Fleet Management Is Now Even Easier

Xerox® CentreWare® Web Version 6.3
Firmware

**Performance Improvements via Hub and Spoke**

Xerox® CentreWare Web has the ability to multi-thread upgrades from a CentreWare Web server to up to four devices at once. With this new update, you can improve upgrade performance by transforming a subset of your multifunction printers (MFPs) into firmware distribution hubs for the remaining MFPs in the fleet.

We’ve also enhanced upgrade reliability with device-managed upgrades through Fleet Orchestrator.* Now, instead of Xerox® CentreWare Web or a hub pushing a file, devices will request it at a scheduled upgrade time. You create the schedule. Xerox® CentreWare Web configures the settings and schedule of the devices. And the devices do the rest. Advanced scheduling features let you configure download and installation times in a way that makes sense for your business and synchronize upgrades across your entire fleet.

**Multiple Version Upgrade Path**

Monitor and Automatically Upgrade mode can now support multiple version firmware upgrades. This means you can set up policies to coordinate firmware updates when a device requires multiple firmware versions as part of an upgrade. So if, for example, you’re upgrading a Xerox® ConnectKey® 1.0 device to ConnectKey® 2.0, the device will automatically upgrade to ConnectKey® 1.5 before installing the final version. We recommend this method when setting up a monitor and automatic upgrade policy for firmware upgrades that need to handle multiple possible versions across devices.

Firmware Repository is a new screen that provides the same functionality as the Qualify field. It lets you keep track of firmware files that have been qualified via a test and firmware that has been uploaded for testing. When the Qualify field is set to “No,” the user can only send the file to a single device through a firmware upgrade policy. When it is set to “Yes,” the file can be sent to any number of devices simultaneously.

*Xerox® AltaLink® devices only, initially*
Passwords

**Password Management**

With the new Password Policies feature, you can update passwords at scale (e.g., 1,000 devices as part of policy/config set).

**Key Features**

- Track previous passwords for each device in Xerox® CentreWare Web
- Track when a password was set in Xerox® CentreWare Web
- Audit known device passwords with Security Policy
- Retry last passwords and even the default admin password (1111) to find and remediate incorrectly stored passwords
- Receive admin audit reports for verified passwords
- Change passwords on a single device or a group of devices simultaneously
- Enable unique passwords for every device
- Create a random password for each device or a single random password for a group of devices
- Create a unique password for each device using a uniqueness pattern based on prefixing serial number/MAC address
- Create unique passwords for each device by appending a sequence number or date stamp with the password

McAfee

**Monitor and Alert on Security Events, Intrusion Detection**

McAfee technologies now proactively monitor and communicate security events on devices discovered by Xerox® CentreWare Web that have “McAfee Embedded Control” enabled and have been registered to communicate with Xerox® CentreWare Web.

The McAfee Security Monitoring dashboard chart provides a complete breakdown of all security events in the past 30 days. Using the drilldown feature, you can view the detailed messages from devices about security events and audit individual events with an appropriate audit determination. And with the McAfee Monitoring Trend chart, you can track security event trends over the previous 12 months.

Discovery

**Automated Remote Device Discovery**

With this feature, supported devices* can now connect automatically with a Xerox® CentreWare Web server.

**Here’s how it works:**

- Device initiates contact with the CentreWare Web server
- CentreWare Web server runs a discovery on the device that sent the request
- CentreWare Web either adds the device or updates its information on the device
- During discovery, CentreWare Web adds its address to the “managed by server” field on the device
- Policies can be created to automatically configure the device upon discovery

*xerox® AltaLink® devices only, currently
Feedback

**IMPROVED ERROR MESSAGING FOR CONFIGURATION SETS**

Configuration set error messaging is now clearer and more specific than ever. Improvements include:

- Revised text in the error messages
- Clear and direct messages on any SNMP set errors to help users diagnose and troubleshoot the problem quickly

**SNMP V3 ACCESS DENIED TROUBLESHOOTING**

SNMP Access Denied is a new device status that applies to any device that is not responding due to SNMP-related issues. This new status helps rectify the SNMP issues listed below and accelerates device rediscovery.

- Invalid Get Community Name
- SNMPV3 Wrong User Name
- SNMPV3 Invalid Auth Key
- SNMPV3 Invalid Privacy Key
- SNMPV3 Invalid Context Name

Configuration

**CONFIGURATION POLICY UPDATES (REMOVAL OF TASKS)**

Configuration Set Tasks have been removed. This functionality is now available in Configuration Profiles. Any existing tasks will be converted into policies when you upgrade. Thresholds that affect remediate and display in the dashboard have also been removed. The new, simplified dashboard will only ever show Green and Red and the policy will always run if it is in remediate mode. Other UI simplifications include:

- Consolidation of History and Actions tab into the Identity tab
- Greater consistency between Configuration Policies and Firmware Upgrade Policies screens

Users also have the new option to receive an audit report whenever a policy error occurs. And a new role can be created called “Customer Report User.” This user can only see the dashboard and the device grid. They are not able to create policies or perform any device modifications.

**SUPPORTED SETTINGS FOR REMOTE CONFIGURATION EXPANSION**

End users can now configure even more device settings remotely. Settings include those that are available via the device’s Embedded Web Server and/or the device’s local user interface such as:

- Wireless Network Settings
- Network Proxy Settings
- IPP Network Authentication Settings
- Google Cloud Print
Dashboard

**DASHBOARD ENHANCEMENTS**

More dynamic dashboard capabilities help give you a more accurate picture of security and compliance.

1. Historical View: See up to 12 months of overall compliance across configuration and password policies.
2. Compliance Graph by Model: View a breakdown of compliance by model across multiple policies.
3. Settings Group Headers: Adds the configuration profile path to the configuration policy audit report for easy access when modifying the configuration profile.
4. Scheduled Tasks View: Review the overall schedule of policies defined in Xerox® CentreWare Web including configuration policies, password policies and firmware policies.
5. Automatic Policy Remediation Results: Get an overview of policy result statuses for Firmware and Configuration policy after remediation.
6. More Specific Policy Results:
   a) Firmware results may contain Passed, Failed, Warning, Aborted and Stopped
   b) Configuration results may be Passed, Failed and Warning

Installation

**ADDITIONAL DEPLOYMENT OPTIONS SUPPORT**

**Regional Support:**
Regional support is now available for the Netherlands. Please note, this is support for the Microsoft Windows® region, not the Dutch language.

**Database Support:**
Support for the SQL 2017 and SQL Azure database platforms has been added. Also, all versions of SQL Express have been removed from the CentreWare Web (CWW) installer and will not be installed automatically by the CWW installer. New CWW installations will be required to install a supported version of SQL prior to installation of CWW. Refer to the installation guide for more information.