What’s New with Xerox® Centreware Web 6.0 and 5.16

1.1 What’s New with Xerox® Centreware Web 6.0 and 5.16
1.2 In this module you will learn about:

In this module you will learn about:

What’s New in CWW 6.0

- Clone Management
- Firmware Policy Upgrades
- Remote Configuration of New Devices
- UI Improvements & Updates
- Device Dashboard
- Device Support Updates
- Support for SQL Server 2016 & Windows Server 2016

What’s New in CWW 5.16

- Retained Device Admin Passwords
- Multiple Threads for Device Software Updates
- Expansion of Configuration Sets for ConnectKey MFPs

Use the Next & Previous buttons below to advance slides or the Menu to the left to select specific content for review.

1.3 What’s New with CWW 6.0
1.4 Clone Management

Clone Management

Users can clone settings from a single device to entire groups of similar devices. This simplifies the printer configuration process typically performed each time a printer is deployed across a corporation.

It’s important to choose the right method for cloning settings from a single device to a group of similar devices. There are 3 different methods for cloning, one for each of the following:

- Xerox Devices
- AltaLink devices or ConnectKey i-Series
- Phasers

1.5 Upgrade Printers Wizard

Clone Management, cont’d.

Users can clone settings from a single device to entire groups of similar devices. This simplifies the printer configuration process typically performed each time a printer is deployed across a corporation.

The CWV Upgrade Printers Wizard can upgrade any printer supporting the common method of firmware upgrade via port 9100. This includes the VersaLink® series of devices.
1.6 Clone Printers Wizard

Clone Management, cont’d.

Users can clone settings from single device to entire groups of similar devices. This simplifies the printer configuration process typically performed each time a printer is deployed across a corporation.

Clone Printers Wizard

To clone **Altalink devices or ConnectKey i-Series devices** with software versions 073.xxx.147.07400 or later, use the **Clone Printers Wizard**.

**Key Features:**
- Secure Authentication using Network User credentials
- Manage multiple Clone Files in a Repository
- Users can easily filter clone files by specified model

1.7 Clone Phaser Printers Wizard

Clone Management, cont’d.

Users can clone settings from single device to entire groups of similar devices. This simplifies the printer configuration process typically performed each time a printer is deployed across a corporation.

Clone Phaser Printers Wizard

This cloning feature copies the configuration settings from one printer to a maximum of 25 printers of the same model running at the same firmware level. This option is used by some Phaser devices.
1.8 Firmware Upgrades & Policies

Firmware upgrades can:
- Supply corrective actions
- Enable new features and the latest security updates
- Facilitate remote management

Benefits:
- Customers can save time while remotely managing the stability of their fleet. Ensuring consistent firmware versions ensures up-to-date security and compliance.

New Firmware Policies will enable customers to easily manage and ensure consistent settings across their device fleet to meet security requirements.

1.9 How to create Firmware Policies

How to create Firmware Policies

- The Firmware Versions Policies grid shows the policies that have been created and their status. Within the grid you can edit and copy policies. You also have the capability to create a new policy, delete it, or perform a release upgrade.

Select the Upgrade Printer Wizard, go to the Device Management Dashboard>Device Firmware, or go to Device>Device Firmware>Firmware Versions Policies.

- To create a firmware policy:
1.10 Firmware Version Policies

Firmware Upgrades & Policies, cont’d.

Firmware Version Policies

How to deploy Firmware Policies

Firmware Upgrades & Policies, cont’d.

Deployment Tasks

- Each Deployment task is associated with a single policy. When the policy is Monitor only or Monitor and Upgrade Only, no Deployment Task is created. For any other case, there should always be one task for each policy.

Notes

- If there is a failure in the upgrade, the process restarts at the last stage of the upgrade task.
- An upgrade task in progress can be Stopped, Restarted or Deleted
1.12 Remote Configuration of New Devices

Remote Configuration of New Devices

You can use configuration sets to configure a newly installed device remotely. Instead of performing the initial setup at delivery on site, the Xerox® CWV administrator can create a configuration set and policy to automatically perform this function.

