Xerox® ConnectKey® WorkCentre® Product Enhancement Read Me

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

Release Date: November 5, 2021   **dc21rn4059**

Xerox® WorkCentre® Product Models Supported as listed below:

Product Model	System Software	Network Controller
WC 3655/3655i	075.060.031.27310	075.061.27310
WC 5845/55/75/90i	075.190.031.27310	075.191.27310
WC 5945/55i	075.091.031.27310	075.091.27310
WC 6655/6655i	075.110.031.27310	075.111.27310
WC 7220/7225i	075.030.031.27310	075.031.27310
WC 7830/7835i	075.010.031.27310	075.011.27310
WC 7845/7855i	075.040.031.27310	075.041.27310
WC 7845/7855 IGB	075.080.031.27310	075.081.27310
WC 7970/7970i	075.200.031.27310	075.201.27310
WC EC7836	075.050.031.27310	075.051.27310
WC EC7856	075.020.031.27310	075.021.27310

Link to Upgrade Tool
Upgrade Tool ckupgrade-092120210147

Contents

Firmware 075.xxx.031.27310 (R21-10) November 2021

Firmware 075.xxx.021.19300 (R21-07) August 2021

1. Various Bug fixes

The issue with PCL files ends up incorrectly printed; object displacement has been fixed.

Firmware 075.xxx.011.11100 (R21-04) May 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 or XDM deployment of the clone file.

Firmware 075.xxx.001.01210 February 2021

1. 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 for URL 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

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".

2. Security Fixes

- Removes the ability of remote attackers to cause a denial of service via vectors involving a TCP packet
- Security: Pages vulnerable to XSS attack

Firmware 075.xxx.030.30710 Nov 2020

1. Configure Smart Card Type

Enable ability to set a single smart card type when the device Login Method is configured for Control Panel Login using Smart Card. The selections are:

- **All Supported Smart Cards**: This is current device behavior used in environments where users have multiple different smart card types.

- **CAC & PIV Cards**: For use in environments where all users have CAC or PIV cards.

- **IDPrime MD cards**: For use in environments where all users have IDPrime MD cards.

- **SafeNet SC cards**: For use in environments where all users have SafeNet SC cards.
  Note: This selection is only available when the Safenet SHAC FIK key has been installed and FIPS has been disabled

2. Various Bug Fixes.

- A timing issue was fixed that could cause some devices to get into a continuous reboot.
- An issue was fixed for the WC 3655 & WC 6655 that resulted in the toner install date to read incorrectly.

Firmware 075.xxx.020.20500 Aug 2020

1. Support for Gemalto DL 128K v2 SCP03 PIV card

Add support for the following smart card in this release:
Gemalto DL 128K v2 SCP03 PIV smart card, ATR: 3B 7F 96 00 00 80 31 80 65 B0 84 23 27 E5 12 0F FE 82 90 00

2. EIP SNMP Web Service Improvement

Enabling only SNMP v3 on the device no longer impacts the use of the EIP SNMP Web Service

Caveat: When using the EIP SNMP Client to write data, the SNMP v1/2 SNMP Set Community Strings must be the same on the printer and within the EIP SNMP Client otherwise an SNMP Timeout error will occur*.*

Firmware 075.xxx.010.12010 May 2020

1. Blackboard Card Reader PS4101

Blackboard Card Reader PS4101 USB Smartcard Reader is supported in this release.

2. Support for Modernized CAC and SIPRNet cards.

Following Modernized CAC cards supporting existing capabilities with reduced/realigned certificates are supported in this release,

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

The following SIPRNet cards are supported in this release:

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.   Various Bug Fixes

- Dropbox button is no longer grayed out when user adds userid and password in Connect 2.0 for Dropbox. **Caveat:** "In addition to this new software release, there is a ConnectKey 2.0 for Dropbox app-side fix that is required as well. There is no ETA as to when this app will be back in the Xerox App Gallery. Please check the Xerox App Gallery periodically to see if this app reappears for download."

- The issue with "Delete All print jobs at Power On" has been corrected.

Firmware 075.xxx.000.02300 February 2020

1. Various Bug Fixes.

- When using SmartCard authentication, the device no longer displays prompt 1 when using on-box accounting back.
- A problem with copy authentication after reboot has been fixed.
- Various security updates.

Firmware 073.xxx.069.32410 December 2019

1. Remote Card Reader Update.

This release enables the ability to remotely perform firmware updates for certain card readers. Card readers currently supported are Elatec TWN4 proximity card reader. The device also displays the card reader firmware version and the date it was last updated. Contact your card reader manufacturer or your analyst that supports your device.

