Version 6.14
May 2024

Xerox® CentreWare® Web User Guide

xerox™

Document version: 6.14 May 2024

Images in this document may not be from the most recent release.

Date	Version	Description
05/13/2024	6.14	Added support for SQL Server®2022. No longer supports Windows Server® 2012 & 2012 R2.
10/15/2023	6.13	Removed support for COM+. Self-signed certificates for fleet orchestration of firmware changed to CA signed certificate. Replace references to EIP Weblets with Workplace Apps.
05/15/2023	6.12	Added support for TLS 1.3. Introduced a Password Policy feature to Enable Password Audit which uses a device's serial number as the admin password. Replaced McAfee references with Trellix. Set when power usage data is retrieved.
10/10/2022	6.11	Added additional details for device certificate management. Removed option for Historical Password Retries in password management. Cleanup Certificate options changed. Added notification options for security certificates.

Table of Contents

Introduction

Product Overview

CWW is a real-time control and monitoring application that can discover, install and configure, manage, monitor, and report on any type of SNMP-compliant printing device attached to an IP network, regardless of manufacturer. Operation of CWW is through the Web browser. As such, no client software is required for access to CWW, and any network connected PC capable of running Internet Explorer can be utilized.

The discovery of networked printers can be selected for specific subnets in an enterprise. CWW features a built-in alert detection system, and through customization of alert severity levels, has the capability to send an e-mail message to a specified recipient when user-defined conditions exist in the devices being monitored. CWW provides clear and concise status of all networked printers, with the ability to group printers in a way that best fits the network environment. Printer status conditions can be displayed and configured to meet specific account needs.

The application includes a number of functions that improve efficiency of your document output environment and potentially reduce costs, including:

- Device discovery

- Monitoring

- Remote diagnostics and troubleshooting

- Device configuration

  - Device configuration auditing and remediation

  - Firmware upgrades

  - Meter management

- Reporting

KEY BENEFITS

The key benefits of CentreWare Web include:

- Enterprise device management improves operational efficiency:

  - Delivers automatic email notification

  - Remotely installs, monitors, and manages your enterprise output environment

- Configuration Management, Auditing, and Remediation

- Remote Diagnostics and Troubleshooting

  - Proactive Monitoring

- Enterprise-wide print management:

  - Enables tracking and management of your paper and toner consumption

  - Creates and manages print queues and print servers

  - Manages local and network devices, ensuring you have no document output management blind spots

- Multi-vendor view of printing:
  - Makes accurate, timely, and informed enterprise device management decisions regarding all your local and networked devices
- Securely upgrade the Android Tablet Firmware on select WorkCentre Multifunction Printers.
  - Tablet upgrade files can be scheduled to deploy overnight to all discovered devices.
  - The upgrades can be stopped, restarted, and deleted as needed.
  - Upgrade status and Android Firmware level can also be viewed to determine the results of an Android Tablet upgrade.

Configuration Management

CentreWare Web enables remote, batch configuration management across multiple devices. Remote configuration capabilities include:

- Print protocol configuration: Allows enabling/disabling printing, as well as changing port numbers.
- Network parameters configuration: Allows remote configuration of various network parameters like DNS Server, WINS Server, Microsoft Windows, networking and IP address assignment.
- Network scan service configuration: Provides detailed configuration management for multifunction devices that support network scanning.
- Firmware Management: Configures and deploys firmware upgrades to an entire fleet.
- Configuration Policies: Offers auditing and remediation features for configuration.

Remote Diagnostics And Troubleshooting

When CentreWare Web detects a problem, remote troubleshooting capabilities allow you to access networked devices from any web browser to determine whether a repair technician is needed.

From a remote site, you can perform vital tasks, including: viewing local user interface messages, rebooting devices, performing ping tests, validating and updating network configuration, and observing current levels of consumables.

Xerox products provide meaningful, detailed, status information via CentreWare Web to enable business process optimization (e.g., status code for referencing, problem description, repair action, state of other MFP functions, etc.).

ENTERPRISE PRINT MANAGEMENT

CentreWare Web contains a comprehensive accounting capability that tracks user-based document output activity both on and off the network. Device usage patterns are represented graphically in Xerox Device Manager using a unique visualization tool. The tool utilizes a patented "affinity" algorithm for determining the relationship of levels of utilization in a specific selection of print devices.

MULTI-VENDOR VIEW OF PRINTING

CentreWare Web's network discovery capability identifies all devices operating on the network, regardless of manufacturer, as well as an extensive list of device attributes, including serial number, firmware level, color capability, network addressing, and more.

Use of filters can dynamically group and identify devices using a number of criteria, including network segment, location, type of device, and device function (i.e., finding all devices that are scan-to-email

enabled). The amount and detailed nature of the information obtained during discovery facilitates effective device management.

CentreWare Web communicates with and reports on a variety of device manufacturers, providing a holistic view of the status of your enterprise fleet.

Using this Document

This section describes the audience and additional resources necessary to use Xerox® Device Manager.

Audience

This guide is intended for all users that manage printers for the fleet.

Getting Started

Upgrading the Application

For this release, you may upgrade from the two previous major releases. To upgrade from an earlier release requires a new installation.

Upgrading

If you currently have a previous version of CentreWare Web installed, you first need to uninstall the application. You can then upgrade the application by obtaining the latest CWW installer from the Xerox Web site. Major releases can be upgraded without loss of historical data, configuration settings (e.g., discovery, polling), or user created groups.

Recommended: Back up your XrxDBCWW and XrxDBDiscovery databases from the SQL Server that the currently-installed CWW uses.

1. To upgrade from within the application, select **Administration > Advanced > Xerox CentreWare Web Updates**, or from a browser, access www.xerox.com/centrewareweb.
2. Click **Download**.
3. Choose your Operating System and Language, then click **Apply Filters**.
4. Click I Agree to the Terms and Conditions.
5. Click **Download**.
6. Follow the instructions to download the software ZIP file to your desktop.
7. After the download has completed, unzip the file and double-click on the EXE file to begin the installation process.
   a. When you get to the SQL Server section in the installation process, select Use Existing SQL Server, enter the SQL server name and the SQL Server User ID and password.
   b. When you get to the database section of the installation process, select Use Existing Database to ensure that any data you had collected in your previous version of CentreWare Web is upgraded and available for use once the installation is complete.

Checking System Requirements

This section describes the hardware recommendations and software requirements for the CentreWare Web server, as well as the device requirements for network and attached printers.

Verifying Hardware Requirements

Listed below is the minimum hardware recommendation for installing CentreWare Web on new equipment in a production server environment.

Hardware Requirement	Recommendations
Processor	Intel® Pentium® 4 processor at 3 GHz or Intel® Core 2 Duo (AMD-equivalent processors are also supported)
Memory	4 GB of RAM, with one of the following versions of SQL Server® installed on the same system: • 2014 • 2016 (Recommended) • 2017 (Recommended) • 2019 (Recommended) • 2022 (Recommended) • SQL Express
Server	Separate server with SQL® installed is recommended if: • The number of groups configured for concurrent status polling is greater than 20, and/or • The number of alert profiles is greater than 20, and/or • job data consumption is greater than 100,000 / week **Note:** If you install the application in the Azure Cloud on a supported operating system, you may use Azure SQL database. You may operate CentreWare Web off-premise in the Azure Cloud with Azure SQL. Routing protocols are in the Certification Guide.
Available Disk Space	Minimum: 3GB Recommended: 40 GB on 7200 rpm hard drive, if collecting historical data on thousands of devices

Examples: Below are our recommendations for hardware, operating systems, and SQL requirements.

Recommended Hardware Operating System And SQL Requirements:

For Installs < 5000 Devices:

• CentreWare Web on Windows Server 2016 with off-box SQL*

  - 2 CPU cores @2.9 GHz

  - 12 GB RAM

  - 40 GB free space (preferably on a non-system disk)

• CentreWare Web on Windows Server 2016 with on-box SQL/SQL Express**

  - 2 CPU cores @2.9 GHz

  - 16 GB RAM

  - 60 GB free space (preferably on a non-system disk)
    * Use the newest version of SQL acceptable to the customer.
    ** On-box SQL is only recommended for very small installations (< 200 devices)

For Installs > 5000 devices:

• Use an off-box SQL Server

• Increase memory by 50 %

• Add 2 CPU cores

For Installs 10,000 devices:

- One terabyte disk space
- 16 GB RAM
- Quad Core 3.4 GHz processor
- SQL Enterprise on separate server

If running on a virtual system, all resources need to be dedicated to CentreWare Web.

Note: If you need to install CentreWare Web on a rack-mounted server, the customer is expected to provide a keyboard-video-mouse terminal interface to the server.

Verifying Software Requirements

The following table describes the software requirements for the CentreWare Web.

Software Requirement	Recommendations
Operating Systems	Windows® 10
	Windows® 11
	Windows® Server® 2016 SP1 x64
	Windows® Server® 2019 x64
	Windows® Server® 2022 x64
	When installing on Windows Server® right-click the installer and select Run as Administrator.
	CentreWare Web does not support Windows® systems running on Macintosh® or non-NTFS partitions. Nor CentreWare Web support the NetWare client running on Windows.
	CentreWare Web does not support installation on a domain controller.
Web Server	Internet Information Services (IIS) 6.0 or above
	The software extension IIS URL Rewrite Modules is also required.
Internet Protocol	Working Microsoft® TCP/IPv4 Stack
Browser	Microsoft Edge browser based on Chromium
	Chrome
Access Components	Windows Data Access Components (WDAC)
	Note: MDAC changed its name to WDAC (Windows Data Access Components) with Windows Vista® and Windows Server® 2008. WDAC is included as part of the operating system and is not available separately for redistribution. Serviceability for WDAC is subject to the life cycle of the operating system.
Microsoft® .NET Framework	Microsoft®.NET 4.8
	Note: The Net Framework is not factory installed with CentreWare Web. You must install it prior to running the installation.

Software Requirement	Recommendations
Microsoft® Core XML Services	6.0 required for some of the application's functionality
Database Server	**Recommended:** Use SQL Server® Standard/Enterprise if available in the customer's IT environment.
	Note: If using a remote SQL Server, both the remote client on which SQL Server is installed and CentreWare Web server client require the Microsoft® Distributed Transaction Coordinator (MSDTC) service to be enabled and configured in order to allow remote client access. If a firewall is running, an exception needs to be created for the MSDTC service.
	When managing more than 5000 devices, we recommend that you install a Standard/Enterprise version of SQL Server® on a separate server. The requirements for the separate database server should match the requirements for the CentreWare Web server.
	Note: The application server and the database server must be set to the same time zone.
	If using an Azure SQL Services installation, the following components need to be installed and the server rebooted prior to installing CentreWare Web:
	• Windows Management Framework 5.1 (Windows Server 2016)

Verifying Network Printer Discovery/Monitoring Requirements

For successful management by CentreWare Web, all SNMP-based printer devices should support the mandatory MIB elements and groups as defined by the following standards.

Network Printer Discovery/Monitoring Requirements	Recommendations
RFC 1157	SNMP Version 1
RFC 1213	MIB-II for TCP/IP-based Internet
RFC 1514/2790	Host Resources MIB v1/v2
RFC 1759	Printer MIB v1
RFC 3805	Printer MIB v2
RFC 3806	Printer Finishing MIB
Optional: RFC 2271-2275	SNMP v3 Architecture

Checking the Systems Infrastructure

This section describes the systems infrastructure that must be in place to operate the CentreWare Web.

Using the Network Ports

CentreWare Web relies on a number of TCP/IP network ports (pre-defined by the Windows® operating system) to perform its activities. CentreWare Web features, network protocols, and ports with the data direction (related to the Xerox Device Manager server) are defined below.

CentreWare Web Feature/Function	Protocol	Port Number Used	Data Direction
• CentreWare Web Web page queries • Auto Driver Download • Cloning Wizard • Scan Template configuration set transfer • Troubleshoot • Configuration Sets	HTTP	80 but could be altered via IIS Administration	Incoming/Outgoing
• Secure CentreWare Web Web page queries • Secure CentreWare Web-to-Hosted data transfer • Upgrading Android Tablets	HTTPS	443	Incoming/Outgoing
• Secure CentreWare Web-to-Hosted retrieval of device specific licensing	HTTPS	8443	Outgoing/Incoming
• Secure CentreWare Web-to-Cloud Hosted auto-upgrade service	HTTPS	8443	Outgoing/Incoming
• Secure CentreWare Web-to-Cloud Hosted auto-upgrade service	HTTPS	8443	Outgoing
• Receive push notifications of printer status	SNMP v1 Trap	162	Incoming
• Network printer discovery using NetWare Server queries via IPX	SAP	452	Incoming
• Network printer discovery • Retrieval of capabilities, status & usage counters • Single device configuration • Configuration sets	SNMP V1/V2, V3 SNMP V1/V2, V3	161 but could vary depending upon OS port allocation 161	Outgoing/Incoming Incoming/Outgoing
• E-mail alerts	SMTP	25	Outgoing
• Printer discovery via Managed Server/Active Directory • Queue-based operations/diagnostics • Locally-Connected Printer discovery • Data synchronization	RPC	135	Outgoing
• Retrieval of computer properties	WMI over RPC	135 + random port	Outgoing
• Network printer discovery for non-SNMP-enabled printers	IPP	631	Outgoing
• Add/Delete Directory • Scan Service Configuration Set • Active Directory Customer Import • Customer Group Configurations	LDAP	389	Outgoing
• Troubleshoot – Print Test Page • Printer Firmware Upgrade	TCP/IP	515, 9100, 2000, 2105	Outgoing
• Managed Print Server • Computer property queries	NetBIOS	137, 139	Outgoing

CentreWare Web Feature/Function	Protocol	Port Number Used	Data Direction
• Network Printer Discovery Troubleshoot / [Test]	PING / CMP	none	Outgoing
• Hard coded for Remote Discovery	TCP	8105	Internal CentreWare Web uses to communicate with Scheduler
• Scheduler (Changeable string entry in the registry)	TCP	8085	Internal CentreWare Web uses to communicate with Scheduler
• Reverse DNS Lookup of discovered devices	DNS	53	Outgoing
• SIEM server connection	TCP, HTTPS	user defined	Outgoing
• Device Security Feed	HTTP	80 IIS Administrator may alter	Incoming/Outgoing

Ports and Protocols Used by CentreWare Web

Some customer environments could restrict the routing of ICMP packets across routers using an access control list to avoid denial of service attacks and worms from impacting their network. As a result, the following CentreWare Web features are adversely impacted:

- Troubleshoot Printers wizard
- Troubleshoot in Printers device view
- Add Printer in Printers device view
- IP Domain Scan for computers in the Discovery Administration tab
- Add Server in Queues device view
- Computer Queue Discovery

Using Windows® Service

The following Windows-based services are part of, or are used by, the application:

- Internet Information Service (IIS)
- Windows® Print Spooler
- Remote Procedure Calls
- Windows Management Instrumentation (for detailed computer information)
- SQL Server® Service

The following services are part of the application. These services automatically start when the system boots and restarts if stopped:

- Xerox® Discovery Service (device discovery and identification and SNMP trap monitoring)
- Xerox® Scheduler Service (automatic and scheduled background tasks, e.g., device polling, discovery)

Identifying Software Requirements

This section describes the requirements for PC access to the CentreWare Web web-served application.

Verifying Browser Requirements

Although the CentreWare Web server can directly browse to the application, it is sometimes necessary to access the application from a remote desktop. The supported browsers are Microsoft Edge (version 91 and above) or Chrome.

Note: The following must be loaded and operational:

• Transmission Control Protocol/Internet Protocol (TCP/IP)

Using SNMP Services

The Windows® SNMP Service installs an SNMP agent on the server and responds to SNMP-based requests for information. The Windows SNMP Service has several known security flaws (refer to the Microsoft's Security Bulletin MS02-006 referenced at http://www.microsoft.com/technet/security/bulletin/MS02-006.mspx

• WIN SNMP APIs are not used

Instead of using WinSNMP API to decode and encode packets, CentreWare Web uses the Xerox SNMP encoding/decoding mechanism.

The CentreWare Web SNMP communication infrastructure is completely .NET managed, and .NET runtime provides fundamental security benefits that include, but are not limited to, preventing invalid pointer manipulations, buffer overruns, and bounds checking. Do the following:

• Disable Microsoft SNMP service on the CentreWare Web server, unless there is a local requirement to use it. The Xerox Device Manager server is only at risk if the Windows® SNMP Service is installed and running.

• Disable Windows SNMP Trap service.

The SNMP agent service that ships with Windows® platforms is neither installed nor running by default.

• Enable the SNMP protocol. This feature might be disabled on several newer network printers as well. If this protocol is disabled, the CentreWare Web application is not able to discover the newer printers.

• Unblock the SNMP protocol. This feature might be blocked at the router level on one or more of the customer's subnets. If the SNMP protocol is disabled or blocked, the application will be unable to discover printers.

SNMP V3 Security Enhancements

SNMP is the most widely used in-band management protocol for communication among network management stations and the devices being managed. In its current form, SNMP's security is limited to three methods of access:

• Read-Only

• Write-Only

- Read-Write

Access from the management station (CentreWare Web to the devices is granted by community strings, which are the groups to which the devices belong). Although disabling the Write function can prevent most in-band attacks, SNMP is a relatively insecure protocol, with nothing more than the community strings acting as passwords.

SNMP V3 includes security and administration. The SNMP V3 framework supports multiple security models, which can exist simultaneously in an SNMP entity. SNMP V3 messages contain a field in the header that identifies which security model must process the message. To ensure some form of interoperability, a User-based Security Model (USM) is implemented to defend against unauthorized modification of managed elements and spoofing. Although SNMP V3 is a huge step forward in secure manageability, it cannot prevent denial-of-service attacks. In addition, its security system must stand alone, meaning every device must have a database of users/passwords. Since this is not likely to happen in most companies, all devices are at risk.

Please note that the more robust security provided by SNMP V3 can slow run times; this is especially true for printer groups with hundreds of devices. When managing large fleets of devices configured with SNMP v3, you may notice longer wait times or timeouts when utilizing large group sizes.

There are many factors that can affect response time including network bandwidth, topography, meter data sizes, device models, etc. For these reasons we recommend smaller groups when the communication technology is SNMP v3 vs SNMPv1/v2.

Recommendations:

- Xerox® Versalink® Devices – no more than 500 devices per group

- Xerox® Altalink® Devices – no more than 600 devices per group

- Xerox® ConnectKey® 2.0 Devices – no more than 500 Devices per group

Use the above group sizes as a starting point to find a group size that works best for your environment. If you adhere to these recommendations and still notice long communication times that result in timeouts, continue to reduce the size of the groups until the issue is resolved.

Setting Additional SNMP V3 Encryption and Authentication

SNMP V3 supports FIPS 140-2, which provides additional encryption and authentication methods. An Administrator can follow the steps below to enable this additional security.

1. Go to **Devices>Printers>New Printer** page.
2. In the Manual Printer Addition section, select discovery options for adding printer(s).
3. In the SNMP Access section, select SNMP v3.
4. Enter the User Name and Context Name.
5. Select the Authentication Mode from the dropdown (either MD5 or SHA1). We recommend SHA1.
6. Select the Encryption Method from the dropdown (either DES or AES128). We recommend AES 128.
7. Select Access Method and enter the corresponding authentication keys or passwords.
8. Press **Continue**.

Using Internet Information Services (IIS) Security

IIS requires particular attention in terms of security. Be sure to apply the latest service packs and critical updates available from Microsoft. It is also a good idea to run virus detection/removal software regularly on the server that hosts CentreWare Web.

Consider the following regarding IIS:

- Set Basic Authentication off
  You can configure IIS to send the user name and password in clear text. With basic authentication, the username and password are encoded, but are relatively easy to decode. When basic authentication is turned off, browsers must connect to these secure areas via Windows$^{®}$ authentication, which never passes the password on the network.

- Authenticated User Access to CentreWare Web
  Users in the following groups have full administrative access to CentreWare Web:

  - Administrators Group

  - CentreWare$^{®}$ Web Users Group.

    Unauthenticated users (anonymous) only have view privileges. They cannot modify any settings in CentreWare Web. You can modify the file permissions in the c:\program files\Xerox\Xerox Device Manager\ folder.
- Change HTTP port number
  Native IIS security features, such as changing the default HTTP port number, IP address restriction, and disabling anonymous access could be utilized to further lock-down the CentreWare Web server, if necessary.

Considering IIS Recommendations

Following are some ways that IIS security settings can be enhanced:

1. In IIS, modify the port number for the CentreWare Web server to something other than port 80. Port 80 is the default, and even simple viruses exploit that. Modify this via Properties on the default web site in the IIS snap-in. After changing this, the URL to connect remotely to Xerox Device Manager is http://<servername>:<port>/xeroxdevicemanager.
2. In IIS, restrict access to the web site to specific IP Addresses. Modify this via the Properties on the default web site in the IIS snap-in.

Logging In

Access to CentreWare Web is controlled through the User Login dialog. This page requires each user to enter credentials to gain access to the application. Application credentials include a valid User Name and Password, which may or may not be synchronized with your network/domain credentials.

Note: The application supports Single Sign On using Security Assertion Markup Language (SAML) v2.0. When logging in with SAML enabled, the user will have to supply credentials to an IdP interface, which will validate the credentials & send a SAML response to CentreWare Web.

Restricting Users and Groups

CentreWare Web restricts access based on the roles assigned to Windows® users including:

- Administrator—used during the CentreWare Web installation and remote discovery procedures
- Power User—used during print management activity
- User—used for local discovery, view-only display and reporting

Important Privacy Note: User names and passwords are not sent over the network.

If a username is provided at installation, that user is authenticated and placed in the local Administrators group. If the user remains in this group only, she/he is able to manage any network-connected print servers, but only local printers and queues.

Restricting CWW-Specific Groups

Access restriction is dependent on the groups to which the user is assigned. CentreWare Web creates CWW user groups during the install that grant members specific rights to the application.

- **CWW Administrators** group—Grants full administrative permissions to members.
- **CWW Power Users** group—Grants print management permissions to users in environments where sysadmin privileges would neither be required nor desirable. Members of this group can:
  - Create/Edit/Delete reports
  - Edit and Modify Traps
  - Edit Printer/Protocol/Scan Properties printer action
  - Apply Configuration Sets/Check Compliance
  - Troubleshoot/Reboot faulted printers
  - Perform printer group administration
- **CWW SQL Users** Group grants rights to run the CentreWare Web application instead of using the Network Services account.
- **CWW Configuration Set Admin** performs all actions on configuration sets and can edit printers, troubleshoot, and reset printers.
- **CWW Edit Device Admin** edits printers, troubleshoots, runs configuration sets, and resets printers.
- **CWW Report Display/User** has limited access to the Reports tab and may view and send reports.
- **CWW Report Edit / Admin** performs all action on reports.
- **CWW Users Members** in this group are granted rights to access the Device Groups if they are a member of that Group.

To add users to any of these groups, you must use the Windows User management workflow.

1. On the Windows server, navigate to **Control Panel > Users and Groups**.
2. Select the user group you want to modify.
3. Add the users or domain groups.

Providing Access to User Group Restricted Content

Users can only view the content of the device groups they are permitted to access. In CentreWare Web, administrators can restrict access to a device group to specified Domain User Groups.

Note: This restriction does not apply to CWW Power Users or CWW Administrators.

By default, this feature is disabled. Navigate to **Administration > Advanced > Preferences and Properties >Group Level Permissions.** CentreWare Web uses the configured RunAs Account to configure and access domain groups. If your configured RunAs user does not have domain access, you will not be able to browse or select other groups.

To grant a user access to Devices in a Device Group:

1. Add any users who need access to a group into the CWW Users Windows group. You may want to add Domain Users to the CWW Users group to identify all domain users as a CWW user rather than doing so individually.
2. On the **Printer** tab, select the group you want users to access.
3. Select **Group Actions > Configuration > Configure**.
4. Under Advanced, go to the User Access section.
5. Select **Actions > Add.**
6. Select the domain groups you want to have access to the group.
7. Click **Add.**
8. Click **Save**. All the users in the domain group now have access to view the printers in that group.

When accessing the Printer tab, the user is asked to authenticate if their current credentials are not part of the CWW Users group on the CentreWare Web server. After authentication, the user sees all the built-in groups and any custom groups for which they have permission. Even though the user can see all the built-in groups, they can only see the content if they have permission for a group.

Checking the Windows® Firewall Status

Certain Windows Firewall settings are required to allow the server to be added as a managed print server, which allows the application to get basic properties from any computer discovery. To retrieve additional detailed computer properties, you must disable Windows Firewall.

To check the configuration of the Windows Firewall software:

1. On Windows Server® select **Start > Control Panel > Windows Firewall.**
2. Click **Change Settings**.
3. Click the Exceptions tab.
4. Enable the File and Printer Sharing program.
5. Click **OK**.
6. Select **Start > Administrative Tools > Windows Firewall with Advanced Security.**
7. Select **Inbound Rules**.
8. Verify that the File and Printer Sharing (Echo Requests) are enabled. The correct enabling should happen when you enable the File and Printer Sharing Exception.

Locking the Session

When a session is inactive for a certain amount of time, the application times out. The default time out value is 15 minutes. When this period has elapsed, you receive a message that your session has ended. You may return to the home page and may be required to sign in again.

Configuring CentreWare Web

Overview

After you complete the installation process, you need to configure the preliminary settings, including:

- Specifying the Site / Administrator information
- Selecting the discovery method and schedule
- Selecting SNMP communications
- Selecting hours of operation
- Defining Alert methodology—local e-mail from Xerox Device Manager.

Additional activities might include:

- Defining custom properties to capture site-specific information
- Defining machine firmware upgrade processes
- Managing print devices with Configuration Sets and Policies
- Generating reports
- Viewing application logs

These processes are described in the following sections.

Running the Getting Started Wizard

The Getting Started Wizard runs when CentreWare Web is first installed and configures the number of printers to find, the outgoing mail server, and proxy server.

After you complete the installation process and licensing, you must configure the preliminary settings described earlier. The Getting Started: Completed screen summarizes the three settings configured during the Getting Started wizard and their status, if applicable. This wizard reappears each time you start the application. You can disable this feature by checking Hide this wizard on startup.

Specifying the Site/Administrator Information

Prior to establishing operation of the CentreWare Web application, you must specify the Site/Administrator Information for your installation.

- **Site Name:** Descriptive name for location of this site.
- **Account Name:** Name of the account.
- **Name:** The name of the administrator for this instance of the CentreWare Web server.
- **E–Mail:** The e-mail for this administrator. Status messages regarding the server or external contacts can reference the administrator through this e-mail.

- **Phone:** The phone for this administrator.

- **URL:** An appropriate URL (beginning with http://), if required.