- This is supported for devices initially set for Dynamic Host Configuration Protocol (DHCP) only.
- The device must be connected to a working network that is reachable by Xerox® CWV.
- Available only for devices that support remote Install Wizard settings.

Use

- Create a configuration set that includes disabling the Install Wizard screen (Security/Disable Services tabs)
- Create a policy.
  a. Add the configuration set that was created in Step 1.
  b. Set the policy to run on newly discovered devices - or - select devices for which to apply the policy.
- Run Discovery that includes the subnet for the new device (either through schedule or on demand).

1.13 New UI & Improvements

New UI & Improvements

Changes and enhancements to the existing UI are being phased in. Users will see several areas that utilize a new UI scheme and workflow.
1.14 Device Dashboard

Device Dashboard

The Device Health Dashboard allows you to monitor devices and resolve issues to ensure that they remain in the desired configuration state. Once you have set configuration or firmware policies, you may view the overall compliance level. Drill down features make it easy to see and understand the policy compliance at each device level.

1.15 Device Support Updates

Device Support Updates

CWW has the ability to update its list of supported devices. This extends the list of devices that firmware updates can be applied to, the devices that protocol settings can be applied to, and what devices can be used with Network Accounting. This alleviates the need to have a new version of CWW to expand device support.

Steps Required:
1. Go to Administration > Advanced and select Xerox Centreware Web Updates
2. In the Device Configuration Settings section select the Update button.
1.16 Support for SQL Server 2016 & Windows Server 2016

Support for SQL Server 2016 & Windows Server 2016

With the addition of support for SQL Server 2016 & Windows Server 2016, Centresware Web now works with a wider range of environments.

1.17 What’s new with CWW 5.16

What’s new with CWW 5.16
1.18 Retained Device Admin Passwords

Retained Device Admin Passwords

An enhancement to the setting of Retained Device Admin Passwords gives the ability to choose "0" to indicate to not keep any saved device admin passwords. This handles the case where a customer would like to temporarily change the admin password for a service call and then reset it to the original password.

1.19 Multiple Threads for Device Software Updates

Multiple threads for device software updates

Multiple threads for device software updates of a fleet greatly improves the speed of upgrading multiple devices.
1.20 Configuration Sets

Configuration Sets

Benefits
Create and use
New Attributes

1.21 Typical customer questions

Configuration Sets

Your ticket to set and maintain Security Policies

Typical customer questions

How can I set a fleet wide policy for the critical configuration settings for my MFPs?

How can I maintain a fleet wide policy for the critical configuration settings for my MFPs?

You answer...
CentreWare Web Configuration Sets

Published by Articulate® Storyline www.articulate.com
1.22 Ensuring consistent settings across the fleet

Customers need to have consistent settings across their device fleet to meet security policies and to ensure easy management.

Options

- Utilize the embedded web page of each device and make the required settings changes.
- Utilize the embedded web page of a device to create and store a clone file and then use CentreWare Web to apply it to devices.
- Create a specific set of configuration settings as desired and a use Config Tasks to apply them to a fleet.

Benefits

- You can use a single Config Set regardless of the number of device models and across the portfolio (cloning is designed to be used on specific models).
- Revisions in a configuration can be handled easily by revising one Config Set, rather than multiple clone files or one device at a time.

1.23 How to use Config Sets and Config Tasks

There are a few steps to creating a Config Set and then calling it via a Config Task to execute it and apply it across your devices.

Preparation

- Before you start, create a separate list of the specific settings the customers desires to set on their fleet of devices.
- Be aware some settings may not be available to be set at all or set remotely on some device models.
- Create a list of the devices the customer desires to have the settings applied to.

