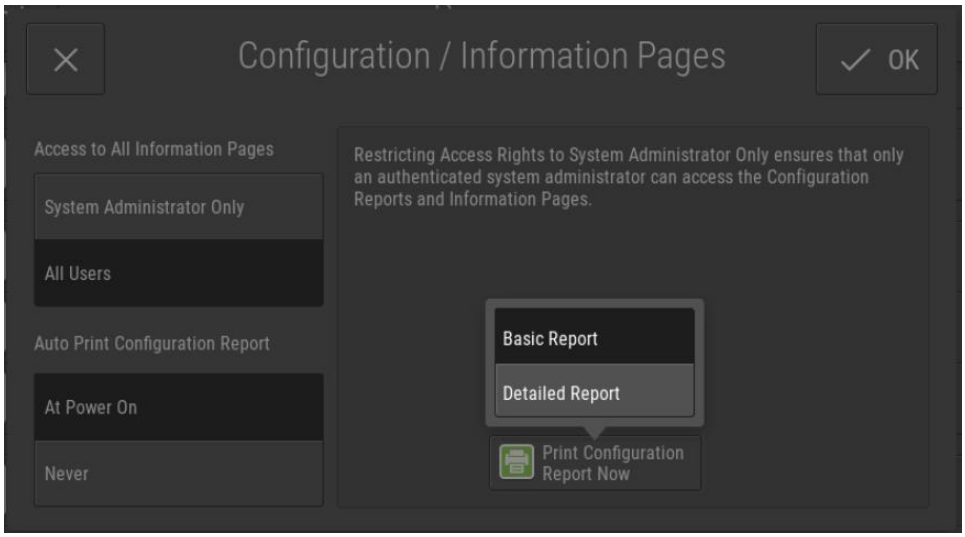
3. Addition of DHCP IPv6 Unique Identifier (DUID) to Configuration Sheet

The DHCP IPv6 Unique Identifier (DUID) in Link Layer format will be displayed on the printed configuration sheet when IPv6 is enabled. The DUID information is labeled “DUID (DHCP Unique Identifier” under the Protocols heading. Additionally, the DUID identifier can be obtained from the EWS Configuration Report when IPv6 is enabled.

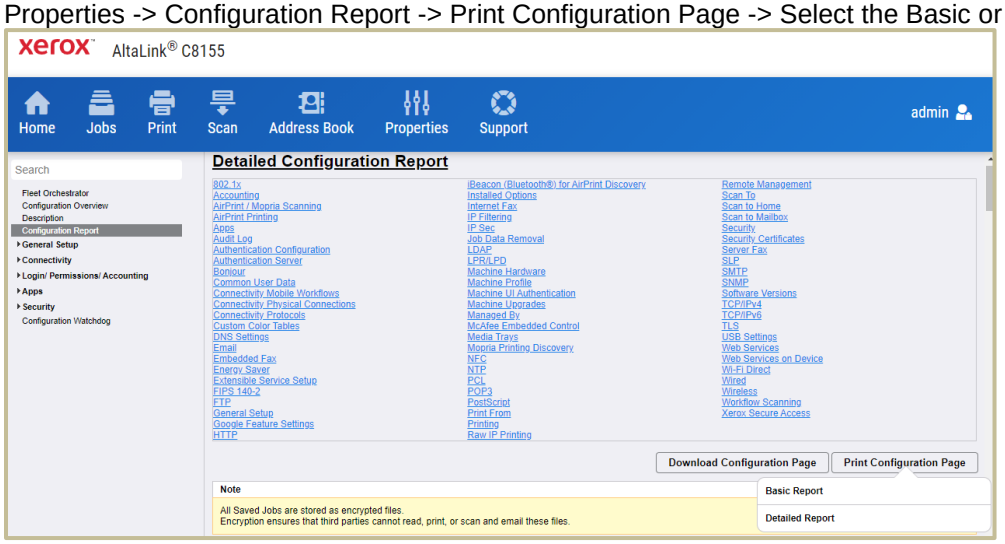
4. Detailed Configuration Report

Introduces new Configuration Report options of Basic and Detailed. Both versions of the report can be printed by the Admin or guest user if access is configured. The Configuration Reports are accessible through the EWS and Local UI.