- **Location:** Location for this server.

- **Comment:** Text comment.

When completed, the Administrator information displays on the Home screen for the CentreWare Web server. Links on the left side (Site Name, Account, etc.) link back to the Administrator tab, Site/Administrator screen. The name links to the URL, if supplied above, and the e-mail is a mailto link, and starts an e-mail message if e-mail is configured on the client.

Using the Quick Configuration Wizard

Quick Configuration is useful as a quick test to confirm the basic network requirements for available CentreWare Web discovery operations, and a way to discover IP subnets on a network if you do not have firsthand knowledge of the company's IP subnet infrastructure. Because Quick Configuration explores several router levels to find device addresses, it can be more of a nuisance than a valuable technique. Because some settings are implied rather than explicitly set, this method is not recommended for daily operations in a full production environment.

Note: Quick Configuration is a useful tool, but it is not recommended for normal production operation. Configuring CentreWare Web from the Administration tab allows full access to e-mail and proxy server configuration, as well as providing more options for device discovery.

You can configure CentreWare Web to perform an initial device discovery to load into the database and the frequency at which the status polling is to be performed. The range varies between not discovering any devices and no status polling, to maximally discovering any device possible and fetching status on the discovered population every 6 hours.

The Quick Configuration tool consolidates the mechanisms of IP subnet scan and IP sweep into a single process. With this method, device discovery is driven by the subnet information stored in the customer's network routers, where the subnets know which routers are used to sweep definitions for discovery. Before running this discovery, contact the network support staff and exclude sensitive addresses. This is particularly important when scanning all subnets within the firewall.

There are three modes of operation. Simple and Intermediate rely on graphic sliders to provide input information for the discovery process; Advanced provides a more descriptive access to the CentreWare Web discovery process. When the Quick Configuration discovery method is running, you can observe its progress from the Network Usage Summary screen.

Since the first part of this method is to perform an IP subnet scan, the first half of this discovery method is only as accurate as the ARP Cache maintained by network routers. Furthermore, the number of detected IP subnets depends on the SNMP community names used by routers configured on the SNMP v1/v2 screen. If the SNMP community name is not known by CentreWare Web, those IP subnets are not detected by this discovery method.

Since the subnet scan yields sufficient subnet information from the router, the second half of this operation sweeps the obtained subnets. Subnet sweep discovery is considered a more reliable way to discover printers, because a packet is sent to each IP address in the obtained subnets, regardless of whether or not an actual device exists at an IP address. Packet collisions are minimal, depending upon the amount of traffic on the network, which enables CentreWare Web to detect each printing device that responds to the initial sweep packet.

Impacting the Network

The amount of traffic generated by IP Easy Discovery is the combination of the subnet scan and directed sweep discovery operations. The traffic by the subnet scan-based portion is less than the SNMP-based ARP cache discovery method, since the traffic is directed towards network routers exclusively. Since only these routers are queried for live IP addresses, the network traffic is minimal. For the sweep portion, the amount of network traffic generated is minimized because the requests are directed to specific IP addresses. Typically, the impact to the network is barely noticeable, although you can see a steady stream of packets.

Setting SMTP and Proxy

If not already set from E-Mail & External Servers, Quick Configuration displays screens to configure the e-mail and proxy server connections.

Configuring E-Mail Server

The Quick Configuration process supplies the default port for SMTP (25) and the default encoding (utf-8), but you can change these if required.

To change the settings:

1. Enter the mail server SMTP address or DNS name.
2. Click **Test Connection** to confirm that the server is visible. If Test returns an error condition, the returned message should help in correcting the problem.
   Note: The SMTP server sends e-mail alerts, reports, and server status messages. Use the From E-Mail Address when you send these messages.

3. If SMTP security is required, complete this section. The Test E-Mail Destination allows a complete simulated test for e-mailing from CentreWare Web. Typically, use your own e-mail address for this test.

Configuring Proxy Server

The CentreWare Web server attempts to detect the designated Proxy server for this network. Uncheck the User Proxy Service option if it is not required for access. Test attempts an outgoing connection to http://www.wb.xerox.com using this proxy server.

1. If Proxy security is required, complete this section.
2. Click **Test Connection** to confirm that the server is correct. If Test returns an error condition, the returned message should assist in correcting the problem.

Using the Interface

Overview

This section provides a brief overview of how to navigate through the CentreWare Web. For detailed information about the various functions available with CentreWare Web, see the individual chapters.

Exploring the Tabs

The following tabs provide access to the features of the software.

- Dashboard: Gain quick access to system statistics, graphs, and policy compliance information.
- Policies: Configure and schedule device, password, and firmware policies.
- Devices: Manage and view devices for your deployment.
- Wizards: Configure and deploy various options for you fleet.
- Reports: Generate and view reports about your system usage.
- Administration: Configure system settings, manage users, and manage groups.

Using the Icons

The table below describes the various icons shown in the CentreWare Web. In the rest of this document, the icons are not shown, they are spelled out.

	OK: Printer status is up and running or action was successful.		Display Icon: Display details or properties screen.
	Warning Non-catastrophic device status or action produced a warning.		Edit (pencil) Icon: Edits properties.
	Error: Attention is required or action failed.		Delete Icon: Delete selected item.
	Unknown: Status from device is indeterminate.		Important Icon: Information important to know, but not harmful.
	Table Preferences: Selects items from a table list.		Check-box Icon: Option selection
	WebUI: Direct link to the device WebUI (if available)		Remote Web: Direct access to the Remote Web interface for the device

Using the Device Management Dashboard

The Device Management Dashboard offers a graphical overview of device health and compliance to both administrators and customers. In order to access the dashboards, a customer must be part of the CWW Users group and the Customer Report User group.
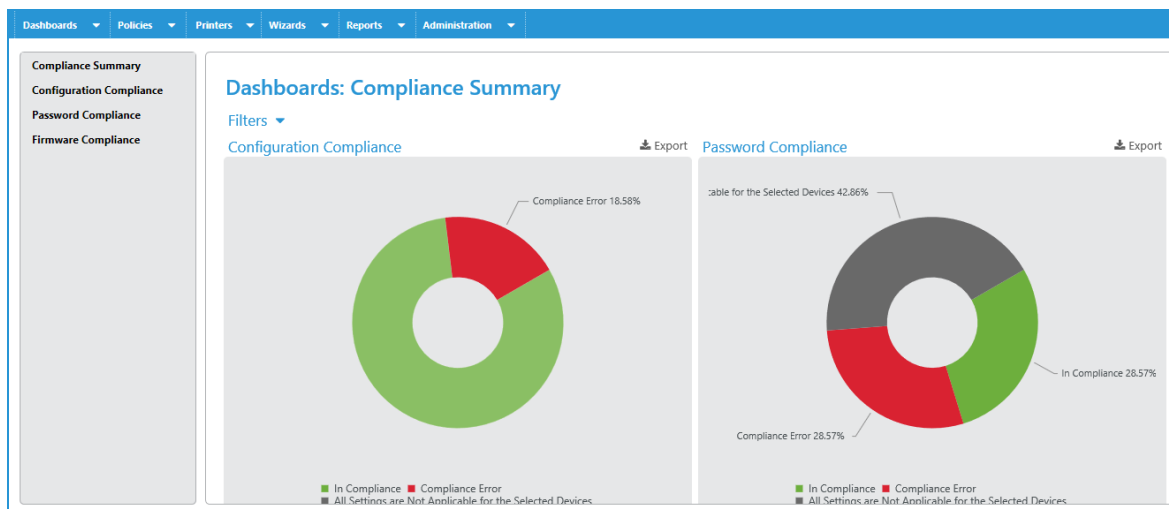
The navigation pane (on the left) lets you move through the dashboard views for configuration, firmware, password policies, and security monitoring. Go to the Compliance Summary view for the overview of your policy compliance and overall device health in all these areas. For greater detail navigate to the specific dashboards or drilldown into the graphics. When you click on a status in the Overall Device Health chart, the print grid opens and is filtered by the status you clicked.

The right pane displays dashboards and tables in which you can find details about policy compliance. The Dashboards show compliance information that you can filter to get additional details. How to interpret the dashboard is discussed in greater detail in the Managing Devices section.

Viewing the Printers Options

The Printers tab is the most often used and consists of:
- Group Selection Menu
- Navigation Pane
- Printer Actions
- Group Actions
- Table Grid

Selecting the Group
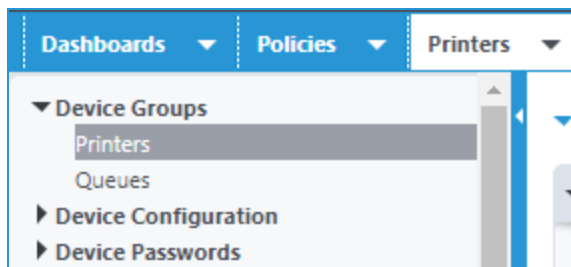
The available groups are described in the table below. The options change, depending on the group that is currently displayed.

Group	Description
Printers	Displays any discovered printers on CentreWare Web. This is the default view.
Queues	Displays any known queues on CentreWare Web-managed servers.

For the purpose of this document, we will stay in the Printers group.

Using the Navigation Pane

The Navigation pane displays the various options available when you make a selection in the Devices groups; in this case, the Printers group.
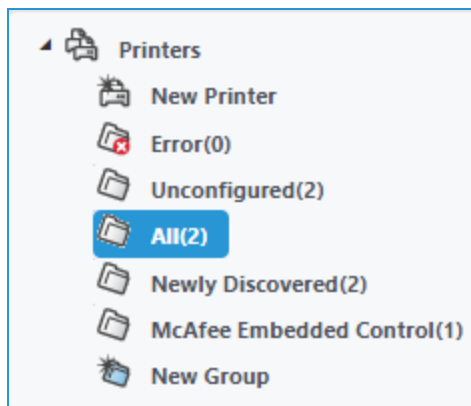
Following is a description of the options displayed when you select the Printers group.

Menu Item	Description
New Printer	Manually establishes a new printer in CentreWare Web. This bypasses the Discovery activity and might be used if a new printer needs to be added sooner than the next scheduled Discovery.
Error	Contains those devices that display the Error status icon
Unconfigured	Contains those devices for which a Queue is not defined.
All	Contains all discovered devices, regardless of state.
Newly Discovered	Contains newly discovered devices, regardless of state.
Trellix Embedded Control	Contains all discovered devices with Trellix security software.
New Group	Initiates the dialog to create a custom device group.

Using the Action Menus

There are two Action menus.

• Printer Actions

• Group Actions

These menus are described in this section.

Printer Actions
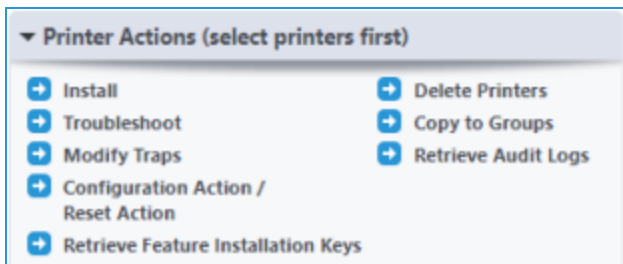
Most of these selections provide Printer Action options similar to those described in the following table. Before selecting one of these options, you must select a device from the Table Grid described in Using the Table Grid.

Action	Description
Install	The selected printers are installed as print queues on the selected server. This option is not available in the All group.
Troubleshoot	CentreWare Web attempts to perform some basic network and print operations on the selected printers to provide a preliminary diagnostic.
Modify Traps	Print device status can be requested by CentreWare Web on a scheduled basis by polling devices (synchronously) or be sent unsolicited (asynchronously) from the print device itself by means of a trap.
Configuration Action/Reset Action	Schedules a configuration task to audit/apply configuration information to devices using a Configuration Set, or to schedule a reset of the selected devices.
Retrieve Feature Installation Keys	Calls the Licensing Server to obtain the Feature Installation Keys (FIK) for the selected devices. The communication is logged in the Action Log. This is available to administrators only.
Delete Printers	All device data, history and page metrics are completely erased from the database, for the deleted devices. This option is not available in the All group. Use extreme caution when making this selection.
Copy to Groups	Copies the database index for the selected printers to the selected groups.
Retrieve Audit Logs	Pulls the device audit logs on newer devices that have the Trellix feature.

Group Actions
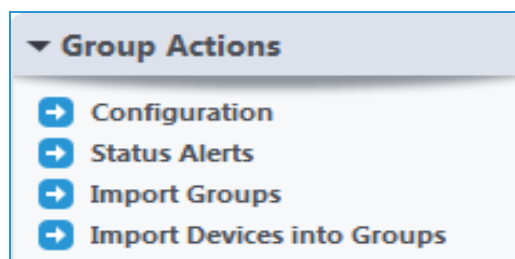
The Group Actions pane offers the actions available for the selected Group, as opposed to individual printers. Like the Printer Actions menu, they vary for different Groups.

Action	Description
Configuration	Allows you to configure the group, set the Identity, configure status polling, and modify the group membership.
Status Alerts	Allows you to configure Status Alert Profiles, selecting what alerts to send and where to send them.
Import Groups	Allows you to import multiple groups (including nested groups) using a CSV file. Furthermore, it allows group membership filters to be added to groups using a different CSV file.
Import Devices into Groups	Allows you to import Devices into groups. You can also add devices to existing groups via a CSV file. If a device does not yet exist in the system, then the system will perform a discovery for those devices

The preconfigured groups (e.g., All, Newly Discovered, Error, etc.) permit only Configuration and Status Alerts group actions.

Using the Table Grid

The Table Grid displays the results of the selection made in the Navigation pane. To change the fields that display click Table Preferences above the grid. You must select a device from the grid before making a selection from the Actions menu described above.

Viewing the Wizards Options

You can select a wizard from one of two methods on the Wizards screen:

• Select from the menu on the left, which provides only the name of the Wizard.

• Select from the pane on the right, which provides the name and description of the Wizard.
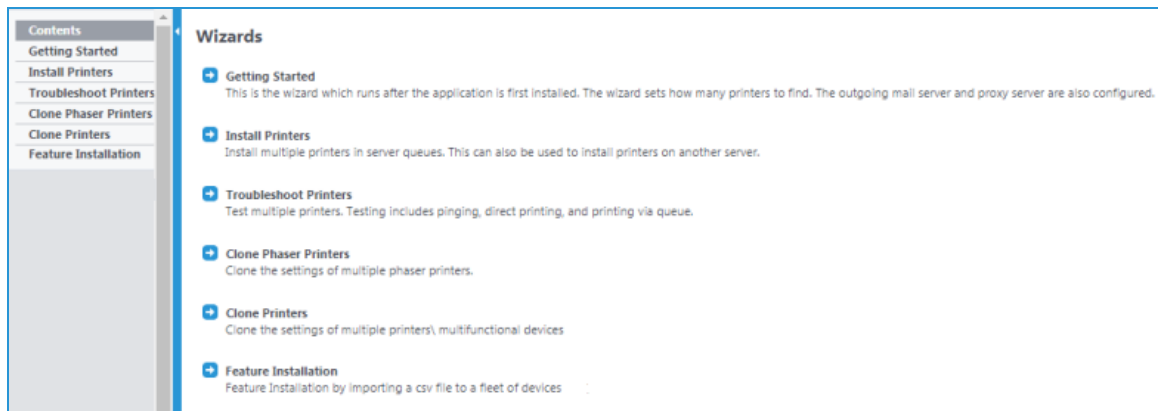
For a complete description of the Wizards feature, see Using the Wizards for Miscellaneous Tasks.

Viewing the Reports Options

The Reports tab is slightly different than the Wizards tab.

- Select from the menu on the left to display the reports associated with that selection.
- Select from the pane on the right to generate the actual report.
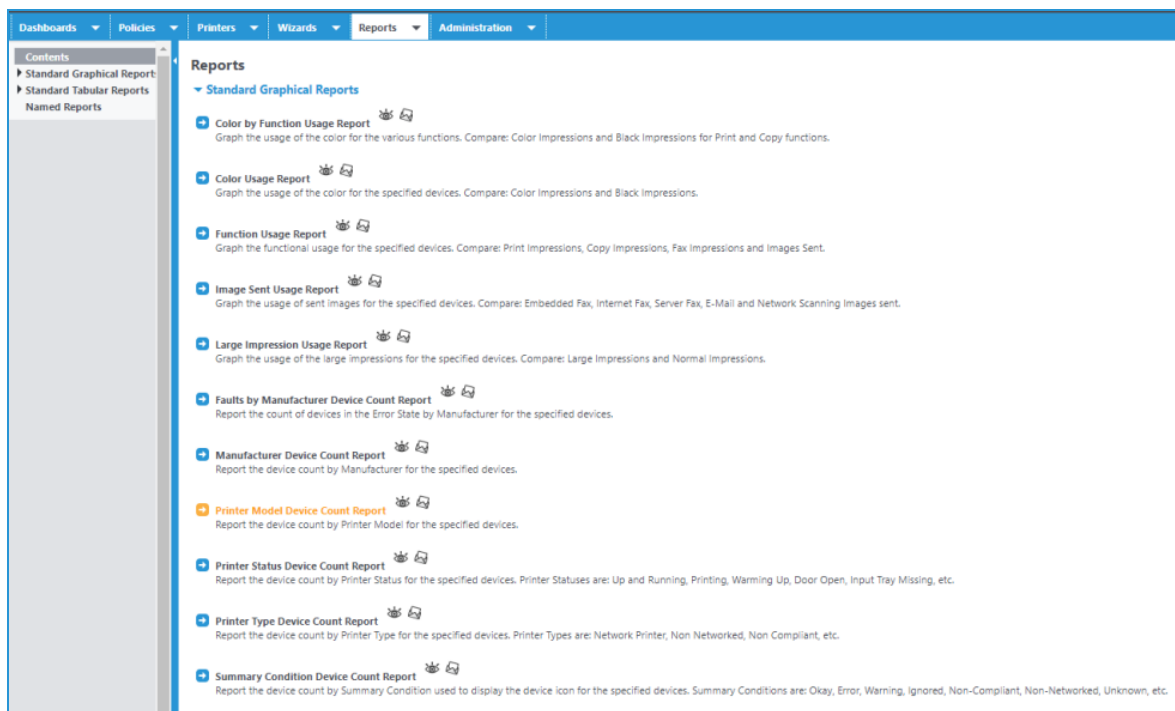
For a complete description of the Reports feature, see Reports Overview.

Viewing the Administration Tab

The Administration tab is similar to the Reports tab.

- Select from the menu on the left to display the administrative tasks associated with that selection.
- Complete the required information in the pane on the right.
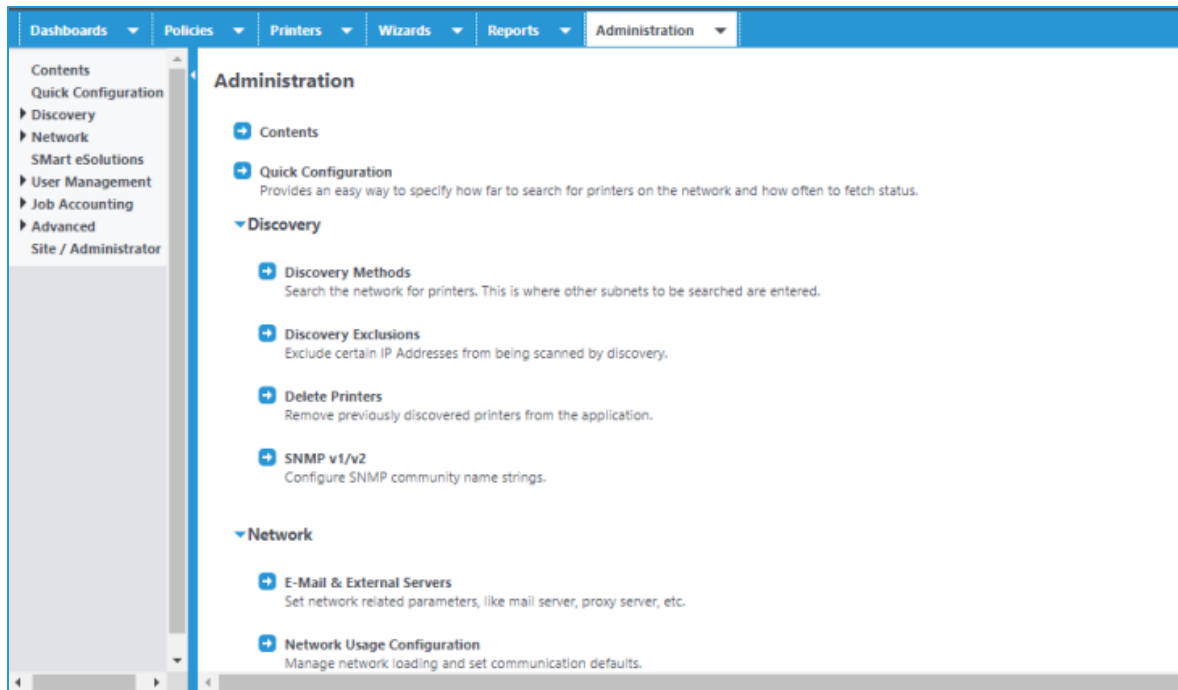
For a complete description of the Administration feature, see Performing Administration Functions.

Using Discovery

Overview

Use the Discovery function to identify printers wherever the application server is connected on the network. Discovering a device consists of a series of steps that query specific network addresses for device type and information about its configuration via SNMP. You can schedule this process to recur at a set period. You may also configure the discovery process to exclude IP addresses.

Although you can perform the network address selection and device identification querying in parallel in some Discovery methods, we recommend creating separate discovery methods to keep these activities separate. You can obtain these addresses by a:

- Manually entered or pre-defined list (.csv file) of addresses

- Manually entered or pre-defined list (.csv) of subnets

- List generated from a broadcast message

- List generated by interrogation of devices with routing tables

Device discovery is essential to identifying and storing networked devices in the database. Since this procedure extensively uses network resources, you should consider customer's expectations regarding device detection and monitoring and minimizing network contention. As a rule of thumb, each discovered printer can generate as much as 200 Kb of network message traffic. This is fairly trivial when compared to typical network-based message traffic, except when thousands of devices are polled fairly frequently.

CentreWare Web and IPv6

CentreWare Web supports the IPv6 communication protocol, which manages devices in IPv6 environments. There are, however, some differences in the behavior of CentreWare Web with IPv6 vs. IPv4.

For IPv6, CentreWare Web can:

- Communicate with devices via IPv6

- Import a file of IPv6 addresses for discovery

For IPv6, CentreWare Web cannot:

- Automatically discover devices on the network with only IPv6 addresses

- Support Queue management of IPv6 addressed devices

Following is an example of the impact of device discovery to the network infrastructure.

Example Of Discovery Network Impact

In this example, we will assume:

- There are 1000 network printers to be discovered in the customer's intranet.

- The total number of bytes transferred between CentreWare Web and the networked printer is approximately 200 KB.

Note: We will ignore the fact that some network address will not respond to the printer querying, and some customer networks are not completely filled with active devices.

- The local account team is responsible for managing all networked printer devices

- In some cases, customers can move, add, and remove devices from the network without Xerox local account team involvement.

This means that:

- The Xerox account team must discover these changes using the Discovery function

- It is agreed to by both parties (customer and Xerox) that the Discovery process be executed once a week during after hours.

The calculation for the network bandwidth loading for this monitoring is as follows:

1,000 printers x 200 KB/printer = 200,000 KB or 200 MB per discovery

This amount is equivalent to downloading several large (image intensive) documents or presentations. If either the discovery procedure frequency or the number of printers in scope increases, monthly traffic loading increases accordingly. A consensus decision between the customer IT department and the Xerox managed service account team, therefore, is necessary as part of the deployment of Xerox Device Manager in the customer's network intranet.

Selecting a Discovery Method

When selecting the discovery methods, the customer must consider the portions of the customer intranet that should be monitored and by which discovery means, as well as which portions should be excluded from the discovery process, if any. Lastly, if the SNMP Community Name Strings for the customer's printers have been set to anything other than public or private (the default Community Name Strings), the discovery methods must include these Community Name values.

CentreWare Web provides multiple IP- and IPX-based discovery methods.

To configure a discovery method, do one of the following:

- Select the New Discovery from the Discovery Methods webpage.

- Edit an existing configured discovery method and set the appropriate options.

By configuring subnet and IP-address information, you can tailor Discovery to find individual printers or specific groups of printers. You can also specify the frequency, date, and time for scheduling automatic Discovery.

Before beginning any large scale Network Discovery, we recommend you communicate with the customer's IT network support staff. Large amounts of sweeping traffic can trigger alarms from some versions of network security monitors.

The following sections describe the different Discovery options in CentreWare Web.

Using the IP Easy Discovery Method

The IP Easy Discovery method:

- Provides printer discovery with minimum user intervention.

- Is invoked from the initial Quick Configuration

- Consolidates the mechanisms of IP Subnet Scan and IP Sweep into a single process.

- Drives device discovery by the subnet information stored in the customer's network routers, where the subnets known by the routers are used to sweep definitions for discovery.

Before running this discovery, contact the network support staff and exclude sensitive addresses. This is particularly important when scanning all subnets within the firewall.

There are three modes of operation – Simple and Intermediate rely on graphic "sliders" to provide input information for the discovery process; the third (Advanced) provides a more descriptive access to the discovery process.

You can specify Subnet Scan methods in terms of the number of Hops the scan is limited to (i.e., restricting the scan to a specific number of hops or all subnets within the firewall).

Note: Zero (0) hops means that the search is limited to the local subnet. Also, be sure to configure IP Exclude before using the All Subnets in the Firewall option. This prevents IP Easy Discovery from communicating with all subnets within the firewall.

Using the IP Broadcast Method

The IP Broadcast Discovery method is:

- A quick and easy method of populating the CentreWare Web database.

- Considered less reliable than the Sweep discovery method (described below) because of the burst of response packets generated as a response to the broadcast. A sharp spike in network traffic usually occurs when these devices all respond at once, which create packet collisions. A single packet is broadcast to every subnet or IP address range defined within Discovery's subnet list specification.

Depending on the customer's network complexity, it may be advisable to adjust the Subnet Timeout value in the Advanced settings of this Discovery method.

Using the IP Sweep Method

The SNMP Sweep Discovery method (IP Sweep) is:

- The preferred method of accurately discovering printers on a network.

- Results in a more controlled and orderly flow of data between printers and CentreWare Web (unlike the Broadcast method). A packet is sent to every IP address in the user-defined subnet or address range list. The amount of network traffic generated by a sweep-based discovery is minimized because the requests are directed to specific IP addresses.

Depending on the customer's network complexity, it may be advisable to adjust the Timeout value per printer setting in the Advanced settings for this method. The recommended Timeout per Printer setting is five seconds and the recommended Retries setting is 1.