2. Additional Smart Cards Supported

Giesecke & Devrient SmartCafe Expert v7.0 144K DI smart card with CAC 2.7.6 Applet (STOPGAP)

Giesecke & Devrient Sm@rtCafe Expert v7.0 144K DI smart card with PIV Applet is now supported.

IDEMIA Cosmo v8 (NEATS) smart card (NEATS) Smartcard Support

SHAC support for SafeNet SC650 v4.1 (3v) Smartcard. The SHAC middleware support is provided for SafeNet SC650 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 01 3d with the following requirements:
- Email signing and encryption are not supported
- FIPS must be disabled
- Feature Installation Key must be installed:
  - o   Install Key: 227334773923
  - o   Uninstall Key: 227434773923
- A Cherry TC-1100 Card Reader must be connected. (This is the recommended Reader)

3. Cherry ST-1100 Card Reader

The Cherry ST-1100 contact smart card reader is now supported.

Firmware 073.xxx.059.25300 September 2019

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

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

2. ## Gemalto MD cards are now compliant with FIPS 140-2 security level 1.

   Gemalto MD 3810 and 830b smart cards now support FIPS 140-2 security level 1. Email Signing no longer fails when FIPS 140-2 is enabled.

3. ## California Password Law

   Updates to comply with 2020 California Password law (SB-327).
   This software release supports the California password law SB-327 effective January 1, 2020. The device admin password and SNMP private string will be the device serial number if a forced altboot reload is performed. The password is case sensitive.

4. ## Energy Star 3.0

   This software release ensures our products will continue to meet Energy Star. Energy Star 3.0 means more stringent power efficiency and conservation requirements and is going into effect October 2019. This software release provides the necessary updates to meet these new specifications.

Firmware 073.xxx.019.14200 July 2019(Re-spin)

1. ## Improvements to Software Reload Process

   Settings like Energy Saver and Accounting Method are properly restored after service rep software reload.

Firmware 073.xxx.019.13010 May 2019

1. ## 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 must be the Login Method on the MFD
   - An LDAP user must be logged in at the MFD
   .

2. ## Enablement of Cherry ST-1144 Smartcard Reader

   Cherry ST-1144 USB Smartcard Readers are supported in this release.

3. Xerox® Lockdown Security Solution

This release introduces other languages in support for this feature.

4. Device Behavior Improvements

Various fixes are provided in this release including:
- PCL6 Jobs now print correctly when "Suppress All Blank Pages" is selected in CWIS
- Fax confirmation report now prints reliably.

Firmware 073.xxx.009.03700 February 2019

1. Xerox® Lockdown Security Solution

This release introduces the Xerox® Lockdown Security Solution which was previously known as Xerox® Healthcare Lockdown Solution, initially introduced with Firmware 073.xxx.197.2850 October 2017. This release is in English language only. Other language translations will be introduced in future releases.

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 073.xxx.197.2850 October 2017 for more details.

2. Closed Envelope Tray message does not clear

When using the envelope tray, the "Close Tray 1 Message" is now properly removed when the envelope tray is closed.

Firmware 073.xxx.068.33100 December 2018

1. Scan to Home

An intermittent scan to home issue has been fixed that ensures files are properly stored in the home repository

2. Printing via IPP protocol

Printing a Tabloid PDF via IPP or IPPS no longer results in the job shrinking to fit on Letter size paper.

3. Authentication

Changes to improve the speed of authentication and EIP screen access when using the VPSX convenience authentication solution.

4. Security

The following security vulnerabilities have been addressed:

SB16-165 CVE-2016-4447 CVE-2016-4449

SB16-277 CVE-2016-6304 CVE-2016-6306 CVE-2016-6306

SB16-333 CVE-2016-9533 CVE-2016-9535

Various cross scripting vulnerabilities (XSS) have been addressed.

Firmware 073.xxx.058.25300 Sept 2018

1. 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 which are now supported with this release.

CAVEAT for this Release:
Email fails to send when using Gemalto 3810 or 830b MD smart card when both Email Signing and FIPS 140-2 (Level1) are enabled. A Pop-up error is displayed to the user stating: "Job Deleted. No messages were sent. Device unable to sign email".

Note: Either FIPS or Email Signing must be disabled to send Email successfully.
If any email signing with these new cards is required, a Xerox technician will be needed to upgrade the device.

2. Message stating device in energy saver mode after card swipe

Fixed an intermittent issue of UI message stating device in energy saver mode after authentication card swipe. A power cycle was required to clear this message.