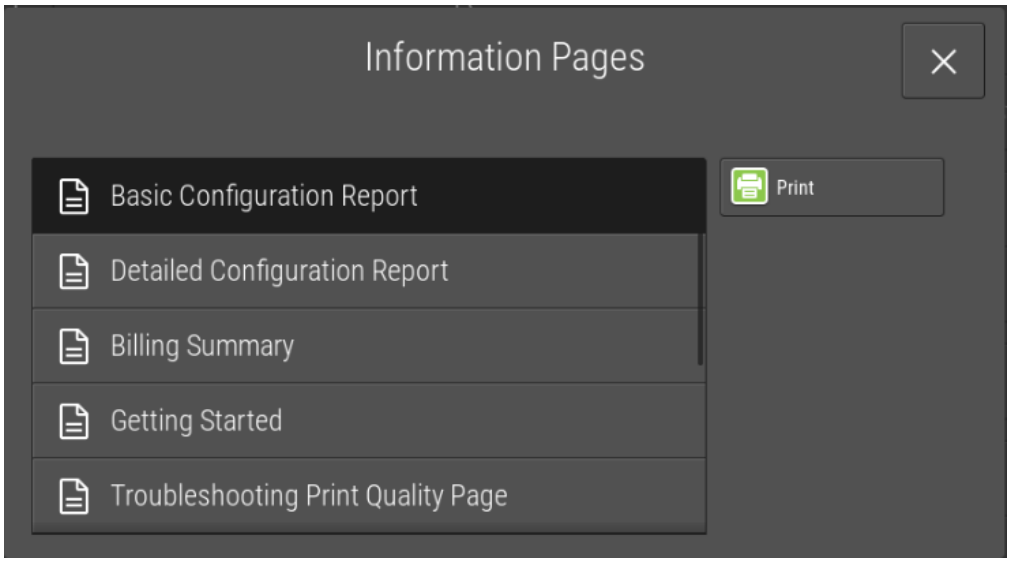
From the LUI, the Admin can configure the device to control access to the Basic and Detailed configuration reports. (Device App -> Tools -> Configuration / Information Pages). Printing of the reports is also available by selecting “Print Configuration Report Now” & selecting the Basic or Detailed Report.



Printing of the configuration reports from EWS:
Properties -> Configuration Report -> Print Configuration Page -> Select the Basic or Detailed Report



Printing of the configuration reports from the LUI:
Select Device App -> Information Pages -> Select Basic or Detailed Configuration Report -> Print



5. Various Bug Fixes

- Security Audit log fixes
- Security Fixes to TLS settings
- Security Multiple certificate fixes
- Security CVE-2016-2183
- Added capability to push IIT logs

Firmware 113.xxx.011.17810 (R21-04) July 2021

1. Customize the Supported Smart Cards List

Enables the Xerox Analyst, Solution Architect or Service Engineer to customize the supported smart card list on the device to add a new smart card for use in environments where more than one smart card type is in use.

The following information are necessary to enable a new smart card:

- Smart card ATR (eg: 3B 7F 96 00 00 80 31 80 65 B0 84 56 51 10 12 0F FE 82 90 00)
- Smart card Manufacturer / Series / Model / Applet (eg: Gemalto IDPrime MD 830b v4.3.5 Applet)

Once the customized supported smart card list has been created, it is uploaded to the device via the Web UI and validation tested to ensure that all smart card related functions work properly.

The customized supported smart card list can then be deployed to other similar devices by either cloning, Fleet orchestrator or XDM deployment of the clone file.

2. Support for Single Sign-On for One Drive and O365 App Gallery App

This feature enables single sign-on for access to Office 365 or One Drive cloud solutions when using Kerberos authentication at the MFP. Kerberos authentication can be performed using either smartcard or network authentication. This feature is to be used with App Gallery SSO apps for Office 365 and One Drive.

The feature is enabled and configured on the device Web UI.