With IP Sweep Discovery, you can add the Internet Printing Protocol (IPP) as a last resort during device querying, in the event that the device fails to respond to SNMP v1/v2 queries. By selecting this option, the Discovery process may experience significant delay in completing the sweep operation, and could introduce additional network traffic.

Note: Routers can block or disable the ability to answer SNMP requests on some printers.

When discovering computers, you can select whether or not to use WMI queries through RPC communication to computers that do not respond to ICMP pings. If not enabled (set by default), those computers that do not respond to an ICMP ping are considered "disconnected" and the discovery method moves on. Routers can block the ability to answer ICMP Ping requests or disabled at the computer. By

adding the WMI interface to the Discovery method, more computers are found, but at the possible cost of additional network traffic due to the WMI RPC calls.

Configuring IP Sweep Discovery

Use the following procedure to set up an IP Sweep Discovery.

To set up a discovery.

1. Select **Administration > Discovery > Discovery Methods**. The Discovery screen displays.
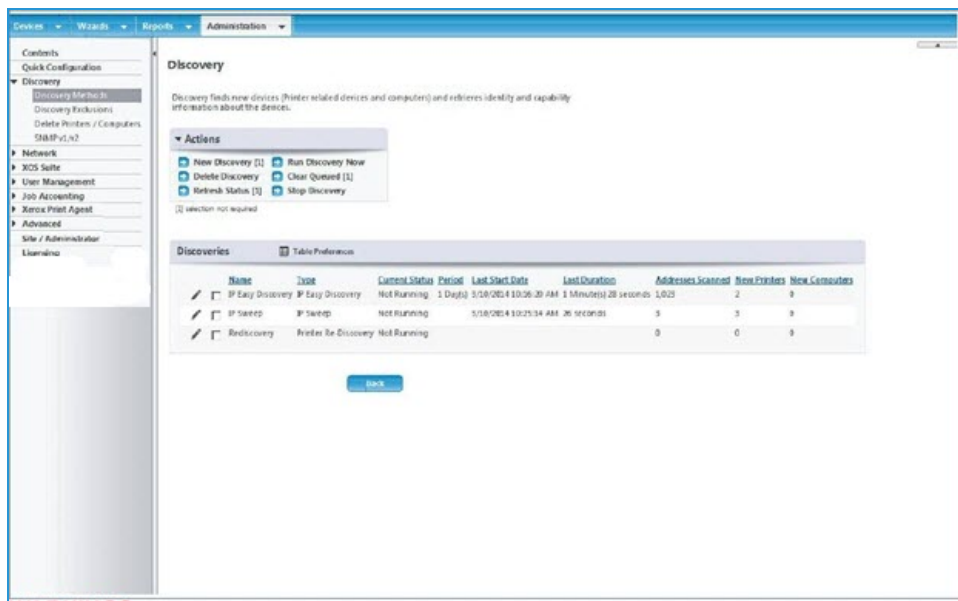
Note: The Actions pane specifies actions to create or modify an existing discovery, while the Discoveries pane lists any existing discoveries. IP Easy Discovery (Quick Configuration) is always listed.

2. To create a new IP Sweep, select Actions > New Discovery. The Discovery Types display.
3. Enter a name for the discovery in the Name field.
4. Select the radio button for the correct Discovery type.
5. If there is an existing discovery to use as a template, select from Currently Defined Discovery. Otherwise, use Blank Discovery.
6. Click **Continue**.
   - Selections are similar between different Discovery types.
   - There may be information displayed regarding the data retrieved from the last time this Discovery method was run.
   - Since this is a new Discovery, any existing computers or printers reflect the results of other discoveries.

   The Discovery name and type display.
7. If appropriate, schedule the Discovery to repeat at a specific frequency (every x days, weeks or months), starting at a particular date and time.
   Note: Selecting Never means to run on demand when you select **Actions > Run Discovery Now**.
8. For the selected IP Sweep, enter IP addresses:
   - One at a time as a Single Address or DNS Name
   - As an address range (e.g., addresses starting at 13.10.20.7 and ending at 13.10.20.18)

- As a subnet, enter a single address and the Mask, and the IP segment is defined

- As a subnet from the list generated from an IP Subnet scan.

  Note: Any number or combination of these entries is allowed.

9. Click **Add**.The values are added to the scan list in the Current IP Addresses box. (Add Local adds the sub-net of the CentreWare Web server.)

10. Select the appropriate Subnet Mask.
    Note: The default is 255.255.255.0.
    If the site has a list of IP addresses or DNS Names, you can import them as a csv file, which conforms to the specifications noted.

11. Click **Import**. The File Import screen displays.

12. Click **Browse** to locate and select the file.

13. Click **Save** to import.

14. From the Advanced section, specify a specific Timeout and Retry count. For successive SNMP requests (all but Broadcast), the timeout period is the wait time after each request is made. The Retry count repeats the SNMP request for the number of times specified. (A starting value of 3-5 seconds for Timeout and 1 Retry is a reasonable starting point.)
    Note: For Broadcast, the Retry count repeats the entire Broadcast.

15. Select Printers to use IPP to catch devices that do not respond to SNMP v1 or v2.

16. When selections are completed, click **Save**.

   Note: You can configure up to 11 separate and distinct IP Sweeps.

   Note: Returning to the Discovery screen, you can select the Discovery to run now or wait for the scheduled time to start.

   - To run now, check the box by the discovery, and click Run Discovery Now. The Status changes from Not Running to Running and a Progress button appears.

   - Click **Progress** to show the current status of the sweep.

   - To stop a discovery, click **Stop Discovery.** This leaves an uncompleted discovery queued.

   - To remove a queued discovery click **Clear Queued** or click **Delete** to delete the Discovery.
     Note: Some sites may allow IP Sweeps or Broadcasts for Discovery, but only if certain IP ranges are excluded.
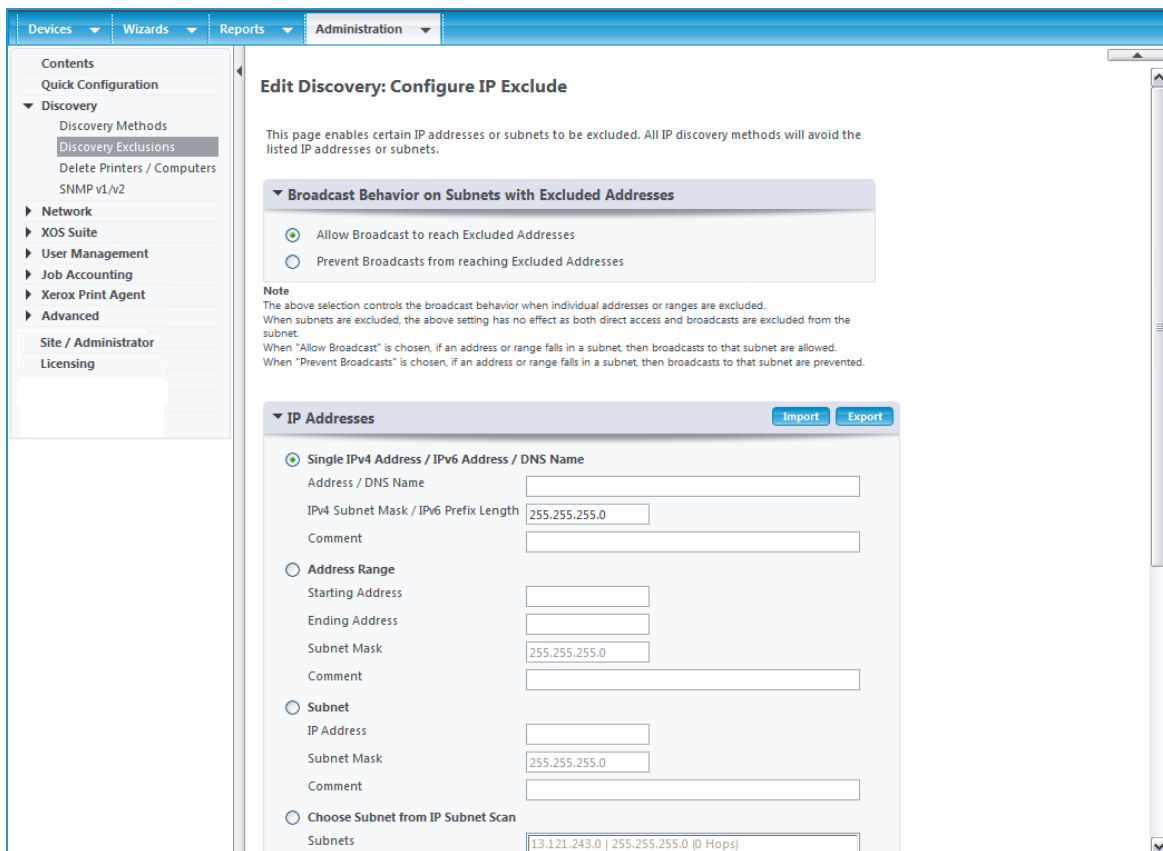
Discovery Exclusions allow you to specify Addresses, Ranges or Subnets, in the same fashion as selecting the same for the IP Sweep. Additionally, you can modify Broadcast behavior, if required.

- Some methods are specified in terms of the number of Hops to which the scan are limited--restricting the scan to a specific number of hops or all subnets within the firewall.

- Zero (0) hops indicates that the search is limited to the local subnet.

- The ability to answer SNMP requests can be blocked by routers or disabled on some printers.

- IP Sweep and IP ARP Cache provide you the ability to add the Internet Printing Protocol (IPP) as a last resort during device querying, in the event that the device fails to respond to SNMP v1/v2 queries. With this option, the Discovery process might experience significant delays in completing the sweep operation, and could introduce additional network traffic.

- When running automated remote device discovery over a REST Service, if you have multiple CentreWare Web services, you must configure a discovery exclusions list.

- It is a good idea to check the completion status of the Discovery to determine if the number of devices discovered is reasonable.

  - If it is much higher than expected, you might be scanning more addresses than you thought you had specified.

  - If it is much lower, you might not be including all address ranges or the discovery is blocked at a router

  - A very high value may imply that the Timeout and/or Retry count is too high. Check the duration of the Discovery.

Using the SNMP v3 IP Sweep Method

The SNMP v3 IP Sweep:

* Is the most reliable method of finding devices configured to use SNMP v3.

* IP Address ranges are swept using SNMP v3 only.

The SNMP V3 Discovery method allows multiple SNMP V3 devices to be discovered at one time. You can set up a discovery method and import a csv file of device addresses, subnets, or ranges with the V3 credentials. You can schedule device discovery so that new devices added to the network with the same credentials are automatically added to CentreWare Web.

SNMP V3 is considered the most secure and whenever possible should be the selected method of communication. It uses authentication and encryption to provide enhanced security over what is supplied by SNMP V1/V2.

Note: Devices that are enabled for Federal Information Processing Standard (FIPS) may be discovered using SNMP v3; however, some steps must be taken prior to discovery. On the computer running CentreWare Web go to Administrative Tools > Local Security Policy > Local Policies and select Security Options. Enable the option for System Cryptography: Use FIPS-compliant algorithms for encryption, hashing, and signing. Reboot before logging in to CentreWare Web.

1. In CentreWare Web go to select Administration > Discovery > Discovery Methods.
2. Select New Discovery and enter the name of the discovery.
3. Select SNMP V3 IP Sweep as the Discovery Type.
4. Click **Continue**.
5. Enter the schedule for when the discovery will run and how often.
6. Import the CSV file with the desired addresses, subnets, or ranges with the corresponding SNMP V3 credentials. **Note:** A template is provided for the CSV file format.
7. Under Advanced, change the default values for timeouts and retries, if necessary.
8. Click **Save**.

Identifying SNMP Response Issues

Discovery connection errors could occur because a device is offline, etc. In order to track and resolve issues with discovery that are specific to SNMP access errors, the device status SNMP Access Denied is used. Any devices that are not responding due to SNMP-related issues fall under this category. Knowing that access is denied for SNMP authentication reasons can expedite resolution. Possible issues included in the SNMP Access Denied status are:

* Invalid Get Community Name

* SNMPV3 Wrong User Name

* SNMPV3 Invalid Auth Key

* SNMPV3 Invalid Privacy Key

* SNMPV3 Invalid Context Name

Using the IP ARP Cache Method

The SNMP-based ARP Cache discovery method utilizes similar concepts to those deployed by the Address Resolution Protocol (ARP).

The Address Resolution Protocol:

- Operates at the data-link layer to provide a mapping of IP addresses to physical machine addresses (MAC Addresses)

- Returns a corresponding MAC address when given an IP address.

- Implements a table, usually called the ARP Cache, on routers to maintain mapping of MAC addresses-to-IP addresses. This table is exposed via SNMP. Although ARP is not used directly, CentreWare Web queries a router's MIB-based ARP Cache to find live IP addresses that can then be queried to identify printers.

- Is not as reliable as the SNMP Sweep discovery method, because it is based on dynamic router information

Use the ARP Cache discovery rather than the SNMP Sweep method most often. Like the SNMP Broadcast discovery, it is a good method for obtaining a quick collection of printers on a network. The traffic generated by the SNMP-based ARP Cache-based discovery is less than an SNMP Sweep discovery because the requests are directed to only "live, known IP addresses" instead of every possible address within the subnet/address range. Typically, the impact to the network is barely noticeable, although a steady stream of packets is visible. Also, router usage-related logs could grow in size due this discovery method.

You can specify Subnet Scan methods to limit the number of hops the scan is limited to (i.e., restricting the scan to a specific number of hops or all subnets within the firewall).

Note: Zero (0) hops indicates that the search is limited to the local subnet. Be sure to configure IP Exclude before using the All Subnets in the Firewall option. This prevents IP ARP Cache Method Discovery from communicating with subnets within the firewall.

Depending on the customer's network complexity, you might want to adjust the Timeout value for each printer in the Advanced settings. The recommended Timeout per Printer setting is 5 seconds and the recommended Retries setting is 1.

IP ARP Cache Discovery configuration provides the ability to add the Internet Printing Protocol (IPP) as a last resort during device querying, if the device fails to respond to SNMP v1/v2 queries. With this option, the Discovery process might experience significant delays in completing the sweep operation, and could introduce additional network traffic.

Note: Routers can disable or block the ability to answer SNMP requests on some printers.

Using the IP Subnet Scan

The IP Subnet Scan discovery method does not find printers. Instead, it finds the IP subnets used for printer discovery. These IP subnets are available to SNMP Broadcast and SNMP Sweep methods. This technique is very thorough, and can therefore be very time consuming.

This discovery method is only as accurate as the ARP Cache maintained by network routers. The number of IP detected subnets is dependent on the SNMP community names used by routers that are configured on the SNMP screen. If the name is not known by CentreWare Web, those IP subnets are not detected by this discovery method.

The amount of traffic generated by an IP subnet scan-based discovery is less than the SNMP-based ARP cache discovery method. However, it is directed towards network routers exclusively. Since only these routers are queried for live IP addresses, the network traffic is barely noticeable.

You can specify subnet scan methods in terms of the number of hops to which the scan is limited to (i.e., restricting the scan to a specific number of hops or all subnets within the firewall).

Note: Zero (0) hops indicates that the search is limited to the local subnet. Also, be sure to configure IP Exclude before using the All Subnets in the Firewall option. This prevents IP Subnet Scan from communicating with subnets within the firewall.

Depending on the customer's network complexity, it might be advisable to adjust the timeout value per printer setting in the Advanced settings of this Discovery method. The recommended Timeout per Printer setting is 5 seconds and the recommended Retries setting is 1.

The subnets found during the last scan will be listed in the Subnets window.

Using IPX Printer Discovery Methods

CentreWare Web also allows you to discover printers using the IPX (Internetwork Packet Exchange) protocol. This networking protocol is used by Novell Netware network operating systems. To discover printers using the IPX protocol, utilize the IPX Servers or IPX Addresses features of CentreWare Web as discussed below.

Note: Access to the IPX based discovery methods are disabled (grayed out) when the IPX networking protocols are not installed on the CentreWare Web web server.

Using IPX Network Scan Discovery

The IPX Network Discovery mechanism finds NetWare® servers and IPX networks. This Discovery method does not find printers, but rather the Netware components (Netware Servers and Networks) that know where IPX networked printers are located. The results of this scan are returned and displayed on the IPX Servers and IPX Addresses Discovery configuration screens, making it easier to configure these Discovery methods. It is recommended that you perform the IPX Network Scan prior to configuring the IPX Printer Discovery mechanisms. IPX Network Scan is useful when you do not know all of the IPX networks and server combinations at your site, which makes the Discovery configuration process more efficient and improves overall Discovery results.

To configure the IPX Network Scan Discovery feature:

1. On the Discovery Methods screen, select Action > New Discovery.
2. Select IPX Network Scan and specify a name.
3. Click Continue.
4. If scheduling this Discovery method is needed, expand the Schedule section and set it in the same manner as the IP Sweep Schedule. You can specify the method of scanning for servers and Networks in terms of the number of Hops the scan is limited to.

Note: Zero (0) hops means that the search is limited to the local network.

Servers and Networks identified during the last IPX Network Scan are listed in the Servers and Networks Found in Last Scan screen.

Using IPX Servers Discovery

The IPX Servers Discovery mechanism locates NetWare® servers and active IPX node addresses by querying routers. You can identify specific Netware IPX servers in the IPX Server discovery setup webpage or select from a list of IPX Servers that were previously discovered during prior IPX Network scans.

To configure the IPX Server Discovery feature:

1. On the Discovery Methods screen, select Action > New Discovery.
2. Select IPX Server.

3. Click Continue.

4. If scheduling this Discovery method is needed, expand the Schedule section and set accordingly.

    Note: The Communications Settings section specifies the timeout period in seconds per printer and the number of communication retries. The recommended timeout per printer setting is 5 seconds and the recommended retries setting is 1.

    Note: Increasing the number of retries can significantly increase the discovery duration.

5. In the Server for Printer Discovery screen, identify the specific server(s) to be used during Discovery by doing one of the following:

    - Select the Specify NetWare Server radio button, and then type one or more server addresses to use for Discovery

    - Select the Choose NetWare® Servers from IPX Network Scan radio button, and then highlight specific servers from the IPX NetWare® Servers list for Discovery. The servers contained in the IPX Network Servers screen were populated by the last discovery obtained by the IPX Network Scan Discovery invocation.

Using IPX Addresses Discovery

Whereas IPX Server Discovery allows you to discover IPX network servers that know the IPX network addresses of IPX network printers, IPX Address Discovery pulls IPX addresses from prior PX Server discoveries to discover IPX network printers. Thus, IPX printer discovery is essentially a two-phased process' discovering the IPX Servers where IPX network addresses of printer are found, and using those IPX network addresses to actually discover the IPX printers.

To configure the IPX Address Discovery feature:

1. On the Discovery Methods screen, select Actions > New Discovery.

2. Select IPX Addresses.

3. Click Continue.

4. If scheduling this Discovery method is needed, expand the Schedule section and set accordingly.

    Note: The Communications Settings section specifies the timeout period in seconds per printer and the number of communication retries. The recommended timeout per printer setting is five seconds and the recommended retries setting is 1.

    Note: Increasing the number of retries can significantly increase the discovery duration.

    In the IPX Addresses screen, you can limit the Discovery process to specific networks, which in turn reduces discovery processing time and resource requirements via the following specification options:

5. Do one of the following:

    a. Select the Single Address radio button, and then populate the IPX Network and BPX Address fields

    b. Select the Specify Network radio button, and then populate the IPX Network field.

    c. Select the Choose Network from IPX Network Scan radio button, and then highlight specific servers from the IPX NetWare® Servers list for Discovery. The networks contained in the Networks screen are populated by the last discovery obtained by the IPX Network Scan feature.

6. Click **Add** to add the networks as specified above to the Current IPX Addresses list.

7. Click **Save**.

Using Community Strings

If the printers on the customer's intranet have their SNMP access community name strings set to anything other than "public" for getting SNMP information and "private" for setting SNMP information, CentreWare Web needs the name strings to access the MIB information stored in the network devices. You can perform this on the SNMP v1/v2 screen in the Discovery configuration section of Xerox Device Manager.
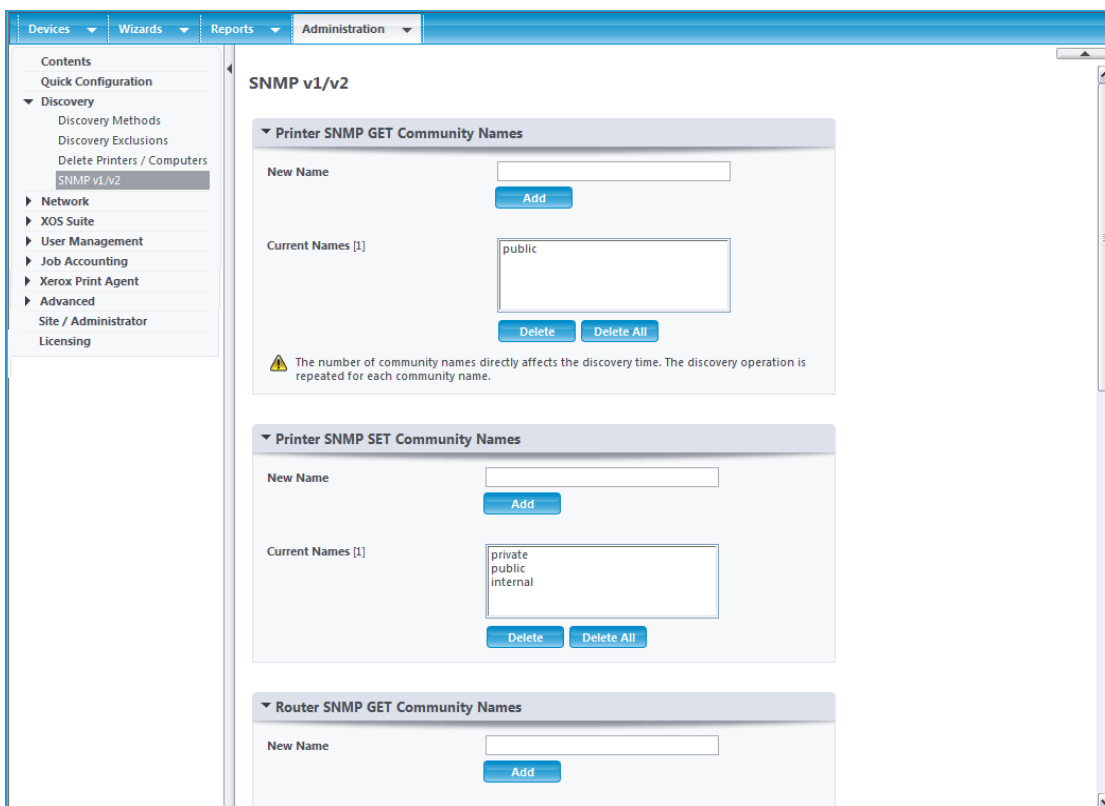
CentreWare Web allows a separate Community Name string to be specified for routers from the same screen.

Community Strings are used by applications as for device authentication. We recommend that any SNMP strings should meet minimum requirements to ensure a basic level of security.

• Strings should be a minimum of 20 characters in length.

• Strings should contain multiple character types:

   - Uppercase Characters (A through Z)

   - Lowercase Characters (a through z)

   - Base 10 Digits (0 through 9)

   - Special Characters ($, %, @, #, etc)

• Avoid using known words.

• Public and Private strings should not match.

- The router GET community name is used by the IP Subnet Scan and IP ARP Cache to query only the routers for the attached subnets. This is provided in addition to the printer GET community name to minimize discovery performance degradation.
- For some routers, you must also be added to the access list to query the router.

Using the Printer Re-Discovery Method

The Printer Re-Discovery Method updates known devices with infrequently changing data, like system name, system location, and printer capabilities (duplex, color, etc.). These parameters are not fetched during a status scan.

Rather than re-running a complete Discovery, which interrogates All addresses, the Printer Re-Discovery Method only interrogates those addresses that have an identified printer associated in the database. Known IP and IPX (when applicable) addresses are scanned for printers.

In addition to devices covered by the traditional IP/IPX discovery settings, printers added to CentreWare Web via Printer Server and Active Directory® enumerations are also included in the Printer Re-Discovery method.

Since the main purpose of this Discovery method is to capture device attributes that change at a slower rate than other attributes, it is recommended that this method be scheduled at an interval that reflects the likelihood of these changes, or that it is run on an as-needed basis to minimize network impact.

Note: You can only configure one Re-Discovery sweep. If one is already defined, the Printer Re-Discovery selection is unavailable (grayed out). To modify, select the pencil icon in the currently defined Discoveries list, or, delete the existing Printer Re-Discovery from the list to re-create.

You can schedule the Re-discovery method like the other methods. Communications Settings behave the same as for other discovery methods: CentreWare Web allows a Timeout per Printer for each address interrogated; any addresses that do not respond interrogations are retried for the set number of times.

Note: Increasing the number of retries can significantly increase the discovery duration.

To use the Printer Re-discovery method:

1. Select which network devices you wish to re-discover.
2. Click **Save**, or click **Cancel** to exit without making changes.

Hours Of Operation

You can configure CentreWare Web to allow Status Retrieval and Alerts during certain Hours of Operation. When configured, Status and Extended Data Retrieval is restricted to the set Operational Hours. This limits CentreWare Web's ability to retrieve Status and Alert updates and is not recommended. By default, CentreWare Web is configured for no restrictions, which means that CentreWare Web can perform Status and Extended Data Retrieval during any part of a 24-hour period.

To access Operation Hours for Status Retrieval and Alerts, select **Administration > Network > Network Usage Configuration > Advanced**.

Under the Operation Hours for Status Retrieval and Alerts section you may select a schedule for Hours of operation.

- Select Hours of Operation are the Same Every Day if the desired schedule is the same for each day.

- Select Hours of Operation are the Specified per Weekday if you want varied hours of operation.

- Select the start and the end time that correspond to your operational hours.

Note: If the retrieval of Status, meters, supplies, alerts or other extended data is currently processing, the tasks will complete regardless of specified hours. In the future, the retrievals will comply with the restricted schedule.

Restricting Discovery by Manufacturer

You can restrict CentreWare Web to only discover Xerox network printers, or it can discover all network printers. You configure it under Manufacturer Applicability found in **Administration > Network Usage Configuration > Advanced**.

Name Look Up

You can specify that the system perform a reverse network lookup after discovery is complete. This will allow names to be used for printer management when performing HTTP network requests. Enable this feature for environments that block HTTP requests to IP addresses. This selection will result in additional network traffic.