PILOT Test

- Create a Config Set and a Config Task pointing to the Config Set with the first few settings to apply and test them on a single device. Review the results and note any exceptions.
- Gradually add more settings and test them on your initial single device.
- Then, apply them to a few other devices to confirm they are set properly.
- When you are successful with these results, expand the Config Task to set these across your fleet.
- Revisions in a configuration can be handled easily by revising your Config Set.
1.24 Creation - Step 1

From the menu select:

- Printers
- Configuration Sets
- New Set

1.25 Creation - Step 2

From the Identity tab:

- Input the Set Name and other descriptive information
- Click on Save
1.26 Creation - Step 3

Creation
Step 3
From the Defaults tab:
- Select the Features option
- You may now set 4 different Secure Print settings to apply across the fleet

1.27 Creation - Step 4

Creation
Step 4
From the Conceal Job Names dropdown, select one of three options:
- Show All Job Names
- Conceal Secure Print Job Names Only
- Conceal All Job Names
**1.28 Creation - Step 5**

Creation
Step 5
From the Method Used for Releasing Secure Print Jobs dropdown, select one of two options:

- Passcode (aka PIN)
- User ID

If the customer uses setup authentication via a card or other method at the MFP's front panel, it is more convenient and secure to use the user ID of the print user instead of a numeric PIN.

**1.29 Creation - Step 6**

Creation
Step 6
From the Security tab:

- USB port Security

You may now disable USB ports remotely.
1.30 Creation - Step 7

From the menu select:
- Printers
- Device Configuration
- Configuration Tasks
- New

The Configuration Task executes the Configuration Set you previously created.

1.31 Creation - Step 8

From the Details tab:
- Identify the Configuration Task for later retrieval
- Link to the Configuration Set you created
- Choose which method to use
1.32 New Config Set Attributes (1)

New Config Set Attributes (1 of 3)

- **Workflow Scan compression defaults**
  - Ability to remotely set file compression settings to reduce file sizes for workflow scanning and scan to home applications.

- **Set preferred Address book**
  - Provides the flexibility to set the scan to e-mail default address book as ‘Network’ or ‘Device’ based.

- **Expanded Network Connectivity Setting Coverage**
  - Added new network protocols including those associated with mobile printing.

- **Added ability to set Energy Saver settings**
  - You may set your fleet’s settings on which to move to low power and sleep mode. You can even schedule the times for the devices to go to sleep and wake up each day.

- **Policy for jobs held**
  - Enables remotely setting policy for both printing around held jobs and for a policy of printing on alternate paper when jobs are held for resources.

---

1.33 New Config Set Attributes (2)

New Config Set Attributes (2 of 3)

- **Added additional Authentication settings**
  - This includes the ability to set the screen title and instructional text of the MFP’s authentication screen to tailor it for your fleet.

- **Creating new workflow scan templates**
  - Provides the ability to define repetitive scan workflows with default values for attributes such as resolution, image enhancements, and file naming.

- **Modifying default templates**
  - Provides the ability to define repetitive scan workflows with default values for attributes such as resolution, image enhancements, and file naming.

- **Secure print policy defaults**
  - May set policy to be Pincode or User ID, set Pincode length, set a policy to conceal print job names & allow authenticated users at the front panel to release secure prints without additional steps.

- **Set minimum certificate length**
  - May set a policy to restrict certificates to have a minimum key length.
1.34 New Config Set Attributes (3)

New Config Set Attributes (3 of 3)

USB port security
May close front or rear USB ports.

Device Configuration Report
May set ability to not print configuration report at device power on and restrict its printing to the Device Admin.

E-mail
Ability to set a variety of defaults across the fleet. These include SMTP encryption, user encryption, digital signing, compression methods, format and the ability to have the resulting document searchable.

Fax reports
Set the policies on when and whether to print fax reports.

Print Held Job time out
May set the device default for the number of days/hours/minutes before deleting jobs held at the device.

1.35 You have completed viewing this course.

You have completed viewing this course.

To register your completion in Learning@Xerox, click the gray forward arrow on the bottom right of this page to submit the Acknowledgment and receive completion credit in your learning history.