3. Device freezes when waking up from power saver mode

Fixed an issue of device lock ups when waking up. A power cycle was required to revive the device.

4. Fault code 319-300 while printing.

Fixed an intermittent issue that caused a 319-300 (Image disk offline) while printing. The image memory buffer occasionally filled up, and caused this error.

5. Tray 2 confirmation screen appears when waking up from power saver

Fixed an issue that displayed the paper size confirmation screen for tray 2 when waking up.

Firmware 073.xxx.008.15000 June 2018

1. Security Cross Site Scripting HTTP header added.

The Qualys Security Scanner detected a cross site scripting (XSS) vulnerability on port 443 for HTTPS which is corrected in this SW release.

2. Fixed duplex printing issue from SAP.

Fixed an issue that prevented duplex prints in SAP environment

3. Custom scan file naming

Fixed an issue that prevented custom scan to file names longer than 8 characters.

4. PDF document printing

Fixed an issue that caused an error sheet to be printed instead of PDF document.

5. The device will go into a hung state and stop processing print jobs

Fixed an issue that caused device to hang and then stop processing print jobs

6. Certificate doesn't update after IP address renewal.

Fixed an issue where after having picked up a self-assigned certificate once, the self-assigned certificate no longer updates when the IP changes

7. Printer unable to resolve SMTP host name via DNS with Server 2012 or 2016

Fixed an issue in scan to email when the smtp server was set as Host, the device could not resolve to the IP.

8. 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:

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

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

3. Select **Edit** for POP3.

4. 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.

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

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

7. Enter password again under **Retype password** and check the **Select to save new password** checkbox.
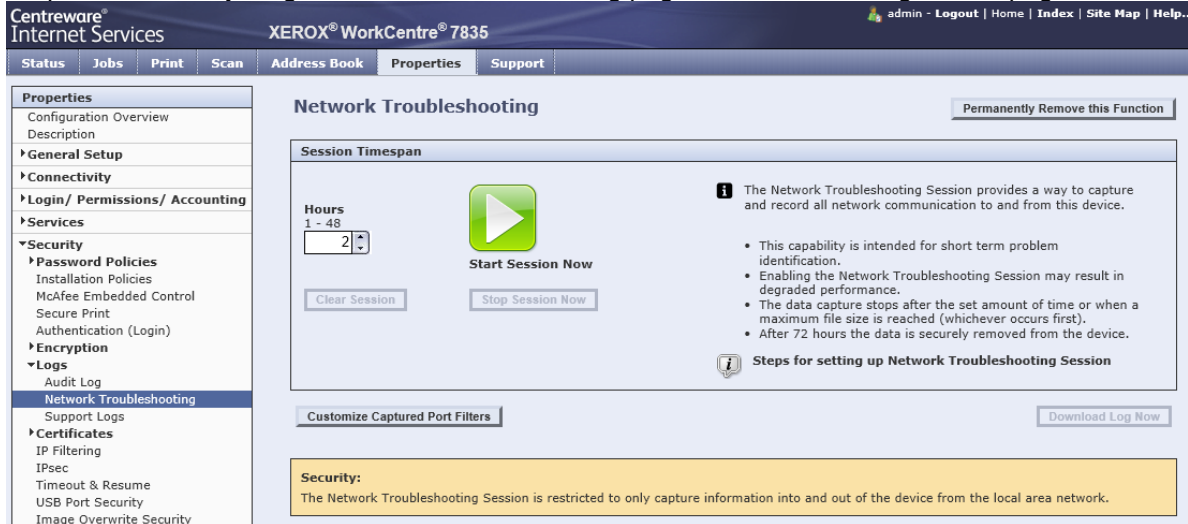
8. Select **Save**

8

9. Hide Network Troubleshooting

Overview: These WorkCentre Devices have added the ability to permanently remove the Network Troubleshooting feature.
Note: This will **_permanently_** remove the Network Troubleshooting feature from the device.