Managing Devices

Overview

CentreWare Web uses the processes of discovering network print devices (Discovery), scheduled device status polling (Polling) and responses to trap events to retrieve MIB data from devices. This data is translated to displayable fields within Xerox Device Manager and shows:

• Device model and manufacturer

• Page metrics

• Levels for consumables (toner/ink, paper, staples, etc.)

• Device configuration (existence and condition of scanners, finishing components) and overall status of the device.

CentreWare Web provides:

• Real-time access to device status and configuration

• Real-time access to managed device queues and servers

• Email alerting to provide device information and status to designated recipients based on user-selected device status events on Print Devices or Print Queues.

In addition, CentreWare Web provides the following tools for printer fleet management at the installation site:

• Standardize Configuration Sets—standardizes device configuration in the environment, and provides a monitor to verify that the devices comply with configuration policies.

• Clone Phaser Printers—clones a supported device's configuration to use on other devices of the same model and firmware. This option primarily applies to Phaser devices.

• Clone Printers—clones device's configuration to use on other devices of the same model and firmware. This option is used by AltaLink® devices or ConnectKey® devices with software versions 073.xxx.147.07400 or later.

• Upgrade Printers—allows propagation of printer upgrade files (firmware upgrade) throughout the print environment.

• Troubleshoot Printers—provides a simple automated procedure to quickly evaluate the status of one or more print devices in response to customer problems, or pro-actively validates network changes.

Working with Groups

CentreWare Web leverages the technology of device discovery and interrogation with the capabilities of ordering this information into visual management units, or Groups. A group is a container into which devices are explicitly selected for inclusion (Static Grouping) or by specifying simple rules, automatically selected (Dynamic Grouping).

Groups can separate:

- Geographically distinct devices (such as devices on the first floor from those on the second floor, or devices in Paris, Texas from those in Paris, France)

- Devices needing service from those that are fully operational

- Devices requiring on-site service from those requiring a toner replacement.

Effective fleet management uses Groups to organize and simplify the processes for alerting, upgrading, and configuring sets.

Creating a New Group

To create a new group:

1. Click **Devices > Printers > New Group**. The New Group screen displays.

2. Specify the Group Name.
   - The comment is visible when you select the Group from the Navigation pane.
   - Advanced allows the Administrator to set group level settings, such as information polling values and parameters. These include: communication and time-out settings, and scheduling for status and history retrieval and synchronization.

3. Click **Save** to close and proceed to the Configuration screens.
Note: There are two types of configuration settings for Groups, a Properties configuration, which includes the previous Identify and Communications settings, and a Membership configuration for defining rules of membership.

Configuring the Groups

You can view the group settings and information on the group properties page. To configure a group, select a group and under Group Actions click **Configuration.** There following sections can be configured.

- Properties
- Membership Filter

Using The Properties

The Properties section shows the settings for Group Identity (name, owner, contact info, and general comments), Communication Settings, Status Retrieval, Extended Data Retrieval, Extended Security Retrieval, Audit Log Retrieval, History Retrieval, Data Synchronization, and Certificate Status Audit for the selected group.

Extended Data retrieval is done on Protocol settings only, and tracks changes to Protocols in the Change History Report.

Extended Security Retrieval is enabled by default. You may customize the retrieval schedule or switch to Never if you do not want to pull extended security data. This data displays on the home page in the Security Assessment - Configuration tile.

Using The Membership Filter

Membership Filter specifies the parameters for automatic inclusion or exclusion from this group.

Note: For the pre-defined groups:

- Selecting Configuration displays the membership filter for that group.

- For example, Error group is automatically populated by any printer in the All group, which has an error state.

- The options are grayed out. The values are pre-defined and cannot be modified.

Viewing Status Alerts

Alert values used in the dynamic group definition (such as the Error group) require you to view the contents of the group to see what devices are included at any point in time. Status Alerts deliver a notification to specified recipients, when the selected events occur.

For more information about Status Alerts, see Working with Alert Notifications.

Creating A New Subgroup

To build a tree structure within a custom group:

1. Select a custom group.
2. Configure the subgroup as necessary.
   Note: Groups entered are listed in alphabetical order.
3. Click **Save**.

Reordering The Groups

To modify the display order of groups at the same level:

1. Select Reorder Group.
2. Reorder the group as desired.
3. Click **Save**.

Settings Parent Group

Set Parent Group can reassign an existing group to a different Parent group. This simplifies the task of reorganizing groups of printers. The group stays intact when it is reassigned to the new parent.

To use this function:

1. Select the group to be reassigned.
2. Click **Set Parent Group**.
3. In the Set Parent Group box, select the New Parent group.
4. Click **Save**. The group is now shown in the hierarchical view under its new parent group.

Deleting A Group

Delete Group deletes the currently selected group, and removes any devices that exist as members. The devices are not deleted from the database.

To delete a group:

1. Select **Delete Group**.
2. Select the group to delete.
3. Click **Save**.

Importing Groups

The Import Groups action lets you import csv file data to create groups and the hierarchy of groups. and add Membership Filters to groups.

The groups support up to 6000 groups and subgroups. You may have up to 20 sub-levels of subgroups. There are templates for Group and Membership that you can export and use to build your import file.

Follow the steps below to import group and membership files.

1. Navigate to **Devices>Printers**.
2. Under Group Actions click **Import Groups**.
3. Follow the instructions to import a csv file to either:
   - Create the group hierarchy.
   - Add filters to existing desired groups.
4. Click **Import**.
5. A results screen tells you how many groups have been added, updated, and how many errors there are.
6. Click **Back**.
7. Your new groups appear in the Printer group list in the left navigation.

Importing Devices Into Groups

The Import Devices into Groups action lets you import csv file data to add device to groups. You can assign new or existing (already discovered) devices to a group. With a new device, CentreWare Web runs a discovery for the provided IP address and assigns the device to the group. There is an Assign to Group template you may export and use to build your import file

Follow the steps below to import devices into a group.

1. Navigate to **Device >Printers**.
2. Under Group Actions click **Import Devices to Groups**.
3. Follow the instructions to import a csv file.
4. Click **Import**.
5. A results view show you how many addresses were found and how many entries were assigned successfully to existing groups.
6. Click **Back**.

Notes:

- Group Path is required and can be either the top level group name, or you can specify a group path such as Grand Parent / Parent / Child where the "/" delimits between parent and child groups.
- Devices will become members of all groups within the parent/child hierarchy.
- Devices cannot be assigned to special groups (such as Error or New Printer).
- If the Serial Number and IP Address (or DNS Name) is specified, then the device will only be added if the new device's serial number matches what exists on the device.
- If using a serial number without IP Address or DNS Name, only devices that have been already discovered shall be added to the specified group.

Exploring Group Functionality

Groups are presented graphically in the left Navigation pane of CentreWare Web. Represented as small folder icons, they function similarly to Windows® Explorer folders—they have a name, and the contents are

either objects or other folders.

CentreWare Web provides the following default device Groups for printers:

- Error—Contains those devices that display the Error icon for a status.

- Warning—Contains those devices that display the Warning icon for a status.

- Unconfigured—Contains those devices for which a Queue is not defined.

- All—Contains all discovered devices, regardless of state.

- Newly Discovered—Contains all newly discovered devices, regardless of state.

- Trellix Embedded Control—Contains Xerox devices with Trellix security software enabled.

You cannot delete or modify the default Groups. They are pre-defined to furnish a consistent base-level of functionality.

The New Group folder is not a folder, but a link to begin the creation of a new Custom Group.

You can populate Custom Groups to a maximum depth of 5 levels, including the top level (i.e., subGroup4 of subGroup3 of subGroup2 of subGroup1 of NewGroup).

Using Static Groups

A Static Group is suited for devices whose selection criteria are not expected to change. Physical location (building) or devices to upgrade are good candidates for Static Groups.

Without a Membership Filter set in the Group Configuration Group Action on a Static Group, the group is empty until devices are copied into the Group. Those devices remain in the Group forever until explicitly removed.

Using Dynamic Groups

Dynamic Groups are created exactly the same way as Static Groups except that the Membership Filter in the Group Configuration dialog pane is used.

1. Create a Group to demonstrate the ability to reflect the current state.
2. Click **New Expression**. A series of parameters display.
   a. Variable—Select a device parameter from the list.
   b. Condition—Based on the selected variable, a list of Conditions to be tested display. Since Printer Status displays a list of defined values for Printer Status, the condition is either Equals or Not Equal to the Value selected.
3. Click **Save** to enter these criteria. This furnishes up-to-the-minute information (based upon status retrieval) membership.

Note: Dynamic Filters are easily verifiable. Since they operate on data already in CentreWare Web, the results from the filter are immediately visible.

Additional Features of Dynamic Filtering

Two additional functions give greater flexibility and power to defining Dynamic Membership filtering:

- Inheritance

- Wildcards

Scenario:

- A filter was created to group all Phaser® 6300 and 6350 devices. These are on various subnets, and we want to select a subgroup of these for a specific action.

- This text match includes as members any devices whose Printer Model name contains the string phaser 63 anywhere in the string (case is ignored).

- The membership filter will include Xerox® Phaser® 6300DN and Xerox® Phaser® 6350DP, so it demonstrates a valid device selection, but it represents subnets that are outside our range of interest.

- Select Phaser devices from the 192.168.130.*, 192.168.142.* and 192.168.154.* segments for this requirement.

To accomplish this, create a subgroup under the Phaser 63xx Group:

1. Select the Phaser 63xx Group in the Navigation Pane.
2. Select **Actions > New Subgroup**.
3. Complete the Identity dialog pane. This will establish the following subgroup of Phaser 63XX named "IP segment 168." After you create the group, navigate to configure and add the following Membership Filter to the new subgroup. Select **New Expression**.

"192.168.1__.% "

This is translated as:

Match all IP addresses where

The first octet is exactly 192 and

The second octet is exactly 168 and the third octet begins with "1" and is between 100 and 199

(Note - there are two "_" characters)

The fourth octet can be any value." ("%")

Note: While the Wildcards operators (here "_" and "%") can represent characters as well as numbers, the context of the IP address constrains the values to be only numeric. Wildcard definitions are included in this section.

This filter will be applied to the Subgroup to determine the filter's membership.

These IP addresses are a valid selection from the filter and segments scanned. However, the original group contained only 7 devices. The Group filter and contents for Parent Group are correct. The problem is Inheritance:

- In the Membership Filter, Membership Inheritance is set to No Inheritance by default. This means that the members of the subgroup are completely defined by devices added statically (if any), and by the Expressions defined for membership.

- Selecting Inherit from Parent forces the filter expression to be applied only to the existing members of the Parent group.

Note: If there is no filter expression for the Parent, Inherit from Parent defaults to selection from the All Group.

- Changing the Inheritance to Inherit from Parent, yields the expected outcome – only those members of the Phaser 63xx parent Group which also meet the criteria of the subgroup membership filter are included in the subgroup.

Keep the following in mind when working with groups:

- Deleting a group does not delete the members from the CentreWare Web database. If the devices exist in any other Groups (they at least exist in the All Group), they remain.

- Deleting devices does completely delete any data about them from the database. They no longer exist. They can be rediscovered, but any Page Usage or Alert History data is lost.

- You can have both Statically placed and Dynamically filtered devices in the same Group.

- You cannot remove a device that is included in a group through use of a Filter Expression. You must exclude it on the basis of additional parameters in the Filter Expression.

- Filter Expressions for groups constructed for status polling have a performance impact on the CentreWare Web server, as they are re-evaluated each time a status poll is run against the group.

- You cannot remove devices from the All group. You can remove devices from the Newly Discovered group. This provides a simple method of checking for new or changed IP devices by examining the Newly Discovered Group—Remove all devices from Newly Discovered before a Discovery process.

Wild Cards

Refer to Wildcard Definitions in the Appendix for a list of wild card strings.

Wildcard Expression Examples

Any Printer Model with the string "Xerox DocuPrint N…", where matching values could include: N24, N32, N3025, N24/N32/N40, or Nuisance.

The Dynamic Group configured as the following:

- Variable = Printer Model

- Condition = Equals Wildcards

- Value = Xerox DocuPrint N %

- Could contain the following devices: DocuPrint N17, N205, N2125, etc.

(Note that while "Nuisance" or "Nonsense" both would match the N % wildcard, they would not be found in the Printer Model name within this string.)

Using wildcards to filter for machine firmware level

Creating a subgroup of WorkCentre Pro 55 devices with the following filter:

- Variable = Firmware Level
- Condition = Does Not Contain
- Value = r01.02.3[67]_.

and

- Variable = Firmware Level
- Condition = Does Not Contain
- Value = R01.0[3-8].%

Will populate the subgroup with all WorkCentre Pro devices where the ESS version level does not contain R01.02.36x. or R01.02.37x., or if the second firmware notation .02. is greater than 2 but less than 9.

Using the Table (Grid) View

The default view into a group is presented by the Table view. This is the result view of a graphical query to the CentreWare Web SQL database.

The Table Grid has the following features:

- The fields specified at the top of the view represent some of the 130 plus device-specific fields; up to 30 of which can be displayed concurrently. Clicking on the field name re-sorts the records by that field order.

- The status display icons provide simple visual indicator for printer (queue) status. See Using the Interface for an explanation of the icons.

- Table Preferences allows selection and placement of these fields as columns in the display.

- The Find query allows selection of any portion of the data from any of the fields, and displays all the matching records for that query.

- The status line at the bottom provides information on the number of records and buttons to change your location in the current display.

- Refer to the Appendix.

Examining Device Data

For devices that are compliant with the IETF SNMP Print Device RFCs, a wealth of data is available for Asset Management, Device Configuration, Problem Analysis and Troubleshooting.

- The Table view presents information for all devices in the view, based on the Table Preferences settings.

- You can select up to 30 of the available fields for display. Fields marked with [1] produce drop-down menus—any values currently in the group selected are available for selection.

Note:

- The information is current at the time of view; If the view is left on the screen it might not reflect the current state of the device. You can refresh the screen. By setting a refresh feature to update the screen every x minutes, the Table view refreshes automatically.

- Increasing the refresh rate will negatively impact performance.

- Altering this view to include queue fields as Last Queue Status Attempt, Print Server, Queue Name and Share Name, will display devices defined as print queues, but with a separate entry for each queue with which they are associated.

- The icons give a quick visual indicator of the device status for the groups in view at the time of examination.

- Selecting a device link brings up a detailed information access screen for the device.

- The page header specifies the device name and printer model. The tabs provide entrance to detailed functional views of this device.

- The Printer Actions options above the grid allows you to perform actions against the selected printers.

- When Edit is selected within the grid it allows you to modify certain device properties.

Software Level Reporting

When enabled, any multi-function printer or connected tablet discovered by CentreWare Web can report its current software level. Once the Software Level Reporting Service is complete, the reported software levels display in the Firmware column of the printer listing page.

To view the software levels of tablets, be sure to add the following fields to the list of Included Fields in your Table Preferences; they are disabled by default.

- Android Device: Indicates whether a tablet is connected to a printer.

- Android Firmware: Specifies the firmware level of the tablet.

These fields can also be viewed in the printer properties. Go to Properties>Asset>Printer Information to find these fields. **Note:** The Android Tablet information displayed cannot be modified. See "Using the Initial Android Tablet Upgrade File" on page 127 for more information.

Displaying the Tabs

This section describes the features on the various tabs in the Printers view.

Using The Device Tab

The Device tab displays detailed information of the device status, consumable levels, printer information, and counters.

Status

- General Status indicates when the last device status was delivered to CentreWare Web, when the last attempt was made to renew status, and overall connect time.

- Alert Details are copied from the internal device status history at the time of the last communication with CentreWare Web.
  Note: To read this level of detail from the devices requires that the Status Retrieval be set to Full.

- If configured, the Target Volume is a reference to measure Utilization Percentage for ad hoc printing optimization.

- Detailed Billing Meters and Usage Counters are presented, including Totals for Color and Monochrome, Print, Copy and FAX, as appropriate for the device.

- Device Audit Details provides:.

  - Overview of the Last Audit Check

  - Apply Configuration

  - Firmware upgrade performed on the device

  - Status of the operation

- Front Panel/Console information (if available)

Consumables

Information regarding the Toners, Drum, Fusers, waste containers, paper trays, etc is available on this screen. Supplies are displayed along with the levels remaining, serial numbers and a chart showing consumption.

Information

- Information supplies detailed device information including:

  - Firmware Level, Device Serial Number, Customer Asset Number, Xerox Asset Number, Network information and whether or not the device IP has been changed. (If it has, the Clear button becomes enabled to reset the "changed" flag).

  - IPX information in a Netware environment.

  - Printer location and contact.

  - Information on the Discovery Method and time of discovery.

- Peripherals: If supported and enabled for a device, card reader information may be pulled via an API. Information includes type, interface, vendor and product IDs, serial number, firmware version, and hardware type. The vendor and Product IDs are converted into hexadecimal values. If multiple card readers are enabled, the total number of card readers displays. However, the details only display for the first card reader. (Versalink does not support multiple card readers.)
  Note: This does not apply to the Elatec TWN4 model.

- Device Capabilities: MIB data from RFC 1759 and 3805 are displayed as English text detailing technology, capacities and capabilities of the device.
  Note: The mark [1] indicates you can edit this information (Finishing Options). This is useful in cases where the finishing features are not reported in the device MIB information. Device Status information includes:

  - Alert Details

  - Device Audit details

  - Front Panel/Console display information.

- Service Details Supported: What services are available on the device and if they are configured.

Usage Statistics

Statistics relating to the device usage are available from this screen.

- Target Volume (per month)

- Utilization Percentage

- 2 Sided Percentage

- Average Cyan Coverage Percentage

- Average Magenta Coverage Percentage

- Average Yellow Coverage Percentage

- Average Black Coverage Percentage

- Extra Long Impressions (with a separate listing for black and color extra long impressions)

Device Counters

- Page Count

- Total Impressions

- Printed Impressions

- Fax, Email and Copy counter information

Using The Properties Tab

The Properties tab allows a closer examination of the print device configured properties. This includes Asset, Printer Defaults, and Protocol/Scan/Security configuration setups, as well as Job Accounting information.

Using The Queue Tab

The Queue View shows all of the queues for a selected printer. The queue information includes the server where the queue resides, each queue installed, the driver installed, and the port type for that printer.

Using The Group Tab

The Group View presents all the groups in which the specified device is a member.

Using The History Tab

The History tab displays the alert, status, usage counter, and change history. You can define a date range to review historical details.

Device View Actions

Select a printer from the table view to open the device view. There is a unique Actions menu available in this view.

- Edit Properties: Edit or modify all the different printer configurations, including Printer Information, Notifications, Protocols, Scan Services, Security, and Job Accounting information.

- Save As New Configuration Set: Makes a copy of the current device settings and makes them a configuration set.

- Add to Group: Adds the device to device groups.

- Printer Web Page: If the http server is enabled for the device, this is the same as browsing to the IP address of the printer.

- Install: Installs the selected printer on a print server.

- Troubleshoot: A series of simple tests are generated against the selected printer.

- Reset Printer: Sends a reset (reboot) request to the device; compliant devices reboot.

- Refresh Data: Acquires up-to-date data from the device.

- Retrieve Job Data: Immediately retrieves the job data from a device.

- Delete Printers: Removes all data for this device from this CentreWare Web server.

Troubleshooting a Printer

By selecting a printer and clicking Troubleshoot, CentreWare Web performs a series of tests, starting with a Printer Ping test, and then querying the device status using SNMP. Additional tests are then performed on associated queues and print servers. The results display in the Troubleshoot Device window.

To troubleshoot the printers:

1. Click **All** from the Printers navigation tree.
2. Click on the selection box associated with the desired printer.

Note: Avoid selecting any printers whose status is Not Communicating.

3. Select Printer Actions > Troubleshoot, and then click **Go**.

Note: If the Printer Actions dialog is expanded, clicking **Troubleshoot** immediately initiates the process.

Once selected, CentreWare Web begins its troubleshooting process by initially performing an ICMP ping test to see if the device responds to this form of communication. If the device responds, the current status of the device is queried through Xerox Device Manager's SNMP interface. If the device has a print queue on one of Xerox Device Manager's managed servers, then the print server's health and the current status of the print queue is also checked. A "progress" busy waiting dialog displays.

When CentreWare Web completes its testing, a Troubleshoot Results screen displays.

When you select Details/Test in the Troubleshooting Results window, the Troubleshoot Device details webpage is visible. The Troubleshoot Device Details page allows you to perform the following remedial actions in troubleshooting device problems:

- Open up a separate browser to display the printer's embedded web server. This function is also accessible from the printer's Detailed Status window.

- Generate a test print by clicking Print Test Page Directly.

Note: This test will not succeed if the printer does not support port 9100, 2000, 2105 or LPR through port 515. These are the standard ports used to send a test print directly to a printer.

- Reset (reboot) the printer

- Directly manage any of the print queues found on CentreWare Web

- Print a test page through any of the print queues.

In addition to these functions, the Troubleshoot Device details page lists any current error or warning status conditions, including detailed information on the skill level involved in correcting the problem along with detailed descriptions and age of condition. This functionality requires the device to be compliant with standard MIB interface provided by CentreWare Web.

Troubleshooting Multiple Printers

CentreWare Web allows you to activate the Troubleshoot feature for multiple printers.

To activate the troubleshoot feature for multiple printers:

1. Click **All** from the Printers navigation tree.
2. Select the check boxes to choose multiple printers to be tested in the All printers group table view screen.
3. Select **Action > Troubleshoot.** When the tests complete, the results for each printer display in the Troubleshoot Results screen.
4. To perform more advanced tests, click Test. This takes you to the Troubleshoot Device feature, as described in the Troubleshoot single printer feature above.
5. Click **Back** to return to the Troubleshooting Results screen and proceed with tests on the rest of the printers.

Exploring the Device Management Dashboards

The Device Management Dashboards allow you to monitor devices and resolve issues to ensure that they remain in the desired configuration state. Drill down features make it easy to see and understand the policy compliance at each device level. The detailed views display specific errors relating to device policy compliance.
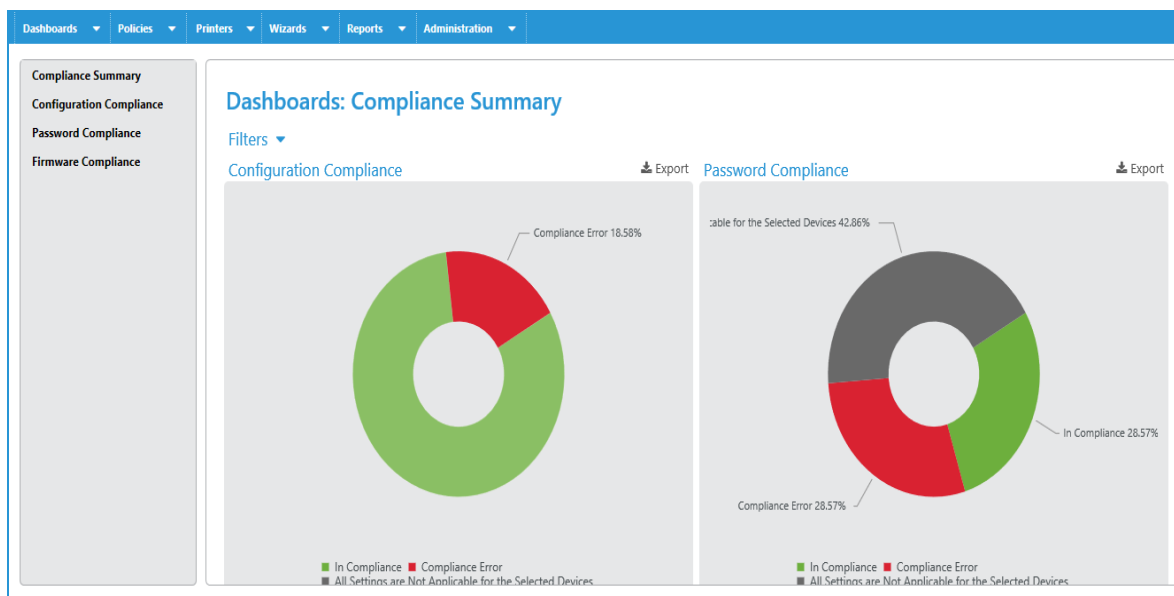
In the left navigation choose which compliance information to display. Most dashboards can display either by percent or count. You can click on the graphs to drill down for greater detail.

In each of the policy charts or bars, click on a ring or bar to drill down for more information about the policy. Click again to view a list of compliant or non-compliant devices. From this view you can enforce the policy.

- Compliance Summary: Shows overall compliance by policy in a doughnut chart. Each ring is a different firmware, configuration set, or password policy. You can filter these views by one or more device groups. When you click on a status in the Overall Device Health chart, the print grid opens and is filtered by the status you clicked. This feature is only functional when a device group is associated with a policy, rather than individual printers.

- Configuration Compliance: Shows compliance for the configuration policies you have set. The dashboards present information in an overall view, by each policy, by model, and by trend.

- Password Compliance: Shows compliance for the password policies you have set. The dashboards present information in an overall view, by each policy, by model, and by trend.

- Firmware Compliance: Shows compliance with firmware policies you have set. You must have a policy type of Monitor or Monitor and Automatically Upgrade in order for the firmware policy to appear in the dashboards.

Policy Drill Down

When you want more information than the high-level dashboards present, click on a ring or bar for more details. Click again to view a list of compliant or non-compliant devices. If you have the appropriate

permissions, you can enforce the policy from this view. Customer Report Users will not see the Enforce button, and it will not display on the Security Monitoring drilldown view.