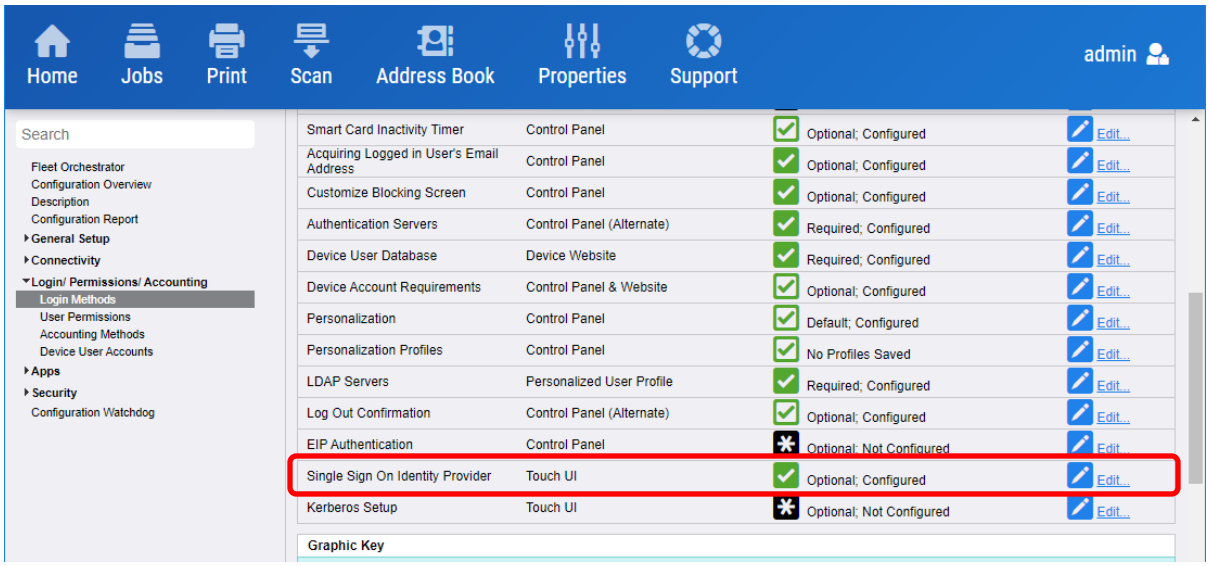
- Under the settings for Smartcard or Network Authentication select Edit for Single Sign-On Identity Provider (see pictures below).
- Check the Enable Box
- Enter of the url for the ADFS server windowstransport endpoint
- Enter the SAML Token Access Code. The SAML Access Token Code can be any string, 14 – 64 characters that the admin wants to use. Note that SAML Token Access Code entry must match the entry made at App Gallery when configuring and downloading the App Gallery SSO apps.
- Select Save. Note that if you go back into the setup and change any setting you will need to re-enter the SAML Access Token Code
- Under the settings for Smartcard or Network Authentication validate that under Kerberos settings, the “Use DNS Canonicalize Hostname” is disabled.

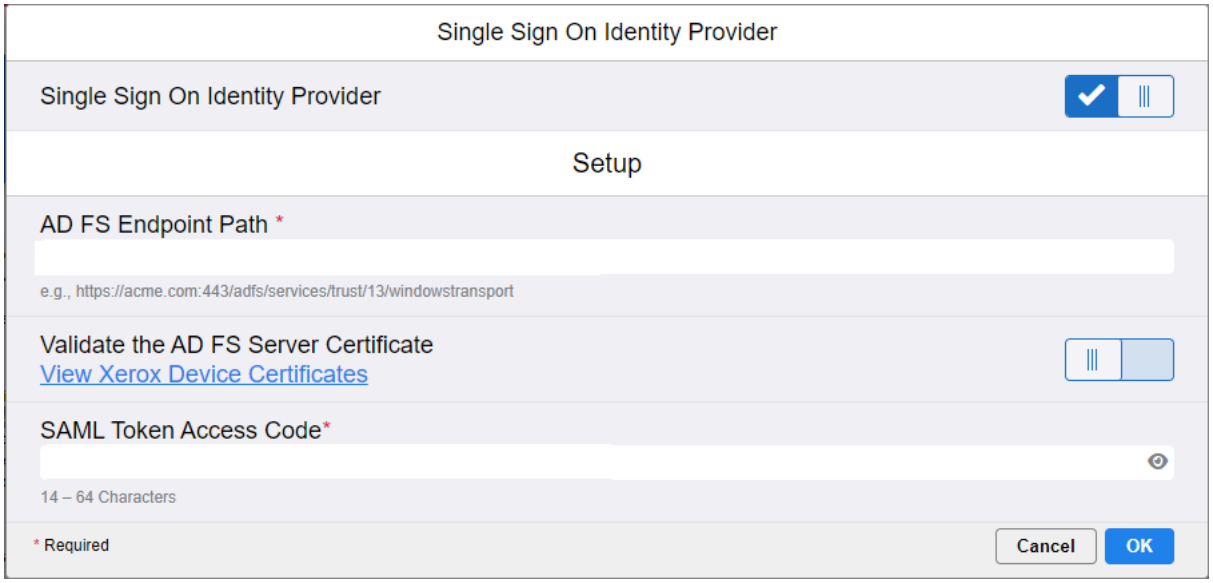
This feature requires that the Job Management setting for “Allow Open Access to Job Information” be enabled.