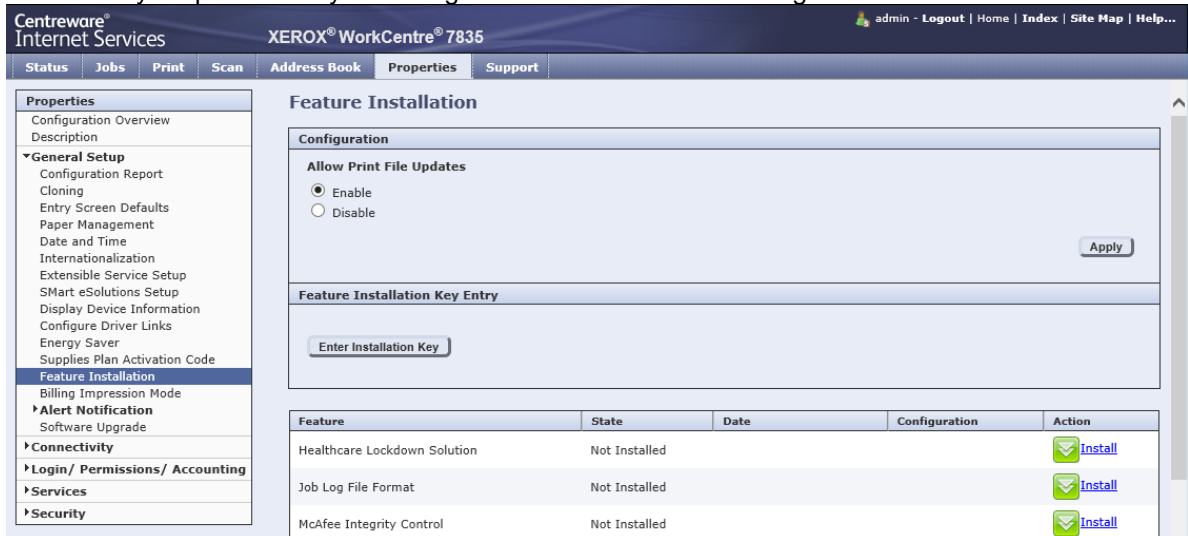There are two methods to remove this feature from the device.

The first method is a button called Permanently Remove this Function on the Network Troubleshooting page. This will allow an Administrator to remove the feature. The button is located on the WebUI under Properties, Security, Logs, Network Troubleshooting page. Below is an image of the page.

The second method is to install a Feature Installation Key (FIK) on the WebUI under Properties, General Setup, Feature Installation. Then select Enter Installation Key.
The FIK key for permanently removing the Network Troubleshooting feature is **468854198391**

Permanently removing the Network Troubleshooting feature can be cloned.
There is also support of a MIB to Hide 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.

Firmware 073.xxx.008.05210 March 2018

1. Device Behavior Improvements

Various improvements have been made in the areas of:

- A fix was added to mitigate the UI screen displaying login screen when authentication is not enabled.

- Large PDF printing has been improved to reduce occurrences of fault codes displayed.

- PDL switching over port 9100 is now more robust.

2. Xerox Dropbox App blank screen

- The patch released in December that enables the Dropbox App to work properly has been integrated into this release.

Firmware 073.xxx.247.32400 December 2017

1. 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.

2. Device Behavior Improvements

Various improvements have been made in the areas of:
- Paper Cut and Xerox Device Manager may report duplicate jobs to job based accounting·
- Device not entering power saver if a secure print job was held.
- Reliability improvements to power saver mode.

Firmware 073.xxx.197.28500 October 2017

1.   PIV Card Support

This release adds support for the following additional Gemalto IDPrime PIV
(**P**ersonal **I**dentify **V**erification) format SmartCards:
- Gemalto TOP DL - protiva PIV applet V1.55
- Gemalto TOP DL V2 – protiva PIV applet V1.55

2. Simplified Chinese Language Support

The ConnectKey® WorkCentre® 7855 XOM devices will be able to support Simplified Chinese language via either of the following two modes:

- Set Simplified Chinese as the default language/keyboard: The default language/keyboard on the device can be set to Simplified Chinese via the user interface Language/Keyboard setting. This setting is accessible to an Admin via: Machine Status > Device Settings > General > Language/ Keyboard Selection. Setting the default language to Simplified Chinese will also set printed reports and banner sheets to appear in this language.

Note: A user can change the current session display language and keyboard to any other language via the 'Language' Hard button on the control panel.

- Select Simplified Chinese language/keyboard for current session only: The default language/keyboard can be set to any other language and a User can select the Language hard button on the console to select Simplified Chinese for their current session only. Enabling Simplified Chinese via the Language button will only last until the user interface session timeout or user logout at which point the device will revert to the default language configured by the Admin. This mode of operation does not affect printed reports and banner sheets.

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 073.xxx.197.2850 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.

Feature Install Key (FIK)
Unlocks the Feature for device Serial Number

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.