Below you can see the Compliance by Policy view, which is showing compliance by percent for firmware. You can apply filters to display different views of the dashboard depending on the data you need. You can see there are several policies out of compliance. Hover over the bar to see the full policy name and percent of devices out of compliance. Click on the bar for a list of the devices and details about their level of compliance. The list view shows you the model and reasons for non-compliance, as well as the other pertinent information for remediation.
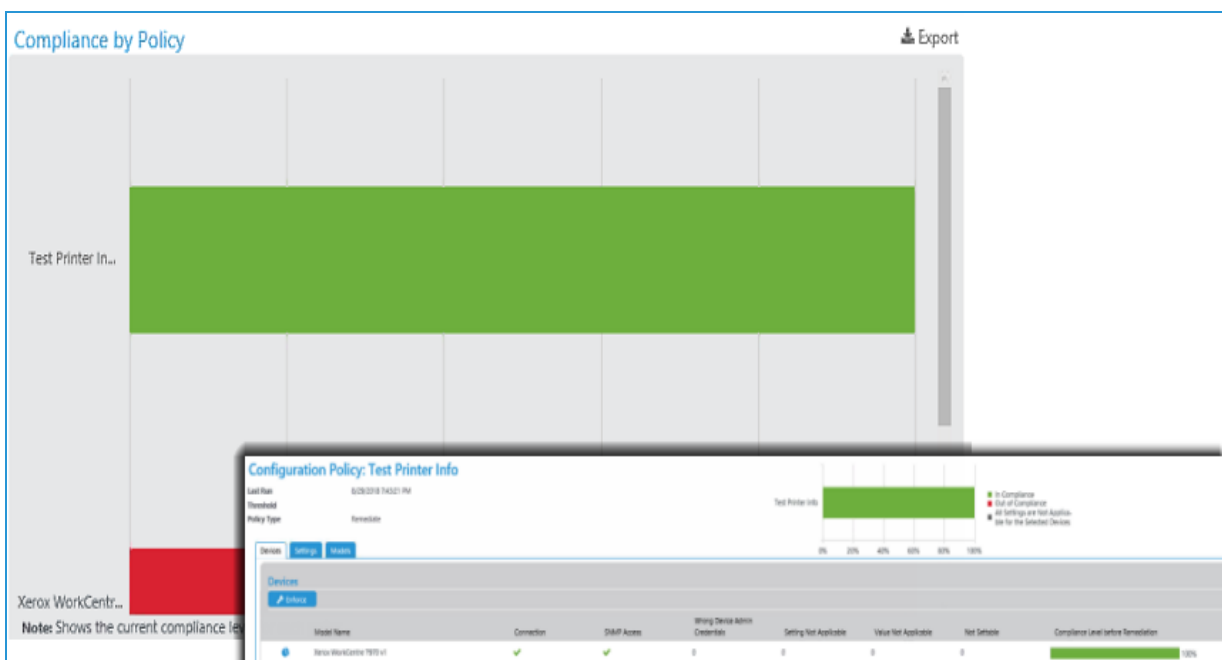
Exporting the Dashboards

Each of the dashboards can be exported and stored locally to support tracking and resolving compliance issues. Follow the steps below to export a dashboard.

1. Click the **Export** icon above the dashboard.
2. In the Export to File pop-up window complete the following fields.
   - Row Grouping: Choose to group by policy or device.
   - Included Fields: Either use the defaults our custom set the fields you want to include in the export
   - Time Span: Set the range of days to include in your export. You can choose all data, a set number of previous days, or a specific date range.
   - Format: In the drop-down select CSV or HTML
   - Language: Choose the language of your export to translate the field names.
3. Click **Download**.
4. Save the file.

Working with Alert Notifications

Overview

While there is an enormous amount of information available from the CentreWare Web user interface, for large print environments, a mechanism to generate notifications on the basis of abnormal conditions—without user intervention—is mandatory.

CentreWare Web can discover printers in NetWare or Microsoft® print server environments, defined in queues or as TCP/IP-connected print devices. Once discovered, you can recover the status of these devices through scheduled SNMP status polling, or by traps sent by print devices.

Setting E-mail Alerts from CentreWare Web

Generating e-mail alerts in CentreWare Web from devices discovered by CentreWare Web requires:

- A fully compliant device connected and functioning in the same network that CentreWare Web is connected and functioning,

- A CentreWare Web group containing the device, for which an alert profile is defined

- A status event that matches the alert profile conditions, and exists for a period of time equal to or greater than the alert threshold time.

Note: The local CentreWare Web group must be a user-created custom group. All and Newly Discovered are not recommended by default, and you cannot modify alert profiles from CentreWare Web in the other groups.

Starting with the required CentreWare Web configuration:

1. From the Administration tab, verify that at a minimum, the following are enabled in the Application Wide Network Traffic Switches section:

   - Status Alerts

   - Status

   - History Retrieval

2. Confirm that the Hours of Operation include the times when the e-mail alerts are to be sent.

   For example, if the hours of operation requires that notification occur only between the hours of 8AM to 7PM, verify that operating hours include that time.

   Limiting the hours of operation affects when you can start status retrieval from the printers, servers, and active directories. Currently running retrievals are completed if the process runs past the closing time. This limit does not affect discovery, historical data retrieval, data synchronization, and services manager data exchange, which are scheduled separately.

Configuring a Group in CentreWare Web for E-mail Notifications

After setting the traffic switches and hours of operation, the next step is to create a device group in CentreWare Web that sets the alert profile.

In this example, the group is named Full Status Retrieval and will be configured for alerts. Subsequently, specific devices could be added as static or dynamic members. In either case, the alert functions behave identically.

Other settings in the Advanced group that you should examine prior to defining the alerting parameters are:

- Communication
- Status Retrieval
- History Retrieval

The Timeout/Retry settings for a group might be different from the values set under Network Usage Configuration from Administration > Network. Changes to these parameters might be required for certain groups whose members may be on long-delay segments of a network.

You can configure Group Status Retrieval to accept the default defined under Network Usage Configuration, or be explicitly set on a group basis. For this example, the polling frequency for examining status will be run every 30 minutes during the hours of operation. In addition, Full Status retrieval is selected to:

- Enable use of the technician dispatch alert
- Provide a greater detail for analysis of the alert history

Configuring E-mail Alert Profiles

The following example sets the various parameters to recover specific critical alerts in the group Full Status Retrieval. The Membership filter is not yet set—you can apply these alerts to members of a static group, dynamic group, or a combination.

To configure the email alerts:

1. Select **Group Actions> Status Alerts**. For a group with no existing alert profile, a message is generated indicating that the Network Traffic Switches need to be set and that a valid e-mail server is required.
2. Select **New Profile**.

Note:

- To use the profile, you must assign it a name and enable it.
- You can flip the Enabled check box to not enabled. This stops the selected alerts from signaling without deleting them.

   There are Alerts that apply to locally connected printers (not directly attached to the network or a print server), and Alerts that are for networked print devices.

   Alerts with a [1] require a device with RFC 2790 2-byte alert compliance.

   Alerts with a [2] are Extended Status Alerts - These items are only supported when the group is configured for Full Status retrieval.

Note: In addition to the standard device-generated alerts, CentreWare Web also supports extended alerts that are derived from the device status for Xerox printers and provide greater insight into a printer's condition. Conditions that were previously grouped under Intervention Required alerts are differentiated and reported separately. For example, a fuser reaching its end of life is reported as such instead of as Intervention Required. Xerox Device Manager also provides alerts on other important subsystems in a printer, including the Xerographic, Scanner, Finisher, Toner, and data subsystems. The functionality of some of these extended alerts might be dependent on the particular printer model.

1. Highlight and use the arrows to select and move the desired alerts from Available Alerts to Included Alerts.
2. Scroll to the Alert Threshold selection.

   The polling frequency (set as Status Retrieval value) indicates how often to check a device for a status change, while the Threshold Time specifies how long the device must remain in the selected alert(s) state to signal a valid alert.

Note:

- Typically, when a device enters an alert state (e.g., Toner/Ink Low), it remains in that state and waits for two conditions to be achieved: alert detected and threshold met, which indicates low toner. However,

since the alert signal at the start of the event and the re-check status occurs when the threshold timer ends, the device can fluctuate between an alert condition and a no-alert condition, and either be successfully caught or ignored. Decreasing the status polling interval (checking the status more frequently) might avoid this fluctuation, but a more efficient route is to evaluate the device Alert History, which is captured during each Full Status Retrieval, for problematic devices.

In the above example, a Status Retrieval value of 30 minutes and a Threshold of 10 minutes indicates that if a device is in an Offline & Intervention Required state at any time during the poll, it must remain in this state for the next 10 consecutive minutes before it signals an alert. The logic that tracks the threshold timer is independent of the polling process. When the threshold timer expires (in this example, when the 10-minute time period has elapsed), another SNMP query is sent to that device to get the most recent status conditions.

Adding Information

You can add information already captured by CentreWare Web to the e-mail alert using the same mechanism of moving fields from Available Fields to Included Fields. This information helps identify the Site Location or System Contact, or supply additional information for a remote Asset Coordinator or CSE.

To complete configuring the e-mail alert:

1. Check the Send E-Mail Alert check box.
2. Add the recipients' e-mail addresses. **Note:** The recipient e-mail can be any valid e-mail address.
3. Configure the e-mail message (subject and text, if required).
4. Click **Save**. The alert profile is summarized.

Constructing E-mail Parameters

You can construct the e-mail subject with information in CentreWare Web for this device. Using the substitution scheme below, include:

• Subject: CentreWare Web Warning: Input Tray Missing with WCP55-118 at Betelgeuse S/N NWL-026094

Note: You can send the subject line as a text-page message for remote support personnel.

The Custom Subject can include the following field descriptors:

- %v = Severity (Error / Warning)
- %p = System Name
- %g = Site Name
- %s = Printer Status
- %1 .. %5 = Custom Property 1 .. 5 (appears in the subject once enabled on the customize page)
- %c = Location
- %m = MAC Address
- %f = Manufacturer
- %n = Serial Number
- %% = % character

After expansion, the maximum allowed subject line is 255 characters.

Constructing The E-mail Message

The subject of the e-mail message is the name of the group that has the alert profile with Input Tray Missing as a selected alert condition. The message itself contains a description of the relevant fields, as well as a description of the alert.

Note: If the page device accepts hyperlinks, you can use the Device screen and the Detailed Device screen via this service.

Using Status Alerts

The application enables sending e-mail messages for only those printer alert conditions and printer queue-based conditions that are considered important. In other words, filter out less important alert conditions (e.g., door open, output tray full, etc.) and send e-mail messages only for the critical ones (e.g., paper jammed, toner low, etc.). Additionally, you can customize the subject line of the e-mail message and provide additional descriptive text in the body of the message. There is an expanded array of alerts for a variety of conditions of concern to the system administrator. These expanded alerts give greater insight into the printer status. For example, there is an alert for when a consumable such as an imaging drum or fuser is reaching its end of life. With this information it is now possible to order replacement supplies in a timely manner to avoid out of service conditions.

In order to conduct this test, you need physical access to a networked printer on which an evaluator can perform tests such as forcing a Door Open or Out of Paper conditions. This printer must also be included in the All Printer group within the application database.

- Verify that the status of the test printer is Up and Running before conducting the Status Alerts test.

- On the Administration>Network>Network Usage Configuration page, in the Status Retrieval section select Every and set a frequency, and select Full Status. On the Administration>Network>E-Mail & External Servers page configure the Mail server if required.

E-mail alerts feature

1. Select the All folder in the Printers Folder navigation window to display the All Printers group.
2. Select **E-mail Alerts**. This displays and sets up the E-mail Alerts for the All printers group.
3. If this is the first time, create a new E-mail Alert Profile. Select **New**. The New Printer E-mail Alert Profile window opens.
4. In the Profile Identity window enter "All Profile" in the Name field.
5. Check the Enabled box.

This feature enables or disables individual profiles from generating Status alerts. This can be useful for evaluating functional alerting without having to re-enter the profile information.

1. In the Device Alerts to Send window, select Door Open from within the Available Alerts sub window.
2. Select → to move Door Open to the Included Alerts sub window.
3. In the Printer Fields window, select>> to include all fields. This is the information about the device included in the mail note sent to the recipient.
4. In the New Recipient field of the E-mail Recipients window, enter a valid SMTP e-mail address for the evaluator.
5. In the E-Mail Alert Format window check the Custom radio button and enter the following text: Testing EMail alert feature.

6. Select **Add**.
7. Select **Save** to save the new E-mail Alert Profile.

You can associate multiple status alert profiles with a group. Different individuals may be notified of different alerts. Each profile may specify different data to be sent to the recipient.

1. On the Configure Group: All page, select **Configure**.
2. On the Configure Group Properties: All page, select the Every radio button and set the status retrieval interval to 1 minute.
3. Select **Save** to apply the Status Retrieval settings.
4. Using the test machine, force a door open condition.
5. Wait at least one minute for a Status Retrieval action to occur.
6. Display the detailed status for the test printer by clicking on the printer's IP address from within the All Printers group display page.

Verify that the Door Open status is identified in the Printer Status window. At this point, an e-mail is generated and sent to the address specified in the Alert Recipients field of the All Profile sub window on the Printer E-mail Alerts page.

1. Verify the delivery and accuracy of this e-mail message.
2. Upon completion of this test, set the status retrieval interval to a value that will not stress the network.

Enabling and Using Traps

An SNMP trap is an asynchronous SNMP message from the device to a network manager indicating that a significant event has occurred on a network device. Traps can occur at any time and typically have minimal impact on network traffic. Enabling alerting by traps can reduce polling traffic. Since traps are delivered via the UDP mechanism of TCP/IP, there is no guaranteed delivery or notification of receipt for traps.

The downside is that there can be events (NIC failure, power outage, etc.) that might not be sent as trap messages to CentreWare Web. To avoid this, and to allow for devices that do not support trap notifications, it is recommended you have Status Polling enabled for alerting, but at a reduced frequency (longer interval) when traps are enabled on devices.

If it is possible to register all managed devices for traps, you could extend any scheduled Status Retrieval for this group, and rely on the status information returned from the trap poll. However, there are some significant trade-offs.

When you enable device traps, CentreWare Web interrogates the device for status and alert history. Warnings, which can be detected in standard Xerox Device Manager polling, are typically not available from a trap that signals only significant events, such as:

- Device power cycle

- Error event

- Unauthorized SNMP access

This might leave a support gap because Low consumable alerts are not detected.

CentreWare Web allows you to conduct SNMP trap configuration modifications such as:

- Registering for traps

- Clearing traps for the CentreWare Web server

• Clearing all traps in the printer (for all destinations)

This feature enhances the capabilities of CentreWare Web to detect and provide notification of printer status. You can complete these activities for several multi-vendor printers via the Modify Trap feature. In CentreWare Web, traps are configurable on an individual printer and a per-group basis.

Note: Not all printers support traps, and for those printers trap actions are ignored. CentreWare Web provides Traps Supported and Traps Enabled device attributes when determining suitability of use.

You can configure CentreWare Web to register for traps on all newly discovered printers, as an alternative to manually registering on an individual printer or per-group basis.

Modify Trap allows you to perform per-group configuration for the following features:

• Register for Traps: Registers to receive trap alerts from printers that support traps.

• Clear Traps for this Server: Clears the traps registered on the local server where CentreWare Web is installed.

• Clear All Traps in Printer (for All Destinations): Clears all traps displayed in CentreWare Web for the associated printers.

Selecting this option de-registers all the displayed traps, not just those registered with the local server.

To use the Modify Trap feature:

1. Select a local group or All from the Printers navigation tree.
   Note: Use the Table Preferences feature to display the Traps Supported column.
2. Click on the selection box(es) associated with one or more of the printer(s). **Note:** Select only printers that support traps.
3. Select **Printer Actions > Modify Traps**. The Modify Traps screen displays the following three options:
   - Register for Traps
   - Clear Traps for this Server
   - Clear All Traps in Printer (for All Destinations)
4. To register printers for traps, click on the associated radio button and click **Confirm**. CentreWare Web contacts the printer(s) through SNMP communications using the SNMP Get and Set Community name strings as authentication credentials and attempts to register its network address with the printer(s) for traps.
   - The Register for Trap progress screen displays the results of the trap registration transaction.
   - All of the printers selected above (that support traps) are now registered to receive the traps specified by the individual printer manufacturer.
   - Selecting a device thus enabled sets the printer Icon to yellow or red, indicating that the printer status has changed from Up and Running to a Trap Detected fault status.
5. You can evaluate Clear Traps for this Server and Clear All Traps in Printer in a manner similar to the steps described above.

Using the Edit Traps Feature

Edit Trap allows you to configure traps on an individual printer basis. You can view the registered traps specific to the selected printers:

- Network Protocol: IP,IPX
- Trap Destination: CentreWare Web server (or any other SNMP manager) for which the trap is registered
- Port: Typically: 162
- Traps: Type: coldstart, warmstart, link up/down, authentication failure or all: Pass Everything

You can also configure individual printers for the following features on a per-device basis:

- Register for Traps: Registers to receive trap alerts from the selected printer. (The printer must support traps.)
- Clear Traps for this Server: Clears the traps registered on the local server where CentreWare Web is installed.
- Clear All Traps in Printer (for All Destinations): Clears all the traps for the associated printers.

Note: Selecting this de-registers the CentreWare Web server from receiving all the displayed traps, not just those registered with the local server.

- Clear Selected Traps: Clear specifically selected Traps

To use the Edit Trap feature:

1. From the Printers Display grid select **Edit Printer Properties** for your selected device.
2. Navigate to Protocols > Traps. The Traps screen displays the following options:
   - Register for Traps
   - Clear Selected Traps
   - Clear Traps for this Server
   - Clear All Traps in Printer (for All Destinations)
3. Select the Clear Traps for this Server radio button and click **Confirm**. The Current Traps field in the Printer table is updated to show that the printer is no longer configured to receive traps and the printer attribute for Traps Enabled is set to No.

Using Traps—Notes

Traps can be a valuable tool for managing large network infrastructures and reducing the frequency of device status polling. However, the following should be understood:

- Not all devices can register for traps; CentreWare Web provides a mechanism for identifying those devices (Traps Supported / Traps Enabled fields)
- The particular site mix of devices that can register for traps might affect the needs for polling specific subnets
- Network outages and certain device failures do not send traps at the point of failure, but only after the return from the failure; this warrants polling as an adjunct to trap recognition.
- Not all device events generate trap messages; errors, reboots, and SNMP authentication generate trap messages, but warning messages, which may be relevant to fleet management, do not.
- The RFC for traps (1157obsolete/1905obsolete/3416/3418) allows specific information to be sent with a trap; CentreWare Web does not read this because of the low levels of standardization on the data format, instead, it interrogates the device for complete status information.
- Registering for traps requests that CentreWare Web query the device whenever a coldstart, warmstart, authentication failure, or critical device failure is detected on the device.

Reviewing Alert History and Status History

Reviewing the Alert History and the Status History (which must be selected with the Full Status option in Status Retrieval polling) can furnish a background on the types of events that should be detected, and which alerts you should select for the alert profile.

The Alerts are listed along with their criticality (Warnings: Input Tray Missing, Non-Compliant Warning Received) and time.

The Status History is only populated whenever a new status is detected from the network printer. This data is gathered either when status polling is enabled on printer groups, managed print servers or active directories, or when an SNMP trap is received from a network printer.

Below is the corresponding Alert History from this device.

- The Alert History is only populated whenever a new alert is detected from the network printer's alert table. This data is gathered when:
  - Retrieve Alerts is enabled for status polling on printer groups, managed print servers, or active directories
  - Collect Alert History is enabled for historical data gathering on printer groups, managed print servers, or active directories
  - Historical data gathering with Collect Alert History is enabled on the Administration tab
  - Device Alerts is included in an E-mail Alert message
  - An SNMP trap is received from a network printer.
- The Alert History can supply:
  - Complete device error code and description of that error code
  - Criticality
  - Skill level recommended
  - Time-stamp.

Correlating the Status History (CentreWare Web's alert filtering) and the Alert History from the device supports intelligent Alert Profile decisions.

The following table has combined the Status and Alert History from a typical device, and has arranged the data by time-stamp.

Note: Status polling (full status alert retrieval) was set for 25 minutes and traps were enabled. Gaps in polling reflect CentreWare Web operations—power-cycle and upgrading).

Alerts that can be set and identified in CentreWare Web are shown in **bold**. These consist of **Offline, Low Paper, Paper Jammed, Intervention Required,** and **No answer from device.**

Status	Description	Timestamp
Up and Running		8/10/2017 10:00:27
No answer from device		8/9/2017 17:00:54
No answer from device		8/9/2017 16:47:27
Up and Running		8/8/2017 17:42:37
Unavailable for any use	Errors: Door Open, Offline, Paper Jammed, Intervention	8/8/2017 17:34:01

Status	Description	Timestamp
	Required	
Untrained	Jam condition detected, prtAlertCode=0 [Paper Jammed]	8/8/2017 17:32:46
Unavailable for any use	Errors: Offline, Low Paper, Paper Jammed, Intervention Required	8/8/2017 17:17:38
Untrained	22-513.04 38-02 Job(s) are held in the printer queue because none of the paper trays are configured with the proper media resources. User intervention is required to resolve media resource conflicts at the local user interface. Printing can continue. [Intervention Required]	8/8/2017 17:13:05
Untrained	22-511.04 16-30 A paper tray-related problem has been detected. User intervention is required to check either the active Alert Table (remote UI) or the active message screen (local UI) for previous tray-related problems. Printing has stopped. [Intervention Required]	8/8/2017 17:12:03
Untrained	10-565 09-10 The machine has detected paper in area 4 (duplex path). User intervention is required to clear paper jam (instructions provided at the local UI). Printing has stopped. [Intervention Required, Paper Jammed]	8/8/2017 17:12:02
Untrained	8-555 09-06 The machine has detected a paper jam in area 2 (paper registration). User intervention is required to clear paper jam (instructions provided at the local UI). Printing has stopped. [Intervention Required, Paper Jammed]	8/8/2017 17:12:01
Untrained	7-525.01 41-02 Tray 1 is empty. User intervention is required to add paper. Printing can continue if the proper media is available from other trays. [Intervention Required, Out of Paper]	8/8/2017 17:11:50
Up and Running		8/8/2017 13:07:39
Functioning but has one or more warnings	Warnings: Intervention Required	8/7/2017 15:55:07
Functioning but has one or more warnings	Warnings: Intervention Required	8/7/2017 15:30:07
Functioning but has one or more warnings	Warnings: Intervention Required	8/7/2017 13:16:24
Untrained	22-513.04 38-02 Job(s) are held in the printer queue because none of the paper trays is configured with the proper media resources. User intervention is required to resolve media resource conflicts at the local user interface. Printing can continue. [Intervention Required]	8/7/2017 13:10:14
Up and Running		8/7/2017 10:04:44
No answer from device		8/7/2017 9:37:41
No answer from device		8/7/2017 9:12:41
No answer from device		8/7/2017 8:58:21
No answer from device		8/7/2017 8:47:41
Up and Running		8/7/2017 8:22:54

Combined Status and Alert History

Available CentreWare Web Alert Events	
Communication Error External [2]	
Communication Error Internal [2]	
Consumable Missing[1]	Direct Printer Access Denied
Direct Printer Initializing	Direct Printer Manual Feed Required
Direct Printer Out of Memory	Direct Printer Page Punt
Direct Printer Paper Problem	Direct Printer Paused
Direct Printer User Intervention Required	Direct Printer Waiting
Door Open	Drum Invalid [2]
Drum Missing	Drum Reorder
Drum Replace	Invalid Tray Empty [2]
Input Tray Missing[1]	Intervention Required
Finisher Failed [2]	Finisher Full [2]
Fuser Invalid [2]	Fuser Overtemp [2]
Fuser Reorder [2]	Fuser Replace [2]
Fuser Undertemp [2]	Hard Disk Missing [2]
Hole Punch Waste Full [2]	Image Disk Error [2]
Input Tray Empty [1]	Input Tray Missing [1]
Intervention Required [1]	Job Accounting Log Corrupted [2]
Job Accounting Log Full [2]	Low Paper
Machine Configuration Incorrect [2]	No answer from device
No Toner/Ink	Non-Compliant Error Received
Non-Compliant Warning Received	Offline
Offline & Intervention Required	Offline Only
Out of Memory [2]	
Out of Paper	Output Bin Full[1]
Output Bin Near Full[1]	Output Tray Missing[1]
Overdue Preventative Maint[1]	Paper Jammed
Scanner Failed [2]	Scanner Feed Roller Reorder [2]
Scanner Feed Roller Replaced [2]	Stapler Malfunction [2]
Staples Empty [2]	Staples Invalid [2]
Staples Low [2]	Staples Missing[2]
Technician Dispatch Required	Toner Level: 10% Low Black [2]
Toner Level: 10% Low Cyan [2]	Toner Level: 10% Low Magenta [2]
Toner Level: 10% Low Yellow [2]	Toner Level: 20% Low Black [2]
Toner Level: 20% Low Cyan [2]	Toner Level: 20% Low Magenta [2]
Toner Level: 20% Low Yellow [2]	Toner Level: 30% Low Black [2]
Toner Level: 30% Low Cyan [2]	Toner Level: 30% Low Magenta [2]
Toner Level: 30% Low Yellow [2]	Toner Level: 40% Low Black [2]
Toner Level: 40% Low Cyan [2]	Toner Level: 40% Low Magenta [2]
Toner Level: 40% Low Yellow [2]	Toner Level: 50% Low Black [2]

Available CentreWare Web Alert Events	
Toner Level: 50% Low Cyan [2]	Toner Level: 50% Low Magenta [2]
Toner Level: 50% Low Yellow [2]	Toner Level: Low Black [2]
Toner Level: Low Cyan [2]	Toner Level: Low Magenta [2]
Toner Level: Low Yellow [2]	Toner Level: No Black [2]
Toner Level: No Cyan [2]	Toner Level: No Magenta [2]
Toner Level: No Yellow [2]	Toner/Ink Low
Tray Configuration Incorrect [2]	WasterBottle Full [2]
Waste Bottle Near Full [2]	Xerographic Module Invalid [2]
Xerographic Module Missing [2]	Xerographic Module Reorder [2]
Xerographic Module Replace [2]	
2 Sided Percentage	2 Sided Sheets
Advanced Finishing Supported	Analog Fax Capable
Analog Fax Description	Analog Fax Modem Installed
Analog Fax Phone Number	Black Copied Impressions
Black Copied Large Sheets	Black Impressions
Black Large Impressions	Black Printed Impressions
Black Printed Large Sheets	Black Rated PPM
Color Capable	Color Copied Impressions
Color Copied Large Sheets	Color Impressions
Color Large Impressions	Color Printed Impressions
Color Printed Large Sheets	Color Rated PPM
Console Language	Copied 2 Sided Sheets
Copied Impressions	Customer Asset Number
Detailed Device Page	Discovery Date
Discovery Method	Discovery Type
DNS Name	Duplex Capable
E-Mail Images Sent	Embedded Fax Images Sent
Embedded Fax Impressions	Embedded Fax Large Sheets
Fax Impressions	Finishing Options
Firmware Level	Hard Disk Present
Hard Disk Size MB	Images Sent
Internet Fax Images Sent	IP Address Changed
IP Default Gateway	IP Source
IPX Address	IPX External Network Number
IPX Print Server Name	Large Impressions
Last Known IP Address	Last Status Attempt
Machine Up Time	Manufacturer
Marking Technology	Network Scanning Images Sent
Page Count	Page Count since Power On

Available CentreWare Web Alert Events	
Physical Memory Total MB	Printed 2 Sided Sheets
Printed Impressions	Printer Location
Printer MIB Language	Printer Web Page
Printer Web Server Enabled	Protocol Version
Queue Information	Scan to E-Mail Capable
Scan to File Capable	Scan to Internet Fax Capable
Scan to Server Fax Capable	Scanner Description
Scanner Installed	Serial Number
Server Fax Images Sent	Site Name
Status Date	Subnet Address
Subnet Mask	Supply Levels
System Contact	Target Volume
Total Impressions	Traps Enabled
Traps Supported	Utilization Percentage
Xerox® Asset Number	

Available CentreWare Web Alert Events
See the Description of Printer Alert Selections table in the Appendix for further information.