- This setting can be found on CWIS>Properties>Connectivity>HTTP>WebServices.

To configure the SSO App Gallery app,

- Open App Gallery and Log on
- Scroll down to Cloud Apps and select the One Drive or 365 App
- By the App icon on the left side select “Configurable”
- Enter the “Tenant ID” (this is provided by Microsoft)
- Enter the “Advanced Custom Configuration (uncommon)”. The “Advances Custom Configuration (uncommon)” entry needs to be the same entry as the entry on the MFP for the “SAML Access Token Code”.





3. Various Bug Fixes

- Since device auto upgraded to .06011, getting error on device of "XSA login failure. The server does not trust the Xerox MFP security Certificate"
- Unable to send email using smtp-relay.gmail.com utilizing TLS

4. Security Fixes

- Audit log improvements
- CVE-2020-29370

Firmware 113.xxx.001.06011(General) March 2021

1. Configure smart card type to allow any ATR of that type.

When the device Login Method is configured for Control Panel Login using Smart Card, this SFR adds the ability to set the smart card type and allow any ATR for that card type. The selections are:
• Supported Smart Cards List
• CAC & PIV Cards
• IDPrime MD cards
• SafeNet SC cards

2. Support for the following Modernized CAC smart cards

IDEMIA Cosmo V8.0 (formerly Oberthur card system) with V2.7.4 Applets T=0/T=CL communication protocol. ATR: 3B D8 18 00 80 1F 07 80 31 C1 64 08 06 92 0F DF
Gemalto IDCore 3020 v2.1 (formerly Gemalto TOP DL GX V2.1) 144K with V2.7.4 Applets. ATR: 3B 7D 96 00 00 80 31 80 65 B0 75 49 17 0F 83 00 90 00
Support for the following SIPRNet cards:
Safenet SC650 v4.0 card: ATR: 3b ff 14 00 ff 81 31 fe 45 80 25 a0 00 00 00 56 57 53 43 36 35 30 04 00 3c
Safenet SC650 v3.3c card: ATR: 3b ff 14 00 ff 81 31 fe 45 80 25 a0 00 00 00 56 57 53 43 36 35 30 03 03 38.

3. EIP

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.
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.

4. Security Fixes

- Bug Fix to TLS settings
- Bug Fix to IPsec
- Authenticated OS command injection (RCE)
- CVE-2020-25641- A flaw was found in the Linux kernel's implementation of biovecs in versions before 5.9-rc7. A zero-length biovec request issued by the block subsystem could cause the kernel to enter an infinite loop, causing a denial of service. This flaw allows a local attacker with basic privileges to issue requests to a block device, resulting in a denial of service.
- Flexon fix to add overwrite to SSD
- Pages vulnerable to XSS attack
- Removed ability for user to delete default actions in CWIS
- CVE-2019-20795 - iproute2 before 5.1.0 has a use-after-free in get_netnsid_from_name in ip/ipnetns.c.

Document Version: 1.0 (January 2020).