How the Xerox® Lockdown Security Solution Works:

The Lockdown Security Solution performs the following functions:

"Locks-down" a set of security settings on the printer as the name implies, 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 /or 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.
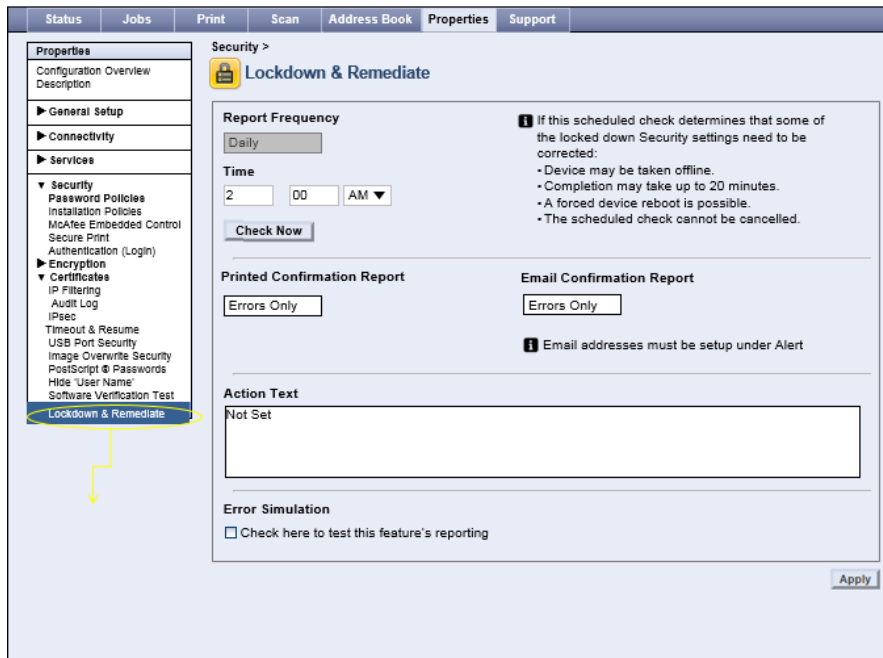
4. Long Media Solution

New system policy to influence how the <u>scanner</u> handles "long" media when it is unable to identify the page size.
This setting can be found under:
General Setup > Paper Management > Required Paper Policies / Default Legal Size. Systems primarily being used to scan or copy 8.5 x 13.4" will want to set this new policy to use 8.5 x 13.4" as the default legal [scan] size.

Note: There are limitations with both the trays and the scanner in regards to being able to differentiate the new 8.5 x 13.4" size from sizes slightly smaller (e.g. 8.5 x 13") or slightly larger (e.g. 8.5 x 14"). There may still be use cases that require the target tray or size be manually specified by the user in order to ensure the system copies to the desired size media.

Firmware 073.xxx.177.14300 June 2017

1. Cloning Web Service

These ConnectKey Devices will accept clone files from Xerox® CentreWare® Web software via a Cloning Web Service with a Network User ID and password. This CWW functionality was released in the summer 2017 CWW release.

CentreWare Web will deliver compatible software for this ConnectKey solution that will Import, export and manage clone files. CWW and ConnectKey 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.

2. EIP Authentication

For EIP web service calls requiring administrator credentials, these ConnectKey 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'.

3. Disable Print Submission of Clone Files

These ConnectKey devices are able to disable the delivery of Clone files through the Print Submission path. This setting is located in CWIS under Properties, Security, and Installation Policies

4. Support Log Tab

The previous Network Log functionality in CWIS will now be called Support Logs. These are located in CWIS under Support, Troubleshooting, Support Logs and also under the Properties, Security, Logs, Support Logs.

5. Disable SNMP Sets

These ConnectKey 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 in CWIS under Properties, Connectivity, Setup, and SNMP.

6. XML Configuration Report

These ConnectKey device Admins will be able to download the Configuration Report in XML format. This capability is in CWIS, under Properties, General Setup, and Configuration Report.

7. Ability to Hide Username for Security Reasons

Note: This Feature is only available on the Xerox® ConnectKey® WorkCentre® 7845/55 & 7970/7970i

ConnectKey WorkCentre device Admins will be able hide the Job Owner on the completed Jobs tab of the local user interface for security reasons. This can be accomplished by entering a Feature Installation Key browsing to the following web page in CWIS.

Go to Properties>General Setup>Feature Installation

Enter Install Code 800288904661*

Select Apply to enable the "Hide Job Owner" feature for Completed Jobs.

8. Duplex Color Scanning Options

The single pass duplex scanner, on the WorkCentre® 7845/55 & 7970 may lead to inaccurate color detection at low resolutions. New options to enable the scanner to scan at 600x600dpi are available. This will allow for optimal color detection, but could negatively impact scanning performance.