Available CentreWare Web Alert Print Fields	
2 Sided Percentage	2 Sided Sheets
Advanced Finishing Supported	Analog Fax Capable
Analog Fax Description	Analog Fax Modem Installed
Analog Fax Phone Number	Black Copied Impressions
Black Copied Large Sheets	Black Impressions
Black Large Impressions	Black Printed Impressions
Black Printed Large Sheets	Black Rated PPM
Color Capable	Color Copied Impressions
Color Copied Large Sheets	Color Impressions
Color Large Impressions	Color Printed Impressions
Color Printed Large Sheets	Color Rated PPM
Console Language	Copied 2 Sided Sheets
Copied Impressions	Customer Asset Number
Detailed Device Page	Discovery Date
Discovery Method	Discovery Type
DNS Name	Duplex Capable
E-Mail Images Sent	Embedded Fax Images Sent
Embedded Fax Impressions	Embedded Fax Large Sheets
Fax Impressions	Finishing Options

Available CentreWare Web Alert Print Fields	
Firmware Level	Hard Disk Present
Hard Disk Size MB	Images Sent
Internet Fax Images Sent	IP Address Changed
IP Default Gateway	IP Source
IPX Address	IPX External Network Number
IPX Print Server Name	Large Impressions
Last Known IP Address	Last Status Attempt
Machine Up Time	Manufacturer
Marking Technology	Network Scanning Images Sent
Page Count	Page Count since Power On
Physical Memory Total MB	Printed 2 Sided Sheets
Printed Impressions	Printer Location
Printer MIB Language	Printer Web Page
Printer Web Server Enabled	Protocol Version
Queue Information	Scan to E-Mail Capable
Scan to File Capable	Scan to Internet Fax Capable
Scan to Server Fax Capable	Scanner Description
Scanner Installed	Serial Number
Server Fax Images Sent	Site Name
Status Date	Subnet Address
Subnet Mask	Supply Levels
System Contact	Target Volume
Total Impressions	Traps Enabled
Traps Supported	Utilization Percentage
Xerox® Asset Number	

Managing the Print Servers

Overview

CentreWare Web can manage local and remote Microsoft® print servers from a single administrative interface. CentreWare Web provides:

- Queue enumeration
- Driver installation
- Queue creation, editing, and deleting

By default, the CentreWare Web installer creates a user to administer the local server's print queues and places the account in the Administrator's Group.

If you use CentreWare Web to administer print queues on remote print servers, you must obtain the necessary administrator credentials for those print servers, either during installation or by utilizing the Xerox CentreWare Web Configuration Utility. If the credentials were not supplied during installation, you can configure them into CentreWare Web as described in the following section.

Modifying Advanced (Local and Remote Servers) Settings

To modify the Run As user for CentreWare Web after installation, use the CentreWare Web Configuration Utility. After changes are made reboot the server so that the components hereafter automatically start as the newly selected user.

Note: When you configure the CentreWare Web Run As user with administrative privileges for remote servers, any authenticated CentreWare Web user can perform queue administration on those servers. This includes print-driver installation and print-queue deletion. When enabling the Run As account for remote print server administration, use care when adding users to the CentreWare Web Users Group.

Domain or Local System Security Policies that mandate password updates will also affect this account. If possible, exclude CentreWare Web Run As from these policies.

Using WebDAV to Install the Print Driver for the Windows® Server

CentreWare Web utilizes Web-based Distributed Authoring and Versioning (WebDAV) to download and install the requested print drivers for the print server. WebDAV is the Microsoft® implementation of the Distributed Authoring and Versioning extension to HTTP/1.1 that facilitates efficient, secure maintenance of remote Web servers. It provides a network protocol for creating inter-operable, collaborative applications.

When you upload a print driver to either the CentreWare Web server or to a print server using CentreWare Web, a web service within CentreWare Web uploads the driver files to a web folder on the target machine. To take a more proactive stance against malicious users and attackers, IIS 6.0 is not installed on some members of the Windows® Server family by default. When you initially install IIS, the service is in a highly secure and locked mode. By default, IIS serves only static content—features like ASP, ASP.NET and Server-Side Includes.

You must enable WebDAV publishing to make it functional. Since CentreWare Web's driver file installation facility requires the use of a WebDAV-based web service, you must enable the WebDAV request handler, called WebDAV web service extension.

Note: "The WebDAV web service extension is not enabled by default to prevent possible malicious use. Before enabling WebDAV, you should thoroughly consider the additional risk it entails. Remember, WebDAV enables access to documents using Microsoft® Office, many versions of IE, and other products that meet the HTTP/1.1 WebDAV specification. It does so over port 80. Therefore, unlike file sharing, which can be blocked at the firewall, WebDAV manipulation of this data can be accomplished across a port commonly open on the firewall. If you intend to allow such access, you must ensure that other controls are in place. If you will be using WebDAV on your intranet only you must still take the appropriate action to block external access to port 80 of the WebDAV-enabled IIS server on your internal network." Excerpted from the free eBook "The Tips and Tricks Guide to Securing Windows Server 2003 (realtimepublishers.com) written by Roberta Bragg and available at http://www.netiq.com/offers/ebooks.(CentreWare Web Job Tracking is discussed later in this document.)

To enable WebDAV request handler:

1. From Computer Management, select Internet Information Services > Web Service Extensions.
2. In the Details pane, click the Web Service Extension that you want to enable or disable.
3. To enable a Web service extension, click **Allow**.
4. To disable a Web service extension, click **Prohibit**.
5. Click **OK**.

Creating a Queue

The easiest way to evaluate the queue management features of CentreWare Web is to create a queue on the same server where the CentreWare Web server is hosted, and then use the CentreWare Web Queue view.

To create a queue:

Note: If you have not previously configured the local CentreWare Web server to be a managed server, do that first so you can verify the queue installation via the Queues view.

1. On the Printers Page, click the check box next to the printer for which you want to create a queue.
2. Click **Install**. You are prompted to select a server. The local server is selected by default.
3. Select the appropriate server, if not the local server.
4. Click **Continue**. The saved configuration settings for this type of printer are displayed.
5. Check the driver signing policy displayed.
   - If CentreWare Web indicates that this server is accepting only signed drivers and the print drivers that will be used are unsigned, change the server's driver signing policy appropriately.

Note: Most versions of Windows require that the printer driver used must be a signed printer driver. These operating systems do not allow CentreWare Web to install an unsigned printer driver, regardless of the driver signing policy setting.

If there is a Domain policy for driver signing, it takes precedence over the local server policy.

If this model of printer has never been installed using CentreWare Web, you probably need to configure the queue setting using the Configure button. Refer to Configuring the Queue-Model Profile.

1. If you are prompted with a Security Warning for a custom control from Xerox Corporation (XrxDriver-Upload.CAB), click OK.
2. Select **Install**. This enables CentreWare Web's Have Disk option to download the driver to the server.

Configuring the Queue-Model Profile

To create the profile:

1. Verify that the port settings are correct for the type of print device you are installing. Consult the manufacturer's specifications for the printer.
2. Verify that the Run As user has Administrator rights on a server to the destination print server.
3. If the customer uses DNS/DHCP for printer addresses, select the Print Via Printer's DNS name option. The Queue/Share Name allows for a queue name template definition, where you can select between two predefined naming conventions or No Automatic Naming convention for print queues.
4. Select the print driver the print server is to use when auto-installing print drivers for driver "point and click" installation from the Install Drivers drop-down menu. Select one of the following:
   - Directly from Windows® server (but is not currently installed): No asterisk appears next to the driver name in the drop-down menu.

   - Drivers currently installed on the server: Denoted by a single asterisk next to the driver name in the drop-down menu.

   - CentreWare Web's Driver Repository: Denoted by two asterisks next to the driver name in the drop-down menu.
5. Click Have Disk to upload any print driver to CentreWare Web to install on the print server.
6. For the queue name, port name, share name, and queue comment, either accept the queue-model profile default or specify other names as required by local policy.
7. Set the printer location field stored in the device. When the queue is successfully installed, a green check mark displays in the results.
8. Add the successfully installed printer to some designated group.
9. Click on the printer's IP address to select the printer that you just installed.
10. Click **Troubleshoot**. The CentreWare Web Printer Troubleshoot dialog displays, giving immediate status on the printer. You can perform several remote diagnostic actions, including accessing the printer's internal web page, printing a test page, resetting the printer, and linking to the printer's online technical support.
11. Select Print Test Page Directly. A test print is sent to the print queue.
12. Verify that the test page printed.
13. To view the print server's print queue, click **Manage Queue**. There you can directly communicate with the print server's print queue interface.
14. To view the status and manage all of the print queues on a server, select Queue on the menu bar.
15. Once the servers are added, CentreWare Web enumerates all print queues.

Managing the Print Server Queue

This section describes how you can manage the print server queue, including the driver properties, adding or deleting a queue, etc.

EDITING THE QUEUE

CentreWare Web provides the capability to change/edit several print queue properties that are managed by the application, including:

- Name
- Share Name
- Location
- Comment
- Share
- Published in Active Directory®

Note: To evaluate the Edit Queue Properties capability of CentreWare Web, a print queue for a printer on a print server must be currently installed.

1. Select **Device Groups > Queues** on the Devices tab. The details for the queues displays.
2. Select the managed print server for the previously created queue.
3. Use the View Printer Properties icon to display the Printer Properties screen.
4. Click the Queue menubar located at the top of the webpage, and select Edit associated with print server. The Edit Properties screen for that queue displays.
5. Change queue properties, as necessary.
6. Verify that the queue properties modified are in effect on the print server.

Editing the Driver Properties

CentreWare Web provides the capability to redefine which print drivers are distributed by the print server when the shared queue is selected using Microsoft's Point and Print print queue sharing services. You can configure the print server driver repository with Windows® print drivers.

To configure the print server driver repository:

1. Click the Queue menubar located at the top of the webpage and select Edit associated with print server's drivers. The Driver Edit Properties screen for the print server displays.
2. Change driver properties, as necessary.
3. Verify that the queue driver properties modified are in effect at the print server.

Adding or Deleting a Server

The CentreWare Web Server enables you to centrally administer print servers without the need to use standard Windows® administration tools (e.g., Add printer wizard, etc.,) on each of your network print servers. This feature minimizes the time-consuming process of remote print server administration. CentreWare Web can manage most Windows® print servers.

CentreWare Web can also browse a network for available domains and Active Directory® partitions. Additionally, CentreWare Web supports the selection of multiple computers per domain when adding a new print server.

Adding a Managed Print Server

Use the procedure below to add a managed print server to your system.

To add a managed print server:

Important! Obtain administrative privilege credentials for any print servers that will be added in this test.

1. Select Device Groups > Queues on the Devices tab.
2. Select Managed Print Server > Add/Delete Server.
3. Enter a Server name or IP Address in the New Server IP Address or DNS Name field.

   Note: You could also select from a list of servers in a particular domain visible to the CentreWare Web server. This list is generated after you select the domain from Domain > Show computers. Click the right arrow to select the print server as a "managed print server".

   Immediately, CentreWare Web begins the process of installing the selected print server as a managed print server and enumerates the queues discovered.

4. Select the print server in the Managed Print Server navigation tree to verify that the new server now appears for the newly configured print server.

Deleting a Server

Use the following procedure to delete a server from your system.

To delete a server:

1. Select **Device Groups > Queues** on the Devices tab.
2. Select **Managed Print Server > Add/Delete Server**.
3. Enter a Server name or IP Address in the New Server IP Address or DNS Name field.

   Note: You could also select from a list of servers in a particular domain visible to the Xerox Device Manager server. This list is generated after the you select the domain from Domain > Show Computers. Click the left arrow to select the print server you want to delete.

   A confirmation dialog box appears asking you to verify that the print server is no longer considered a "Manage Print Server" and to remove it from the Managed Print Server.

4. Verify that the server was removed from the Queues folder.

Working with the Active Directory®

Active Directory is Microsoft's directory service, which is a collection of objects that represent physical and logical enterprise resources such as computers, printers, servers, shared folders, user accounts, groups, etc. A collection of these resource objects can be organized in a hierarchical, upside down tree-like fashion and stored in a database.

The CentreWare Web Server enables you to query a Windows® Global Catalog server and an Active Directory® Partition for those network printers that have associated Windows-based print server(s). CentreWare Web automatically queries the Global Catalog server and provides a list of available Active Directory Partitions. You can then select the appropriate Active Directory Partitions you want to check for network printer/queues.

When a network printer is detected from the Active Directory Partition, CentreWare Web checks its database to determine if the printer needs to be added. If the printer does not exist in the CentreWare Web Server's device database, it is added. If the printer does exist in the database, the Active Directory Partition attribute is then updated for that printer's record.

CentreWare Web also allows you to query Global Catalog servers. In any event, the CentreWare Web Active Directory feature causes more printers to appear in the default All printer group. This could be considered another form of printer discovery.

Adding or Deleting a Directory

Use one of the following procedures to add or delete a directory from your system.

To add an Active Directory:

1. Verify that you have administrative privileges for any active directories that will be added in this test.
2. Select Device Groups > Queues on the Devices Printers tab.
3. Select Active Directories > Add/Delete Directory.
4. Enter an Active Directory name in the Manual Entry field.
   Note: You can also select the directory from the Available Directories list, and click the right arrow. The Active Directory will have been added and is queried. Depending upon the number of printers, it may take several minutes for the detailed information about the printers to display. Select the added directory to view the contents.
5. Verify that the new Directory now appears in the Active Directories portion of the Managed Print Server navigation tree.

To delete an Active Directory:

1. Select Device Groups > Queues on the Devices tab.
2. Select Active Directories > Add/Delete Directory.
3. Select the directory from the Available Directories list and click the left arrow.
4. Verify that the Directory was removed from the Queues folder.
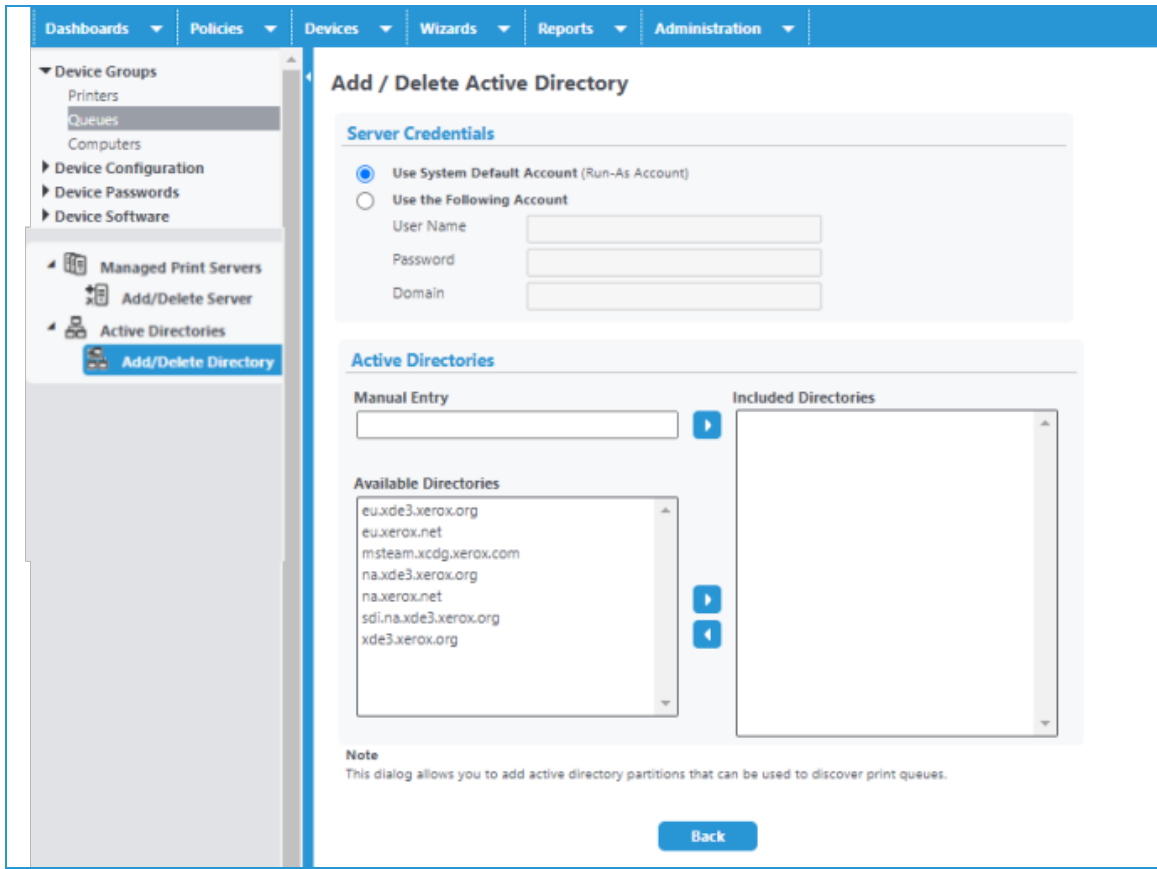
Importing Customers from the Active Directory

There are two modes in which you can automatically import customers from the Active Directory of your account:

• Disconnected Mode

In Disconnected mode, if there is an import currently in progress, CentreWare Web displays the <> symbol, and the screen alerts you that the import process is busy. Similarly, in Connected mode, if there is an import currently in progress, CentreWare Web displays the <> symbol and the screen alerts you that the Import process is busy. CentreWare Web then directs you to Xerox Services Manager, where it reports the status of the operation in the Import / Export log.

Note: Customers are only available in CentreWare Web after a sync operation is executed. You may click **Disable Import Now** to cancel the operation. If all the required fields are not completed for an Active Directory import, then a warning message displays at the top of the page and a red x displays next to the required fields that need to be completed.

Exploring The Active Directory Customer Import Screen

The following table describes the sections on the Active Directory Customer Import screen.

Section	Description
Import Status	Displays details about the last import made: • Last Import Start Date – date and time the last import began • Last Import End Date – date and time the last import completed • Last Import Status – whether or not the import completed successfully • Records Added – number of records added • Records Updated – number of records modified • Records Deleted – number of records removed • Records with Errors – number of records with errors after the operation
Active Directories	Manually enter the Active Directory that you wish to connect to or select it from a list of Active Directories. If you enter a name, the LDAP fields are loaded when the page is loaded. You can specify up to 10 Active Directories from which to import.
Import Option	Use this option to import entries from Active Directory. The system creates customers based on the entries in your Active Directory, so that you do not have to enter them manually. If you are not going to run the import immediately, schedule the import and whether to create, update, or delete the records.
Field Mapping	The Test button displays the mapping between the fields in the system and those obtained using the import from Active Directory. Complete the required fields marked by [1] when creating new customers. The Identification settings default to the expected value. CentreWare Web only displays the first several entries. In Connected mode, CentreWare Web sends the imported customers directly to Xerox Services Manager where Xerox Services Manager reports the status as an import in the Import / Export log. Customers are available in CentreWare Web after a sync operation is executed.

Working with Device Configuration Policy

Overview

In any managed site, there is a need to efficiently and effectively manage the settings common to a particular class of machine. In CentreWare Web, you can create policies and associate configuration sets with these policies. This can significantly aid in conformance stability, especially in a large fleet of devices and/or where there is a high level of device Moves, Adds or Changes. Configuration Sets provide a re-usable template to both monitor and set various device configuration parameters. To apply settings to these devices, you must first configure the Configuration Set.

CentreWare Web Configuration Sets provide the tool to record and maintain templates of device configuration settings. These configuration settings include:

- Asset
- Defaults
- Protocols
- Scan Services
- Security
- Job Accounting

The settings in each group display in the user interface in a tree-view format. You can also configure settings for non Xerox devices. Currently, this area supports only HP device-specific settings that are not related to Protocol settings. HP Protocol settings are configured in the same manner as Xerox devices. You can then schedule the Configuration Set templates to be applied to devices or to check compliance using Configuration Policies.

CentreWare Web Configuration Policies provide a task-based mechanism to schedule and monitor the application of Configuration Sets. Configuration Policies can have a set schedule, or can run on a device

discovery. You can create multiple Configuration Policies to apply differently configured Configurations Sets to devices based on existing groups in CentreWare Web, or on a specified filtered list of devices.

Periodic application of Configuration Sets can identify non-compliant devices (Audit Check Action) and also reset specific fields to conform to site requirements (Apply Configuration Set or Audit Check/Apply Configuration Set). You can create Configuration Sets from a blank template or from a pre-configured device to pre-populate a template. You can apply Configuration Sets to a single device or a group of devices for both checking and setting configuration.

Note: You can create a Configuration Set using a mix of device settings. Example: A Configuration Set can include a combination of some Protocol, Security, and Network Scanning settings.

Some fields in a Configuration Set are appropriate only to a specific model, some are generic and can be applied to any model, and some are appropriate for only a specific support or service function, but appropriate for many model types.

Each Configuration Policy maintains the result of the policy, providing valuable information on what task was performed and against what devices. The results show what happened the last time the Configuration Policy ran. The results can also be e-mailed to any recipients by enabling the Configuration Policy Audit Notification on the Audit Notification tab in the Configuration Policy. You must also configure the CentreWare Web Server for an E-Mail server in Administration > Network > E-Mail & External Servers.

The Audit Check Report reports the results of multiple Audit Check Configuration Policies simultaneously, providing an audit history. The Audit Check Report is in the Reports menu option.

Recommended Usage

- Apply policies to groups and monitor them for compliance and remediation in the dashboard.

- Use the Check Configuration Set to confirm which settings need to change and which should remain. There might be specific printers that require settings that are different from standards; individual requirements should be confirmed.

- Test the configuration. Apply the Configuration to one device while that printer status is visible.

- Confirm that the outcome of the new device settings is as expected. Different firmware levels in the same product family might behave differently—multiple firmware levels on the devices in the same family might suggest multiple tests.

- Apply the Configuration to a known group of printers and confirm the status and setting.

- Use the Audit Check to audit devices against defined configurations.

- Use the Audit Check /Apply Configuration to the first audit devices and then to reapply the appropriate configuration.

- Use Reset Devices to schedule a device reboot for devices selected. This does not check or apply configuration settings.

Using Configuration Sets

This section describes how you can create, delete, or copy an existing Configuration Set, or create a Configuration Set by copying the settings from a device that has the desired settings.

Follow the steps below to create a Configuration Set.

To navigate through the possible configuration settings and property panels, use the arrows on the left navigation to expand and collapse features and sub-features.

Search Configuration Properties

You can also search for device configuration properties. In the search text box enter the device property in which you are interested and click **Enter**. To search on multiple keywords use a plus sign (+) to add terms. Click **X** to clear the results. The tree view filters to list only the nodes for the property on which you searched.

Create a Configuration Set

1. Select **Policies > Configuration > Configuration Sets.**
2. In the Action menu select New and click **Apply**.
3. On the Identity tab configure the Set Identity Information. Configuration Set Name is required to uniquely identify the Configuration Set.
4. Configure the settings on the following tabs:
   - Asset: In this section, you can add a Workplace App in order to deploy App Gallery weblets to devices. Use this section to standardize Workplace Apps across the device fleet. See the Other Actions section below for more information.
   - Defaults

        Note: You can opt to suppress toner warnings in the Display Low Supply Warnings on Local UI section.
   - Protocols
   - Scan Services
   - Security
   - Job Accounting
   - Other: The Other tab contains settings for non Xerox devices, and currently only supports HP default settings. HP Protocol settings are configured along with Xerox® Protocol settings. All other HP settings that are configurable are contained in the Other tab.
   - Summary: The Summary tab displays the device property path and the value set. Click on the path to go the specific feature setting.
5. Click **Save**. The Configuration Set is saved.

Other Actions

To install weblets to ensure all devices in fleet have same set of apps:

Before getting started, create a printer group and map the Xerox devices in that group. Be sure enable the [Extended Data Retrieval] option from the Group Config Settings. This allows you to to run a Workplace App Distribution Report after the process is complete, and check if your Apps are pushed to devices.

Follow the steps below to push weblets to devices.

1. Follow the process to add a configuration set. Go to **Asset > EIP > Workplace App Management Node.**
2. In the Workplace App Management section, select the Workplace App Actions checkbox, in dropdown choose the Add Workplace Apps option. Invoke the Add Weblet option from the Action menu to open the Upload Workplace Apps page.
   Note: Use the Add Configuration Template option in the Workplace App Actions to flush and fill the

Workplace Apps on the device fleet. The Workplace Apps installed in the devices will be deleted and the Apps added in the Configuration Set will be installed.

3. Select **Actions >New** to add an EIP application. Enter the weblet files in the Workplace App Upload section.

4. Once all the required apps are added, save the configuration set.

5. Use this configuration set to create a configuration policy, and run it in Enforce mode. This is the normal configuration policy workflow.

6. Use the appropriate options available in the section to add or remove individual apps with the same method.

To delete a Configuration Set once it has been saved:

1. Select **Policies > Configuration > Configuration Sets**.

2. Check a Configuration Set you want to delete.

3. In the Action menu select Delete Sets and click **Apply**. Click **OK** to confirm your decision. The Configuration Set is deleted.

To copy a Configuration Set once it has been saved:

1. Select **Policies > Configuration > Configuration Sets.**

2. Check each Configuration Set you want to copy.

3. In the Action menu select Copy Set and click **Apply**. The Configuration Set is copied and the Edit - Copy of [Configuration Set] opens.

4. Rename your configuration set and revise any properties. Click **Save**.

To create a Configuration Set from a device:

1. Select **Devices > Printers**.

2. Select the View icon for the desired printer from the printer list.

3. Select **Actions> Save as New Configuration Set**.

4. Use the default Set Name, or define a new one.

5. Edit the New Configuration Set, if necessary.

6. Click **Save**. The Configuration Set is saved.

Note: You can add an externally hosted, third party EIP application in a Configuration Set from **Asset > EIP > Workplace App Management > EIP Applications**. (We do not support Xerox-hosted EIP applications.)

Configuring Devices Remotely

You can use configuration sets to configure a newly installed device remotely. Rather than have a carrier perform the initial set up at delivery on site, the CentreWare Web administrator can create and schedule a configuration set and policy to perform this function. They then turn off the Install Wizard screen for the device.

Requirements:

• 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 CentreWare Web.

- Available only for devices that support remote Install Wizard settings.

To use this feature follow the steps below:

1. Create a configuration set that includes disabling the Install Wizard screen (Security/Disable Services tabs)
2. 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.
3. Run Discovery that includes the subnet for the new device (either through schedule or on demand).

Creating Configuration Policies

Policies allow you to manage a fleet's configuration—both firmware and configuration sets. There are extensive configuration options that can be linked to individual or multiple groups. Configuration policies offer a more intuitive way to update and audit device settings. When you create a policy and apply it to groups, it is used as the basis for policy execution and reporting. Taken in conjunction with the Dashboard, which is a graphical display of compliance successes and issues that you can drill down into for details, configuration policies are a powerful tool for fleet management.

1. Go to **Policies > Configuration > Configuration Policies.**
2. In the Action menu select New and click **Apply**.
3. On the Identity tab click **Enable** to turn on the policy. Enter a name and description. Click **Next**.
   Note: This tab also contains details about when the policy was last run or edited.
4. On the Actions tab complete the following fields as needed, and click **Next**.
   - Actions Section:
     - Audit: Select to check whether the specified devices match the configuration set.
     - Enforce: Applies the configure settings to devices.
     - Reboot Devices Only: This is unselected by default. Use this option for troubleshooting devices. It will not check or apply settings.
   - Configuration Profile Section:
     - Choose one or more configuration sets from the drop down.
     - If you select Skip non-compliant settings at Configuration Task Runtime, at runtime the task will compare all settings in the configuration set against the Compliance Database in CentreWare Web and ignore settings that are not compliant for each individual device. Skipped settings will be logged in the task and policy results tabs. Skipped settings will not be counted against policy compliance on the dashboard screens.
   - Schedule Options Section set the frequency and the next date and time.
     - If you do not want to schedule a run date/time for the policy, set the frequency to Run Manually. This disables the scheduler. You can edit the schedule options later if you no longer wish to run the policy manually.
     - You have the option to apply the policy to a device when it is first discovered.
5. On the Assign tab, select the groups or individual devices to which you will apply the policy. You may assign groups that do not contain any printers; however, the policy will neither audit or enforce until devices are added to the group.
   Note: You must assign printers by group, in order for those devices to report on the Dashboard.

- Assign: Choose the device or device groups.

  - Group: From the drop-down list choose the groups to which you will apply the policy.

  - Assign Printers: Select the desired printers to be part of the policy (if the policy is not linked to a group)

- Advanced: Create a device expression that further specifies to which printers the policy is assigned.

- Device Admin Password: Choose Auto to use the default password, or select Specified and enter the Administrator user name and password.

6. On the Audit Notification tab indicate who will receive emails about configuration policy status and what the notification will contain. Send E-Mail Notification to turn the notifications on and open the fields for updates; it is off by default. You have the option to only send notifications for errors or warnings.

7. Click **Save**.

8. After a policy runs, go to the Dashboard to view the compliance dashboards.

Editing a Configuration Policy

Follow the steps below to edit a firmware policy. You cannot edit a policy that is running.
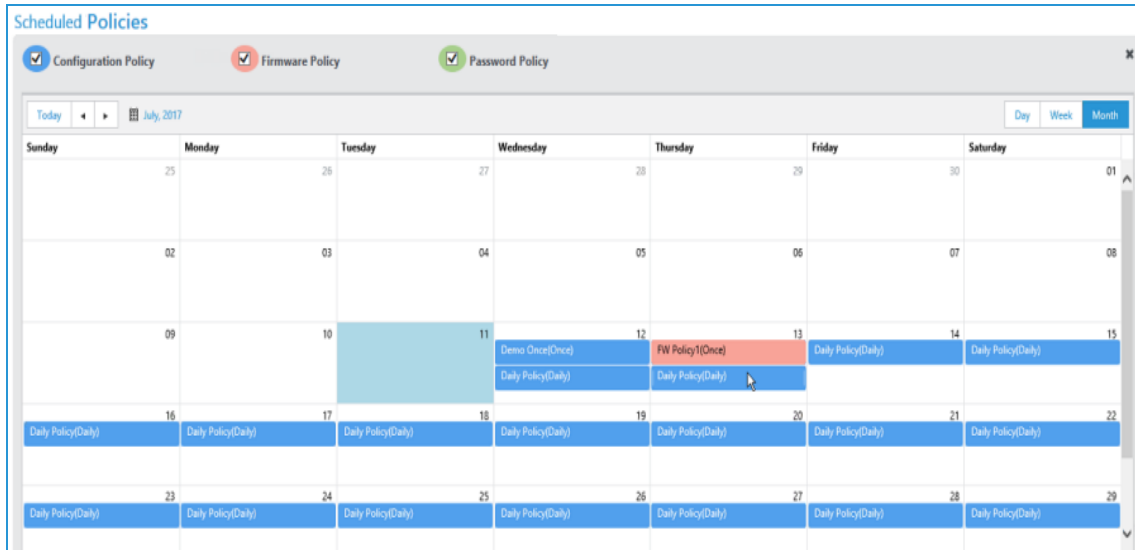
1. In the Configuration Policies screen, select a policy and click the **Edit** icon.

2. You may modify the settings on the Identity, Actions, Assign, and Audit Notification, as needed.

3. In addition, in the Edit Details view, the Identity tab has a Last Run Details section for the policy. This shows the last change that took place. Click **Result** to link to the results. In the Results table, click a row to see details from that instance.

In Addition To The Actions Described Above, You Can Also Do The Following:

- Run: Enforces the selected Configuration Policy.

- Delete: Deletes a selected Configuration Policy.

- View Results: Click the pie chart icon in the table to see the current status and progress of a selected Configuration Policy and the results of a completed Policy.

- Conflict Status: In the Policy Status column click the conflict status to see details about the conflict. feature, sub-feature, and configuration sets.

Scheduled Policies

Once a configuration policy, firmware policy, and password policy have a scheduled time, then all the scheduled tasks display. You can access the schedule from Policies > Scheduled Policies.

- Use the checkboxes at the top to choose which types of policies display. The color for the policy type in the header corresponds to the color of the scheduled task in the calendar.

- Use the buttons above the calendar to choose whether to display scheduled tasks by day, week, or year. Use the navigation buttons on the top left to move backwards and forwards through the calendar.

- Hover over the scheduled task to see details about the policy.

Changing the Scheduled Policy Occurrence

If you find conflicts in the scheduled task calendar, you can change the schedule.

1. Go to **Policies > Scheduled Policies**.
2. Select the policy you want to reschedule and drag it to its new time. A policy scheduled to run once is done after this step.
3. If the policy is recurring, when you drag it to the new time, the Configuration Policy Schedule pop-up opens. Set the frequency for a periodic schedule (Once, Hourly, Daily, Weekly). Set a start date and time for the periodic schedule.
4. Click **Save**.

Working with Device Password Policy

Overview

Device Password Policies allows you to manage the password policies for multiple devices across an account. This section is subdivided into:

- Password Policies
- Stored Device Passwords

CentreWare Web can support password updates at scale (i.e., 1000 devices as part of policy/configuration set). This feature includes the following capabilities:

- Ability to track previous passwords for each device in CentreWare Web.
- Ability to track when a password was set in CentreWare Web.
- Ability to audit known device passwords.
- Option to retry the default admin password to find and update the incorrect one stored in CentreWare Web
- Ability to change passwords using the list of devices and show password to administrators.
- Audit Report for verified passwords (admins only).
- Audit page for verified passwords (admins only).
- Ability to change passwords for single devices or a set of devices.
- Enable a unique password for each device that is either system-generated or user-generated
- Ability to create unique password per device by using uniqueness pattern by prefixing Serial Number/MAC Address.
- Create unique password per device by appending a sequence number or date stamp with the password.

The Password Policies grid shows the policies that have been created and their status. Within the grid you can create, delete, audit, update, and stop policies. You also have the capability to edit and view the status of the policy in the dashboard.

Creating New Password Policies

Follow the steps below to create a new password policy for a group of devices.

1. Go to **Policies > Passwords > Password Policies**.
2. In the Action menu select New and click **Apply**. The New Password Policy screen displays. Complete the Identity, Actions, Assign, Audit Notification, and Results Options tabs.
3. On the Identity tab click **Enable** to turn on the policy. Enter a name and description. Click **Next**.
4. On the Actions tab complete the applicable fields and click **Next**. One or both of the sections must be enabled.
   - Monitor and Remediate Password section: The Enable Password Audit option allows you to check device passwords against stored passwords and set up a schedule for that audit. If you enable Serial Number Retry, the serial number can be set as the default password. This allows the device management applications to test a device's Serial Number as the administrator password for audit purposes.
   - Update Password section: You may opt to have a user-generated or system-generated password. If you select a system-generated password, you can further configure the password complexity and length.
   - You can have the policy create device unique passwords for user-generated sources by appending a unique identifier and/or the date. The password complexity for system-generated passwords is defined as follows:
     - Low: A random string containing only digits (0-9). (e.g. '14128')
     - Medium: A random string containing letters (a-z and A-Z) and digits (0-9). (e.g. 'q8TuvW51')
     - High: A random string containing letters (a-z and A-Z), digits (0-9), and the following characters: ! # $ % & ' * + - / = ? ^ _ ` { | } ~ ; . (e.g. 'Uz$8rS*!Oq')
5. On the Assign tab you can select the printers to which the policy applies. Then click **Next**. You may assign groups that do not contain any printers; however, you can neither audit nor enforce the policy until devices are added to the group.
   - Group: From the drop-down list choose the groups to which you will apply the policy. If you toggle on the option to Link the Policy to Selected Group(s) then the policy will automatically be applied to any devices added to the group. The policy will also be disassociated from any printers that leave the group.
   - Assign Printers: Select the desired printers to be part of the policy (if the policy is not linked to a group).
6. On the Audit Notification tab indicate who will receive emails about password policy status and what the notification will contain. Enable Send E-Mail Notification to turn the notifications on and open the fields for updates; it is off by default. Click **Next.**
7. On the Result Options tab customize what data you want to include in the dashboards and the notifications.
8. Click **Save**.

After a policy runs, go to **Dashboards> Password Compliance** to view the related compliance dashboards.

To delete a policy file, select it from the grid, choose Delete in the Action menu and click **Apply.** Confirm your selection.

Manually Audit and Update Password Policies

You have the option to manually initiate a password policy audit or password update. In order to manually audit or update, the policy must support these options.

1. Select the policy you want to manually audit or update in the grid.
2. Choose an action.
    -   Select **Audit Now** and click Apply to check the passwords for compliance. If the audit finds passwords that are out of compliance, it will attempt a remediation.
    -   Select **Update Now** and click Apply to cause the policy to update the passwords.
3. Click the **View Results** icon to see the progress and results of the audit or update.

Editing Password Policies

Follow the steps below to edit a password policy. You cannot edit a policy that is running.

1. In the Password Policies screen, select a policy and click the **Edit** icon.
2. You may modify the settings on the Identity, Actions, Assign, Audit Notification, and Result Options tabs, as needed.

In addition, the Edit Details view shows the change history for the policy. Click **Result** to link to the results. In the Results table, click a row to see details from that instance.

Viewing and Updating Passwords

In the Stored Device Password section you can manage the passwords for devices. The grid displays all the printers in the selected groups for password policies. The grid also shows passwords for any devices in the database for which CentreWare Web knows the password (i.e., manually entered in the device edit properties). By default, the password is hidden, but you can select devices in the grid and click **Show All Passwords** to display the actual passwords in the Password column.

Applying a Password

Note: Updating the password within the Stored Device Password only updates it in the database to match what is currently on the device. It does not change the password on the device.

1. Go to **Policies > Passwords> Stored Device Passwords**.
2. In the Update Stored Device Admin Password field enter a new password. The password must be between 4 and 63 characters.
3. In the Verify Password field re-enter the same password.
4. In the grid, select the printers to which you want to apply the new password.
5. Click **Apply to Selected**.
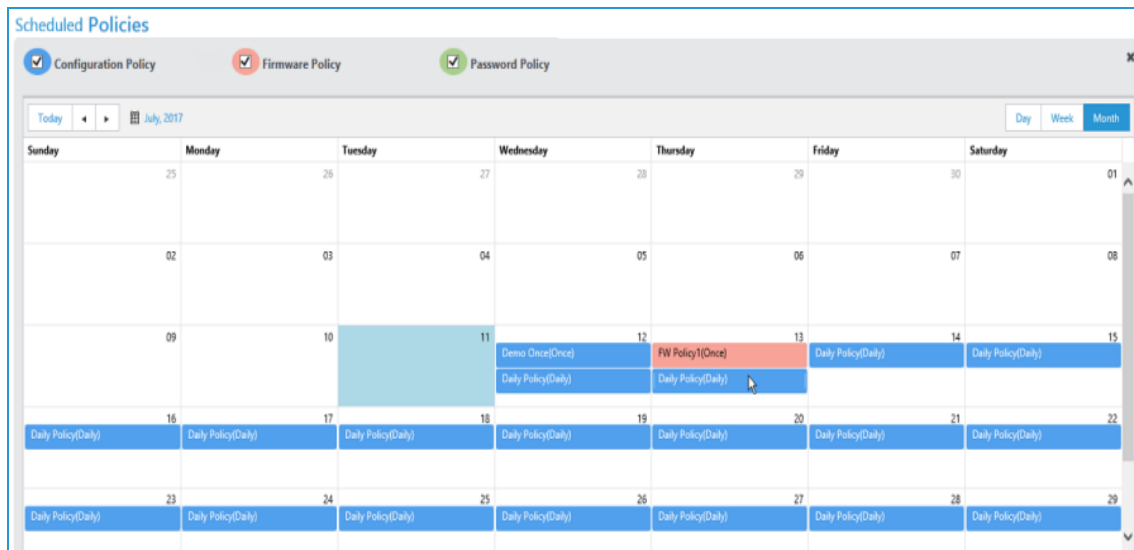
Importing Passwords from CSV File

1. On the Stored Device Passwords page click the Import Passwords from CSV File link. This takes you to **Administration > Advanced > Import Device Passwords**.

2. On the Import Device Passwords screen enter or browse for the correct CSV file and click **Import**.

3. If you do not have a CSV file of passwords, you can click **Export Template**. Complete the Admin User Name, Password, Serial Number, and MAC Address fields and save the file.

4. Click **Import**.

Scheduled Policies

Once a configuration policy, firmware policy, and password policy have a scheduled time, then all the scheduled tasks display. You can access the schedule from Policies > Scheduled Policies.

- Use the checkboxes at the top to choose which types of policies display. The color for the policy type in the header corresponds to the color of the scheduled task in the calendar.

- Use the buttons above the calendar to choose whether to display scheduled tasks by day, week, or year. Use the navigation buttons on the top left to move backwards and forwards through the calendar.

- Hover over the scheduled task to see details about the policy.

Changing the Scheduled Policy Occurrence

If you find conflicts in the scheduled task calendar, you can change the schedule.

1. Go to **Policies > Scheduled Policies**.

2. Select the policy you want to reschedule and drag it to its new time. A policy scheduled to run once is done after this step.

3. If the policy is recurring, when you drag it to the new time, the Configuration Policy Schedule pop-up opens. Set the frequency for a periodic schedule (Once, Hourly, Daily, Weekly). Set a start date and time for the periodic schedule.

4. Click **Save**.

Working with Device Firmware Policy

Overview

A firmware upgrade policy gives you the ability to manage and deploy firmware changes to an entire fleet of printers in order to improve printer capabilities and functions. The Firmware Version Policies pages have a streamlined look and additional functionality, such as scheduling retries for failed upgrades, and adding options to restart only failed upgrades.

In addition to our standard method of updating firmware on your devices, we also offer a hub and spoke model for firmware deployment for Xerox® Altalink® devices. We are also compatible with Fleet Orchestrator; a hub and spoke model for firmware deployment to Xerox® Altalink® devices.

Firmware upgrades can:

- Supply corrective actions
- Enable new features
- Extend support capabilities for existing print devices

CentreWare Web provides a simple procedure to:

- Organize printer firmware upgrade files
- Select a population of devices for upgrade
- Schedule the upgrade
- Report back on the success or failure for each device
- Schedule retries for failed upgrade and restart upgrades that have failed.

To navigate to this screen go to **Policies > Software > 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.

We support updating Xerox printers, HP printers, and HP JetDirect cards, Lexmark, and Honeywell. The manufacturers whose devices we support continues to expand.

Notes:
- The task list of printers to be upgraded is kept in the database so if there is a failure in the CentreWare Web server, the process restarts at the last stage of the upgrade task.
- An upgrade task in progress can be Stopped, Restarted or Deleted. A new upgrade task cannot be started until the final device of the previous upgrade task has reached the verifying state.
- Typically, the device goes offline as it reboots to apply the upgrade file. It must be contacted again to confirm the upgrade was successful.

Adding / Deleting Files to the Repository

Use the Software File Repository to house the files you need to support upgrades. Generally, these files can be downloaded from the device manufacturer's site.

1. Click **Software File Repository** to view the Software File Repository grid.
2. If the appropriate upgrade file is not available, in the action menu select Add File and click **Apply**.
3. Select the Manufacturer from the drop-down list. A link to the manufacturer's website displays.
4. Select either the exact model printer for which these files are appropriate from the drop-down menu, or when a file may be appropriate for multiple members of a family, select Printer Model Contains, and specify the string to be matched.

Note: For HP devices, only the Printer Model Contains option is available.

1. Click **Browse** next to Upgrade File. You can now upgrade the uncompressed file.
2. Highlight the file and select [**Open**] in the Choose File box.
3. By default, Qualify is set to **Off** for all upgrade files. When Qualify is off, the upgrade file may only be sent to one device at a time. You may also change the Qualify setting from the Firmware File Repository grid. Change Qualify to **On**, if you want to send the file to any number of devices simultaneously.
4. If there is relevant documentation associated with this particular upgrade, select Attachment, and then select the appropriate file. You should attach Word (.doc), text (.txt), PowerPoint (.ppt) or Adobe (.pdf) files.
5. Enter a short explanation for why or when to use this file in the Description field.
6. Click **Save** to return.

To delete an upgrade file, select it from the grid, in the action menu select Delete File, and click **Apply**. Confirm your selection.

Creating a New Firmware Policy

This section describes how to create a firmware policy. To create a firmware policy:

1. Select **Policies > Software > Firmware Policies.** The Firmware Version Policies screen displays.
2. In the Action menu select New and click **Apply**. The New Firmware Policy screen displays. Complete the Identity, Assign, and Schedule tabs.
3. On the Identity tab, complete the following fields as needed, then click **Next**.
   - Enable: Toggle to enable/disable the policy.
   - Policy Name: Enter a unique name.

- Type: From the drop-down list choose the policy type. The policy type drives the rest of the configuration within the policy. When you choose Monitor or Monitor and Automatically Upgrade, these policies report through the Dashboard, so that you can see how compliant the fleet is to a given version of firmware.

  - Monitor Only: Monitors the firmware upgrade for the desired versions.

  - Schedule Only: This allows you to upgrade the firmware to the desired version without any monitoring. Note you cannot downgrade firmware remotely. This is most similar to earlier version's Upgrade Printer Wizard.

  - Monitor and Automatically Upgrade: Monitors the firmware version and attempts to upgrade if the version is not on the desired version. Note, you cannot downgrade firmware remotely.

- Model Selection: Choose a printer model from the drop-down list or the Printer Model contains option.

- Use Fleet Orchestration Method: The Fleet Orchestrator method configures devices to pull the file at the scheduled runtime of the policy. The default topology for this distribution is flat; in other words, all devices in the schedule will make a request to CentreWare Web, which will respond with the file. When you select this option, an alert pops up noting a CA signed certificate is recommended, and advising on additional required steps.
  Note: Currently, we only support Xerox® Altalink®devices.

- Description: Enter a short explanation for why or when to use this file.

- Monitor: For a Monitor task or a Monitor and Automatically Upgrade task, you need to set a version for which to check. For Monitor and Automatically Upgrade only, you also have the option to upgrade for multiple versions of the firmware if you enable the version range. In this case, the policy only upgrades when the firmware of the device is within a specific range of versions. If the major version were upgradeable to 073 firmware only when the device is on 072, then the range would be set to min 072 and max 072. Then, when the firmware is not on the desired version and it is within the version range, the system will trigger the upgrade at the scheduled time. You can then set up multiple policies to cover the entire range of possible firmware versions, and the firmware will upgrade each night when it isn't on the desired version.

- Upgrade: Click **Select** to choose a single file for upgrade. In the Upgrade Files pop-up choose a file. These files are typically downloaded from the device manufacturer site. If they are in compressed file format (Zip, Rar, or other), uncompress them to a known file location. The list of upgrade files can be modified through the File Repository.

Note: For the following devices, you must have the admin user name and password saved in CentreWare Web in order to upgrade them: PX4i, PX6i, I-Class, H-Class, M-Class, A-Class.

4. On the Assign tab you can select the printers to which the policy applies. You may assign groups that do not contain any printers; however, you can neither audit nor enforce the policy until devices are added to the group.

   - Group: From the drop-down list choose the groups to which you will apply the policy. If you toggle on the option to Link the Policy to Selected Group(s) then the policy will automatically be applied to any devices added to the group. The policy will also be disassociated from any printers that leave the group.

   - Use Hub and Spoke Mode: Toggle to enable/disable the method of firmware policy upgrade. When enabled, the system will assign a device on the subnet as hub and the remaining devices will be spokes. This improves overall deployment speed to a fleet of devices, as it distributes the network load across the network since devices can request the file from other devices, rather than all devices requesting it

from **CentreWare Web**.

- Assign Printers: Select the desired printers to be part of the policy (if the policy is not linked to a group).

5. Click **Next** to continue.

6. On the Schedule tab you can schedule the time to monitor, monitor and upgrade, or schedule a date/-time to run an Upgrade Only. You can schedule when, and how often to poll the results from the printer. You can set retry attempts for any devices that the version does not change after the polling window.

   - Schedule: The options vary depending on the policy type.

     • Schedule Upgrade Only: You can choose to Upgrade Now or Upgrade Later and set a start time.

     • Monitory Policy Types: Set the Policy Check Start time.

     • Regardless of policy type, you have the option to Hold Auto Upgrade for Manual Release. This means that you can perform a verification before the upgrade is set.

     • The Advanced settings are available with Fleet Orchestrator and offer greater flexibility for when the policies download and actually install. In addition to setting different download and install times, you can set a delay interval so that devices do not all communicate with CentreWare Web at the same time when they call to request the file.

   - Checking the Upgrade Results: Polling allows us to determine if the upgrade is successful because we can check if the firmware version changed.

     • Poll every: Set time in minutes.

     • Poll for a duration of: Set time in minutes.

   - Retry: For Scheduled Upgrades you can allow up to 5 retries. For Monitor policy types, only one retry is allowed.

     • Enabled: Toggle on and off.

     • Number of Retries: Options depend on your policy type.

     • Hours Between Retries: Choose how many hours between retries. For example, if a retry is unsuccessful because a device is turned off, it might be better to wait before trying again, so that the device has time to come back online.

     • Retry Window Enabled: Enable to specify the times during which retries can run. For example, you could set the retry window to exclude morning hours.

     • Retry Window Start Time: Enter start time for retry window.

     • Retry Window End Time: Enter end time for retry window.

7. On the Audit Notification tab indicate who will receive emails about firmware policy status and what the notification will contain. Toggle send E-Mail Notification to turn the notifications on and open the fields for updates; it is off by default. You have the option to only send notifications for errors or warnings.

8. Click **Save**.

Firmware Upgrade Policies that are set as Monitor or Monitor and Automatically Upgrade are also reported through the Device Dashboard if enabled, so that you can see how compliant the fleet is to a given version of firmware.

Manually Releasing an Upgrade

If you have set the Hold Auto Upgrade for Manual Release option on the Schedule tab, you will need to manually release the policy upgrade from Firmware Version Policies.

1. Select the policies that you want to release in the table. The Policy Status will be Hold for the policies you want to release. You can select multiple policies.
2. Click **Yes** in the confirmation pop-up.
3. Click **Release Upgrade**.

When upgrading the printer firmware:

- Use meaningful names for software upgrade files uploaded to CentreWare Web.

- Add release notes and clear descriptions to identify reasons for the upgrade.

- Use dynamic groups to organize printers that need to be upgraded.

- Ensure all faults are cleared from the target devices before applying the upgrade.

- Test the upgrade file on the target machine before applying it to the fleet.

- Apply software upgrade files after regular business hours to increase the probability of success.

- Rediscover newly-upgraded printers so CentreWare Web can detect changes in FW/SW levels.

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. Think of the deployment task being created or updated to enforce the policy. The table tracks the results of the policy.

Editing a Firmware Policy

Follow the steps below to edit a firmware policy. You cannot edit a policy that is running.

1. In the Firmware Version Policies screen, click the **Edit** icon for the policy you want to revise.
2. You may modify the settings on the Identity, Assign, and Schedule tabs, as needed.
3. In addition, in the Edit Details view, there is a History tab for the policy. This shows the last change that took place. Click Task History to link to the results. In the Results table, click a row to see details from that instance.

Miscellaneous Tips

- The task list of printers to be upgraded is kept in the database so if there is a failure in the CentreWare Web server, the process restarts at the last stage of the upgrade task.

- An upgrade task in progress can be Stopped, Restarted or Deleted. A new upgrade task cannot be started until the final device of the previous upgrade task has reached the verifying state.

- Typically, the device goes offline as it reboots to apply the upgrade file. It must be re-contacted to confirm the upgrade was successful.

Scheduled Policies

Once a configuration policy, firmware policy, and password policy have a scheduled time, then all the scheduled tasks display. You can access the schedule from Policies > Scheduled Policies.

- Use the checkboxes at the top to choose which types of policies display. The color for the policy type in the header corresponds to the color of the scheduled task in the calendar.

- Use the buttons above the calendar to choose whether to display scheduled tasks by day, week, or year. Use the navigation buttons on the top left to move backwards and forwards through the calendar.

- Hover over the scheduled task to see details about the policy.

Changing the Scheduled Policy Occurrence

If you find conflicts in the scheduled task calendar, you can change the schedule.

1. Go to **Policies > Scheduled Policies**.
2. Select the policy you want to reschedule and drag it to its new time. A policy scheduled to run once is done after this step.
3. If the policy is recurring, when you drag it to the new time, the Configuration Policy Schedule pop-up opens. Set the frequency for a periodic schedule (Once, Hourly, Daily, Weekly). Set a start date and time for the periodic schedule.
4. Click **Save**.

Managing Users

Overview

Use the application to create customers (end users), import customers from a formatted file, or import them from an Active Directory. Customers can then be associated with Chargeback codes that can be used during Job Tracking activities.

Managing the Customers

CentreWare Web provides the capability to add and edit customers. You can create or modify the list of customers on the Customer Management screen.