How to Enable this Feature:
Properties>Services>Scan Services>Defaults & Policies

Duplex Color Scanning Options

- **Select fastest scanning speed** means that the device will scan at 600x300 whenever the user selects 300dpi or lower
- **Select best auto-color detection accuracy** means the device will scan at 600x600 whenever the user programs a job for 300dpi or lower with duplex scanning and auto-color selected, as well.
- **Select best auto-color detection accuracy and color image quality** means the device will scan at 600x600 whenever the user programs a job for 300dpi or lower with duplex scanning and auto-color or fill color selected, as well.

Default setting is fastest scanning speed.

Why an SA would change this: If they use accounting and account for mono scans differently than color scans, they would want to change this setting. However, we expect most users will not notice a change in system behavior if this setting is changed.

9. Network Troubleshooting Log

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.

Firmware 073.xxx.147.07400 March 2017

1. Inter Job Offset Disablement

This adds the ability to disable job offset (the offset between jobs). A new setting was added to CWIS that controls Job Offset for all jobs independent of submission methods (e.g. Xerox Global Print Driver, LPR, and CWIS).
This feature will now allow the ability to print jobs to the MFD as a single aligned stack on the output tray.

In CWIS, the Admin must navigate to Properties/Printing/General/ and set the Offsetting Between Jobs feature to "No Offset Between Jobs" on the MFD.

Note: When submitting a print job through the print driver, to disable offsetting between sets, the user must go to Printer Properties/Advanced/Offset Output and change the setting to No Offset.

Firmware 073.xxx.136.34300 December 2016

1. Improve Hold All Jobs Security When Logging Out

There is a new feature in Hold All Jobs which can prevent jobs from printing when the job owner is not logged in. This policy builds on the current Hold All Jobs feature and applies to a specific user's print jobs. This new feature can automatically delete any in progress or pending print jobs if the job owner logs out of the device. This can reduce the likelihood that jobs might be accessible to anyone other than the job owner.

Enablement is done in CWIS. Go to Properties >Services >Printing>Hold All Jobs >When Users Logout Occurs:
- Delete all jobs in queue
- Continue to print all jobs in queue

Example: If the policy is set to delete, when the User logs out any job printing or pending in the queue belonging the logged out User will be deleted.

Hold All Jobs Enablement needs to be set to Hold Jobs in a Private Queue

2. Pause System Timer While Printing

A new feature that allows the printing to pause the system timer while a job is printing. This feature prevents the User's session from timing out during log print jobs. While a job is printing the system timer will not be active. Once the job has finished printing, the system timer will start again.

Enablement is done via a FIK Key*. Go to Properties>General Setup>Feature Installation
- Enter Install Code 6657 7466 5227
- Uninstall Code 6658 7466 5227

Go to Properties>Security>Timeout & Resume> Pause System Timer While Printing.

Firmware 073.xxx.106.26100 September 2016

1. Custom Administrator Solution

This release enables a new level of Administrator called Custom 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.

Note:
- Custom Administrators permissions are determined by the Admin.
- Administration of the Custom Admin role can only be performed via CWIS.
- 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 CWIS.

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.

1. Create a new Custom Administrator role
   a. Login to the device CWIS as Admin
   b. Select **Properties** > **Login** / **Permissions** / **Accounting** > **User Permissions**
   c. On User Permission Roles row, select **Edit**
   d. On User Permission Roles page, select **Device Management** tab
   e. On Device Management tab, select **Add New Role**
      i. Type in **Role Name** (e.g. Custom Admin Role) and **Description** (e.g. Some settings are Read Only)
      ii. Select **Create**
2. Assign permissions to the Custom Administrator role
   a. On **Add Management Role** page, select **Properties** tab
   b. If **Forbid All** is selected, this role will not have rights to change any of these settings.
      i. To give users in this role the rights to change a particular setting, set the pull-down in the status column to **Allowed**.

3. Assign users to the Custom Administrator role
   c. On **Add Management Role** page, select **Assign Users to Role** tab
   d. Select **Add New User**
   e. On **Add New User** page, define the corporate wide **user** and **password**
      i. Type in **User Name** (e.g. HealthAdmin) and **Friendly Name** (e.g. HealthAdmin)
      ii. Type in **New Password** and **Retype password** (e.g.1234 or other unique password)
      iii. Select **Save**
   f. On **Add Management Role** page, **Assign Users to Role** tab
      i. Select the **check box** in front of the new user (e.g. HealthAdmin)
      ii. Select **Apply**

4. Creating a logged-in user role (optional)
   a. Login to the machine as Admin or Custom Admin
   b. Select **Properties** > **Login** / **Permissions** / **Accounting** > **User Permissions**
   c. On User Permission Roles row, select Edit
   d. On User Permission Roles page, select Logged-in Users tab
   e. On Device Management tab, select Add New Role
      i. Type in **Role Name** – "Logged-in user" and **Description** – "Allow logged-in users unrestricted access to all features except Tools"

Firmware 073.xxx.086.15410 June 2016

1. Billing Meter Read Email Setup

ConnectKey® WorkCentre® device Admins will be able to set and submit billing meter reports from the device with an option of scheduled or manual email submission.

Note: Email feature is required and must be configured on the device to use this feature and you must select Apply once all recipients and groups are created or the information will be lost when going to another screen in CWIS.

Go to Properties> Alert Notification> Email Alerts and enter the email address you want the device to send the report to. Individual recipient groups can be created and recipient group preferences can be selected.

To Schedule or manually submit the billing meter report you must select Edit under Actions for Email billing meters for manual submission.

Recipient Group Preferences				
Status Codes (Glossary)	Group 1	Group 2	Group 3	Action
Billing meter reads reported by SMart eSolutions	✔	✔	✔	
Email billing meters for manual submission	✔	✔	✔	✏ Edit...
Device or some services are not available	✔	✔	✔	
Potential persistent problem exist	✔	✔	✔	
Device requires administrator assistance	✔	✔	✔	
Device is operational, but degraded	✔	✔	✔	
Paper supply is low	✔	✔	✔	
Paper jam is detected	✔	✔	✔	
Supplies or CRU's are low	✔	✔	✔	
SMart eSolutions enrollment is cancelled	☐	☐	☐	

Set jam timer for release of status to selected groups

0   minutes (1-60)

✅ **Required Configuration Settings**

Setting	Status	Action
SMTP	✔ Required; Configured	✏ Edit...
From Field	✔ Required; Configured	✏ Edit...

Sending a Billing Meter Report Now:

This Allows the Admin to submit a billing meter report as soon as the "Send Billing Meter Report Now" button is selected.

Note: It can take up to 15 minutes to receive the report from when the button is selected.

Setting the day of the month for billing reports to be sent:

If a scheduled billing meter report is desired then the Admin can also set up the report to be sent on the same day and at the same time of every month by Selecting the desired Time and Day and selecting Apply.
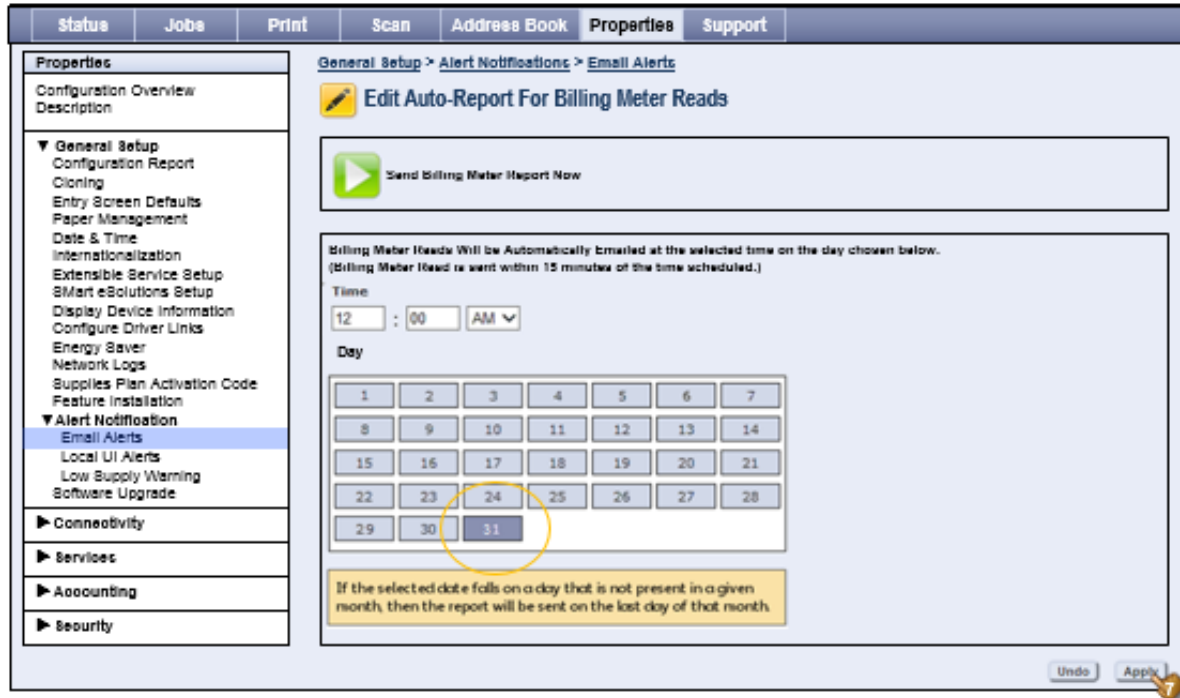
Firmware 073.xxx.066.08210 April 2016

1. Wake on Swipe

The RFID Integrated Card Reader Alternative Power Retrofit Kit 497K18900 for WorkCentre® 78xx and 79xx products equipped with RFID Integrated Card Reader Kits that was previously announced is currently unavailable. See caveats below as a result.

The "Wake on Swipe" capability introduces the ability to control the USB ports power state in sleep mode giving the administrator the ability to separately set the front or rear USB ports as either 'powered' or 'not powered' while in sleep mode. The 'powered' setting enables USB accessories connected to the USB ports to function when the device goes to sleep such as:

- USB Wi-Fi dongle network connectivity
- USB authentication card readers to be able to read access card, wake device and login user

Previous Release, 073.xxx.055.33800, introduced this feature control from CWIS via Properties > Connectivity > Setup where the administrator can set the USB ports as either 'powered' or 'not powered' while in sleep mode.
Previous Release 073.xxx.066.08210 introduced Local User Interface controls for the administrator to manage the power to the USB ports during device sleep mode. A "USB Port Sleep Mode" setting page is added to Local UI under Tools > Network Settings > USB Settings > USB Port
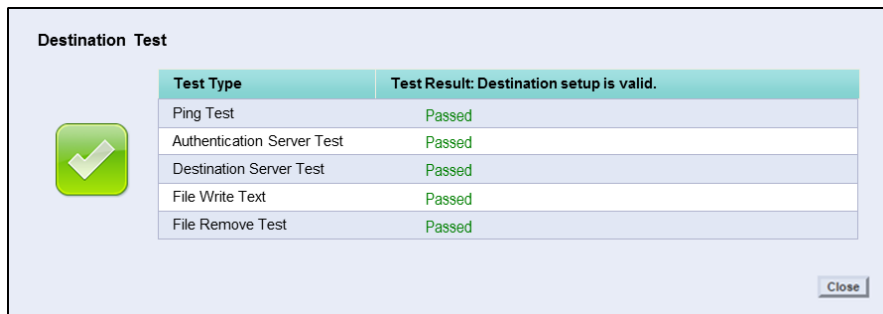
Caveats:
- If adding a USB hub to the device, the device must be awake when the hub is plugged in to operate properly.
- WorkCentre 78xx and 79xx: Front USB port power control is not currently supported on WorkCentre 78xx or 79xx. Kits that use the front USB port such as Xerox Integrated/Programmable RFID Reader Kits do not support Wake on Swipe on this product.

Workarounds:
- Press Energy-Saver key on the keyboard to wake MFD, wait for MFD to wake, swipe card and login. (replacing the workaround to the current caveat)
- CSE utilize the NVM switch to turn "Energy Saver off"
- CSE or admin set the "Sleep and Wake up at Scheduled time" to: Wake up before anyone arrives at the work place, Sleep after everyone has left the work place.
- Install external RFID card reader that plugs into the rear USB port instead of Xerox Integrated / Programmable RFID Reader Kit which uses the front USB port.

2. Scan to Destination Setup Test Button

The Scan Destination Setup Test Button feature saves the Administrator time by providing the ability to test, and then receive troubleshooting assistance while setting up scan destinations.
Prior to this feature enhancement the Administrator would set up the device but was unable to test it in CWIS, leading to service/support calls. The Destination Test Button is available once the file destination settings are entered and then selected.

Destination Test

Test Type	Test Result: Destination setup is valid.
Ping Test	Passed
Authentication Server Test	Passed
Destination Server Test	Passed
File Write Text	Passed
File Remove Test	Passed

Close

Caveat: If using IPV6 addresses, the Scan Destination Test available on the Embedded Web Server will incorrectly fail its Ping test even though the IPv6 address works in an actual scan if all other settings are correct. For Scan Destination Test purposes please use either the hostname or an IPV4 address.