To manage customers:

1. Select **Administration > User Management > Customers(End Users)**. The Customer Management screen displays.

2. Complete the information, as necessary
   - Customer Actions:
     - New Customer: Add a new customer
     - Import Customers: Import an existing customer from a file
     - Delete Customer: Remove an existing customer
     - Export Customers: Export the existing customers to a file

- User Configurations:

 • Identity: Customer properties, such as first name, last name, email address

 • Chargeback: Customer-associated chargeback codes

You can add customers manually or import them via a CSV file.

To import customers:

1. Select Customer Actions > Import Customers. The Import Customers screen displays.
2. Enter the file name or browse to and select the file.
3. Click **Import**. The Import Users screen displays.
Note: For the import file format, use the "Export Template" option.

You can also export a file of customers from CentreWare Web.

To export customers:

1. Select Customer Actions > Export Customers.
2. Click All Customers to export the entire listing of customers. Click Customers to export only those customers checked in the Customers and Chargeback Codes view.
3. Click **Download**. The file is saved.

Configuring Groups

CentreWare Web provides the ability to group customers. You can create or modify the group on the Group Configuration Management screen.

To configure groups:

1. Select **Administration > User Management > Group Configuration**. The Group Configuration Management screen displays.
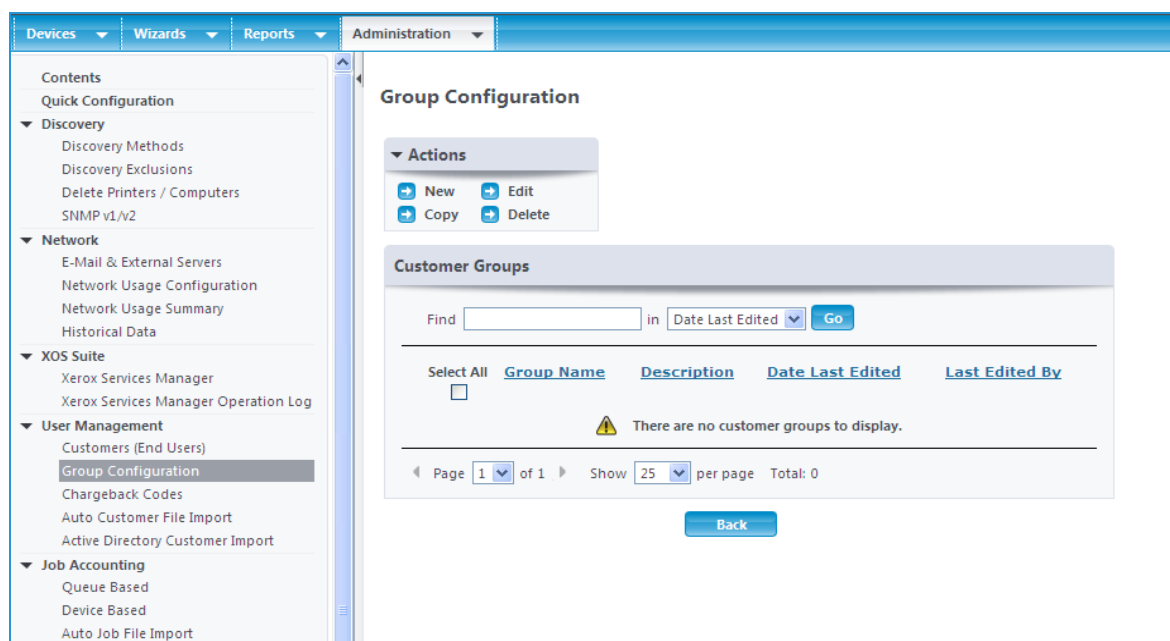
2. Complete the fields, as necessary.

- Customer Actions:
  - New: Add a new group
  - Edit: Change configurations for an existing group
  - Copy: Create a copy of an existing group
  - Delete: Remove an existing group
- Group Configurations:
  - Details: Group identity details, such as group name and description
  - Customers: Customers that are part of this group. You can add existing customers known to CentreWare Web.
  - Domain Groups: AD (windows domain) groups. If an AD group is included, all users in that group are automatically part of this group. You can include groups from active directories that are included in the same trust relationship as the CentreWare Web Server.

Managing Chargeback Codes

CentreWare Web provides the ability to manage chargeback codes. You can create or modify chargeback codes on the Chargeback Code Management screen.

To manage chargeback codes:

1. Select **Administration** > **Job Accounting** > **Chargeback Codes**. The Chargeback Management screen displays.
   - Actions:
     - New: Add a new chargeback
     - Edit: Edit an existing chargeback.
     - Delete: Remove an existing chargeback
     - Export: Export a list of chargebacks
   - Chargeback Code Configuration Items:
     - Name: Official name of the chargeback code
     - PIN: Identifier for the code
     - Description: Optional text description of the code

   Note: You can associate selective chargeback codes with customers, and configure the list of associated chargeback codes with any customer on the Customer Management screen.

Importing an Auto Customer File

You can schedule and automatically import customers to CentreWare Web using the Auto Customer File Import feature.

To perform an Auto Customer File import:

1. Select **Administration** > **User Management** > **Auto Customer File Import**. The Auto Customer File Import Management screen displays.

2. Check the Enable Scheduled Import option.

3. Enter a directory reachable from CentreWare Web in the Import Directory Path field. If the defined directory does not already exist, CentreWare Web creates it.

Importing the File

If you export files in a suitable format from the third-party application into the Import Directory defined above, within a few minutes CentreWare Web processes them. The first time that happens, CentreWare Web creates two sub-directories in the Import Directory called done and exec. When CentreWare Web is ready to process the import file, it moves the file from the Import Directory to the exec sub-directory. Processed files are then moved from the exec sub-directory into the done sub-directory. Depending the success of the import, the output can vary:

- If the import was completely successful:
  - The import file is moved to the done directory and no other output file is created.
  - CentreWare Web is populated with all the data from the import file
  - The Windows Application Event Viewer shows two informational events on the success of the import
- If the import was partially successful, but some records could not be imported (e.g., because they had no entry in a required field):
  - The import file is moved to the done directory and a new file with the same name, but with "_errors" appended, is also created and contains a copy of records not imported. There is no indication as to which fields are in error or the actual nature of the error
  - Successfully imported records are added to the users table in the CentreWare Web database.
  - The Windows Application Event Viewer shows two events: one that the import has completed and one showing the number of records that could not be imported and the total number of records in the import file.

- If the import file cannot be read at all by CentreWare Web (e.g., the file format is not a supported CSV format):
  - The import file is moved to the done folder, but no error file is created.
  - No users are added to the CentreWare Web table.
  - The Windows Application Event viewer shows one error, indicating the import failed.

Matching Customer Data

CentreWare Web uses the Network User Name field to match customer records. Therefore, if a customer with same Network User Name does not already exist, a new customer record is created. If record already exists, it is updated. Importing and Matching Chargeback Codes

You can also import customer association of chargeback codes.

To import the customer association of chargeback codes:

1. Set the Restricted to Chargeback codes field in the CSV to one of the following values:
- Set "*" to mean No restriction, thus, the customer can use any existing code.

- Set to an Empty value to mean that the customer is restricted from using any existing code.

- Example: Delta:Pin1means the customer is associated with chargeback code named "Delta" and PIN is "Pin1".

- Example: Delta:Pin2;Golf:Pin2 means the customer is associated with two chargeback codes, first code is named "Delta" and PIN is "Pin1," and the second code is named "Golf" and PIN is "Pin2".

Example: Pin1,:Pin2 means the customer is associated with two chargeback codes, first PIN as "Pin1," and second PIN as "Pin2".
The import process is capable of automatically creating chargeback codes, if they do not exist, provided the syntax provides the chargeback code name. If only PIN is provided, the code is not created and the import for the customer record may only partially succeed.

Using the Active Directory Customer Import

If the customer keeps user information up-to-date in the active directory, the Active Directory Customer Import is the most preferred way to replicate the customer information into MPS suite. You can access multiple active directories at one time and also select specific containers to restrict the import to only few departments in the customer account.

To use the Active Directory Customer Import:

1. Select **Administration > User Management > Active Directory Customer Import**. The Active Directories/Containers screen displays.

2. Verify that the active directories or specific containers to import are populated in the Include Containers list box.

Note: If multiple active directories are selected, it is assumed that the active directory schema is consistent across these directories.

3. Map the customer fields correctly to active directory user fields. If you do not want to import a given field, leave the mapping list box blank and it is not imported.

4. Click **Test** to browse the active directory user records as per the configured mapping, thus verifying the expected results.

Importing and Matching Chargeback Codes

You can import customer association of chargeback codes.

To import the customer association of chargeback codes:

1. Set the Restricted to Chargeback codes field in the CSV to one of the following values:
   a. Set "*" to mean No restriction, thus, the customer can use any existing code.
   b. Set to an Empty value to mean that the customer is restricted from using any existing code.
      • Example: Delta:Pin1 means the customer is associated with chargeback code named "Delta" and PIN is "Pin1".

- Example: Delta:Pin2;Golf:Pin2 means the customer is associated with two chargeback codes, first code is named "Delta" and PIN is "Pin1," and the second code is named "Golf" and PIN is "Pin2".

- Example: Pin1,:Pin2 means the customer is associated with two chargeback codes, first PIN as "Pin1," and second PIN as "Pin2".

This is as done exactly like the CSV import configuration of field "Restrict to Chargeback Codes." Refer to the same section under Importing an Auto Customer File.

Using Job Accounting

Overview

CentreWare Web can archive job accounting information for Print/Fax/Copy/Scan jobs. You can collect the information in one of the following ways:

- Device-Based Accounting (DBA): Identifies and reports on jobs processed by devices capable of job-based accounting (JBA); either walk-up functions such as Fax/Copy/Scan, or both walk-up functions and printing. Jobs are associated by customer and chargeback code.

- Import Jobs: Imports job data from a third-party tool such as Equitrac or Pharos.

CentreWare Web provides accurate and detailed information about your printing environment with reliability and simplicity. This data makes print technology decisions easier to implement. You can use this data for user, department, or project-level chargebacks.

Using Device-Based Accounting

CentreWare Web supports device-based accounting by which jobs are tracked on the printer but collected centrally by CentreWare Web. The printer records the user and printing attributes for each print job, and this data is then made available to CentreWare Web.

For a list of printers that support DBA and are supported by CentreWare Web, check the CentreWare Web website.

Using DBA for Multi-function Devices (MFDs)

Job accounting on MFDs can track all different job types: Print, Scan, Copy, and Fax. As part of the device-based accounting, the device can provide user validation against a list of approved customers on-box validation, or via a separate server; off-box validation. The CentreWare Web server itself can function as the off-box validation server. CentreWare Web also provides you with the means to create and edit the lists of approved customers, as well as the associated chargeback codes for job accounting.

Configuring Multi-Function Devices For Device-Based Accounting

You must configure printers capable of device-based accounting (called Job Based Accounting or Xerox® Network Accounting) for service and data retrieval. One simple way to determine which devices support DBA is to enable the device accounting state for devices. Those DBA-capable devices show the accounting state as Running versus Unknown or Not Supported.

To enable DBA for a device:

1. Access the device's Detail screen from the Devices view and click the Edit Actions > Edit Job Accounting Properties. The Edit Job Accounting Properties screen displays.
2. Select Device Based Accounting from the Print Job Accounting drop-down menu. If the device also provides walk-up job accounting, this is selected in a similar fashion.
3. Select the DBA protocol settings. The supported protocols are automatically determined.
4. Select the Validation Mode.

- Off-Box Validation: An external server is used when validation is required.

- On-Box Validation: The user list is maintained on the device itself.

5. Select whether to validate only walkup users or print job and walkup users via the Validation Scope radio buttons.
    - For Off-Box Validation, select the Validation Server. The Communication Failure Policy determines device behavior in the event communication fails with the validation server. You can either grant or block access to the device. After all of the settings are configured, click Save to apply them to the chosen device. Alternately, click Save as New Configuration Set to create a configuration set that you can then apply to a multitude of printers.

Configuring Validation Codes

You can validate using two fields: userid and accounted. In Xerox® Office Services, userid is the Accounting User Name and accountid is the Chargeback Code PIN, and you can configure them for each customer in the User Management section. Refer to Managing Users Overview.

As customers utilize printing services on a specific device, the data necessary for establishing the associated printing charges for each job is assigned to the selected chargeback code. This allows the printing charges to be allocated to the various chargeback projects.

Enabling Data Retrieval

You must enable data retrieval to access the DBA data from the printers.

To enable data retrieval:

1. Select **Administration > Job Accounting > Device Based**. The Device Based Accounting screen displays.
2. Select the retrieval date and time.
3. Select the other options.
4. Click **Save**.

Note: You can retrieve the data every 6, 12 or 24 hours. Data can also be retrieved immediately by clicking Retrieve Now.

Using E-mail Notification

CentreWare Web can inform users via an e-mail alert message whenever it fails to pull accounting data from a device. This is configured via the E-mail Alerts section of the Device Based Accounting screen.

Remotely Set Devices to Use DBA

Network accounting can be set remotely as the accounting method on Xerox devices that support this property. You may use device edit or configuration sets to configure this feature.
Note: network accounting method must be enabled in order to use device-based accounting.

Follow the steps below to remotely set devices to use DBA via device edit:

1. Go to **Properties > Job Accounting tab > Job Accounting Options**.
2. Set Accounting Method to "Network Accounting" and save.
3. Re-discover the device from the Discovery page.
4. Go back into Device Edit.
5. Go to **Properties > Job Accounting tab > Job Accounting Options**.
6. Set Print Job Accounting to Device Based Accounting.

7. Optionally, set Walk Up Accounting to Device Based Accounting.

8. Click **Save**.

   Follow the steps below to remotely set devices to use Device Based Accounting using configuration sets:

   1. Create a new configuration set.
   2. Go to Job Accounting Options.
   3. Set Accounting Method to Network Accounting and save.
   4. Create a second configuration set.
   5. Go to Job Accounting Options.
   6. Set Print Job Accounting to Device Based Accounting.
   7. Optionally, set Walk Up Accounting to Device Based Accounting,
   8. Save the configuration set.
   9. Create and run a policy to run the configuration set created in Step 1.
   10. Re-discover the device(s) from the Discovery page.
   11. Create and run a policy to run the configuration set created in step 4.
   12. Delete this text and replace it with your own content.

Using DBA for Phaser Devices

Xerox® Phaser printers come with built-in support for job accounting (also called Phaser accounting). Similarly to MFDs, Phaser printers track user and job attributes for each job printed. This information can be collected centrally by CentreWare Web from multiple printers. Make sure the printer is added with the hard disk enabled, as all job data is cached temporarily in memory and data is prone to be lost if the printer is rebooted. When the hard disk is enabled, the data is written to the drive and is safely stored and retrieved by Xerox Device Manager at a configured interval.

Using DBA for Production Devices

Accounting for production devices is mostly supported by front-end controllers such as DocuSP, EFI Fiery, and Creo. CentreWare Web supports many production devices, depending on the accounting features supported by the controllers. Similar to the above families, CentreWare Web can periodically poll production devices to pull job accounting logs from production device controllers. For a complete list of printers that support DBA and are supported by CentreWare Web, see the CentreWare Web website.

Generating Reports

Overview

The Reports screen provides a reporting facility to generate and either view or e-mail links to the reports about devices discovered by CentreWare Web. The primary application of these reports is ad hoc reporting, or generation of operational data for baseline asset evaluation or print-device utilization.
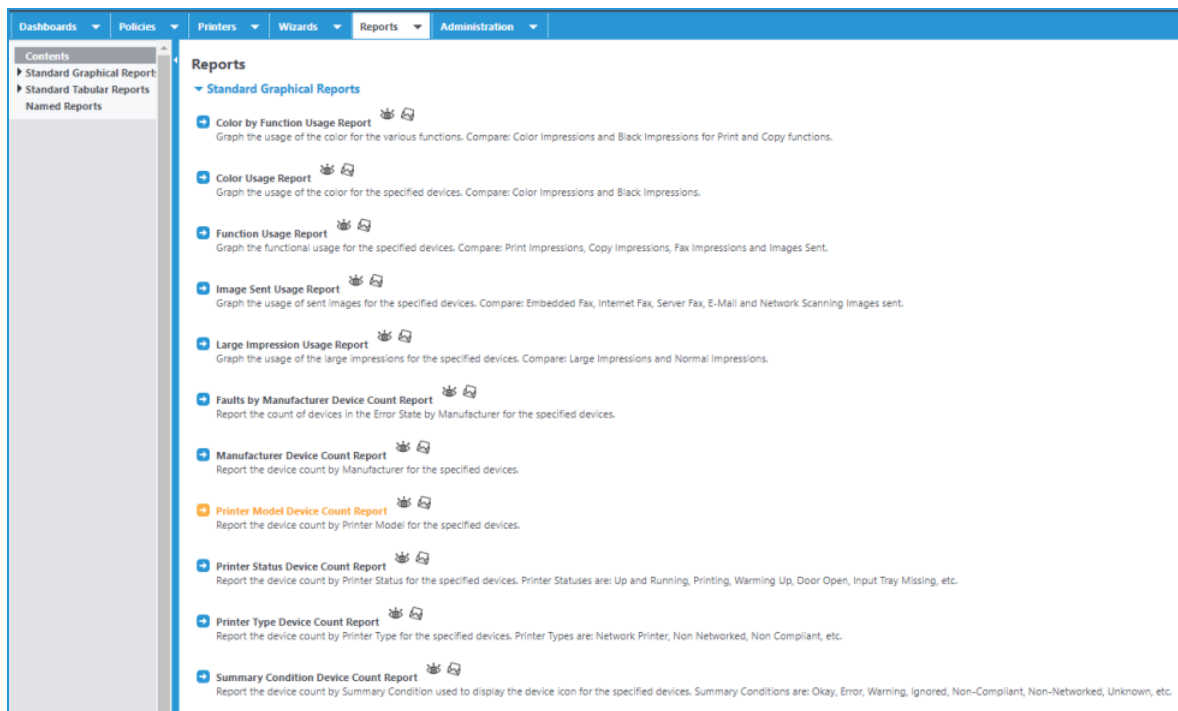
CentreWare Web provides both graphical and tabular reports for a variety of conditions and functions. Graphical reports are offered in pie, bar and line formats. You can customize both the graphical and tabular reports and assign a unique name under the Named Reports function.

Exploring the Reports Available in CentreWare Web

The following tables describe both the standard graphical reports and standard tabular reports you can generate in CentreWare Web.

Standard Graphic Reports

This table describes the Standard Graphic Reports available in CentreWare Web.

Report Name	Description
Function Usage Report	Compares print Impressions, copy Impressions, fax Impressions and images sent for the specified printers.
Color-Usage Report	Graphs the usage of color and monochrome printing.
Color by Function-Usage Report	Compares color and black impressions for print and copy functions for the specified printers.
Large-Impression Usage Report	Compares the usage of large impressions and normal-size impressions.
Image Sent-Usage Report	Graphs the usage of scanned images.
Manufacturer Device-Count Report	Provides a count of devices by manufacturer.
Printer Model Device-Count Report	Provides a count of devices by model.
Printer Type Device-Count Report	Provides a device count by printer type (networked, non-networked, non-compliant, etc.)
Summary Condition Device Count Report	Provides a device count by the overall printer status.
Printer Status Device Count Report	Provides a device count by the printer status, such as "up and running", "door open", etc.
Faults by Manufacturer Device Count Report	Displays the count of devices in an error condition by manufacturer.

Standard Tabular Reports

This table describes the Standard Graphic Reports that are available.

Report Name	Description
Printer Asset Report	Printers discovered on network by CentreWare Web.
Printer Status Report	Printers that might need attention.
Usage Counter History Report	Page counts for printers in a selected group. You must enable historical data collection from the Administration screen. CentreWare Web requests information in the printers SNMP daily page count as scheduled.
Alert History Report	Alerts for printers in a selected group. You must enable historical data collection from the Administration screen. CentreWare Web requests information provided in the printers SNMP alert table on a daily basis as scheduled.
Job Accounting Report	A report of the job tracking data, by device. The report contains a row for each job.
User Summary Report	A report on the job tracking data by user.
Audit Check Report	Reports on specified audit check tasks performed against devices over a specified time period.
Fleet Security Report	Report detailing security-related settings for Xerox printers.
Trellix Embedded-Control Report	Report on Trellix Embedded Control events.
Supply Report	Report displaying the supply names and current levels for each selected device. Enables you to check supply levels and re-order supplies before the device triggers an alert that the supply is low.
Password Audit Report	A report for seeing the history of password updates and audits on devices

Report Name	Description
Workplace App Distribution Report	Provides a snapshot of app distribution across the fleet of devices.
Named Reports	Allows customized reports to be saved by name. Named reports also include all the standard report types.

Generating the Reports

You can generate reports in any one or combination of the following file formats:

- CSV: Comma-separated value for import to Excel®, Access™, or other database applications.

- HTML: Hyper Text Markup Language for on-screen display or export to Web page.

- XML: Extensible Markup Language for import into XML-input applications.

You can customize the amount of data and the order the data appears in these reports. You can define both the data fields and the column position for its reports.

Some reports include additional default user-defined fields. For example, the Page Count History report adds a page-count column and a page-difference column to the user -defined fields, while the Alert History report adds the polling date and detailed machine status information to the user-defined fields. As a result, the report file sizes can vary greatly. For large corporations with thousands of printers, it is common to have report sizes in excess of 2-3 MB.

You can obtain reports by clicking on the eye icon or Display Report link, or via an e-mail message that contains up to 3 URLs (one for each report format) pointing to the actual files stored on the server. CentreWare Web only maintains the last report that was generated by the server; there is no repository for previously generated reports. The URL links to the actual files on the CentreWare Web server can minimize the impact CentreWare Web has on a customer's e-mail system.

Note: To generate meaningful report data for the Usage Counter History Report and the Alert History Report, you must enable the Historical Data Gathering function.

The CentreWare Web database can store up to two years of report-related data generated by the Historical Data Gathering function. Each report contains both a site and server name, for the server that generated a report. This is useful when multiple servers are deployed within a large enterprise.

Note: You must configure CentreWare Web to specify a valid SMTP server. If this was not done at installation, you must complete this prior to sending reports via e-mail.

To specify a valid SMTP server:

1. Select **Administration > Network**.
2. Click **E-Mail & External Servers**.
3. Enter data for the SMTP server and e-mail address.
4. Click **Test** to confirm that the server specified is active.
5. Click **Save** to apply the settings.

Exporting the Reports

You can export reports directly from the Report Edit screen. The exported file contains the report in the selected report format.

1. On the Reports tab, select the report you want to export.
2. Select **Export Report**.

3. Click **Save**. The contents are saved to your local system.

Creating Named Reports

Named reports provide the ability to define the fields included in any of the standard reports, and to save that configuration with a unique name to be recalled and used at a later date or time.

To utilize the Named Reports feature:

1. Select **Reports > Named Reports**. The Named Reports screen displays.
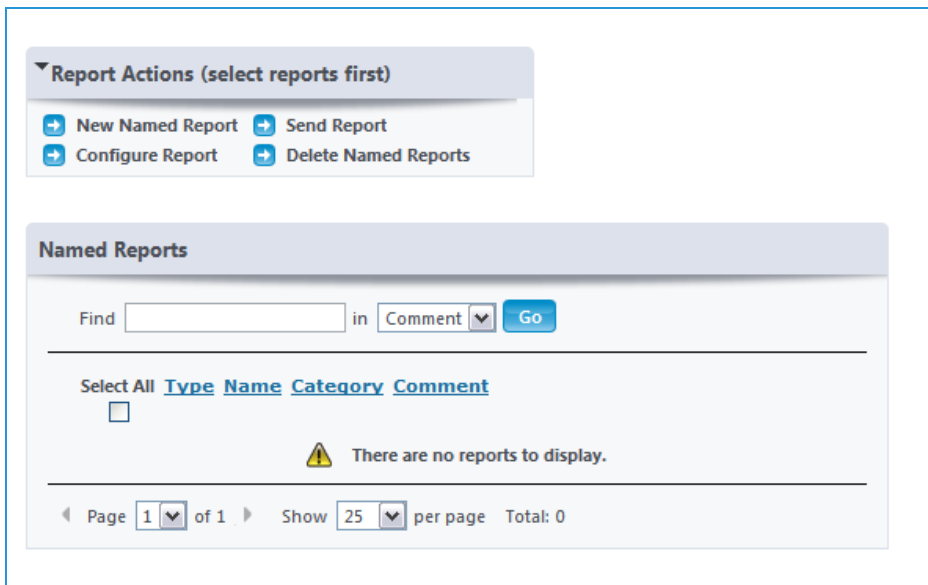
2. Select **Report Actions > New Named Report**.
3. Select the type of report. The screen refreshes after the selection.
4. Select the report template. The report template can be either an existing report or blank.
5. Click **Continue**. The Configure Report: New Report dialog box displays.
6. Enter a name for the report in the General Properties screen.
7. Use the arrows to select the Included Fields from the list of Available Fields.
8. Select Schedule Period frequency if the report is to be recurring. This option never allows ad hoc reporting.
9. Scroll to the bottom of the dialog box and click Save to navigate back to the Named Reports screen. The new report displays in the Named Reports screen.
10. Select the eye icon that corresponds to the new Named Report to view the output of the report. The new Named Report, containing the defined fields, is displayed.

Generating Graphical Reports

Graphical reports provide a convenient way to quickly assess a wide variety of parameters related to your printing environment. Data that might otherwise be buried in a tabular report often stands out visually in a graphical report.

A typical graphical report might show the overall usage for color vs. black & white printing and copying for a group of printers. Graphically, it is immediately obvious the most often used service for the selected group

of printers. In addition to the visual relationships, you configure the report to include the actual counts in this graph.

To configure a graphical report:

1. Select the type of graphical report.
2. Choose the group or groups to report about.
3. Select the Chart Type.
4. Select the Display Values check box if you want to include the numeric data in the chart.
5. Select the time span for the data to be displayed.
6. If the report is to be e-mailed, configure the recipients and any accompanying message.
7. Select the Report Colors.
   - Saturated Colors creates bright, vivid graphs
   - Pastel Colors is a more subdued pallet
   - Greyscale is useful for printing on monochrome devices where some color subtleties may otherwise be lost
8. Select the Schedule Period and report Language.
9. Click **Save**.
10. To directly view the report, return to the top of the page and click Display Report in the Report Actions box.

Note: The Alert History report is only gathered once daily (when enabled) and does not contain intermediate printer alerts that were cleared before the historical data gathering occurred.

Using the Wizards

Overview

The Wizards screen provides step-by-step procedures for accomplishing tasks that are run on an infrequent basis from CentreWare Web.
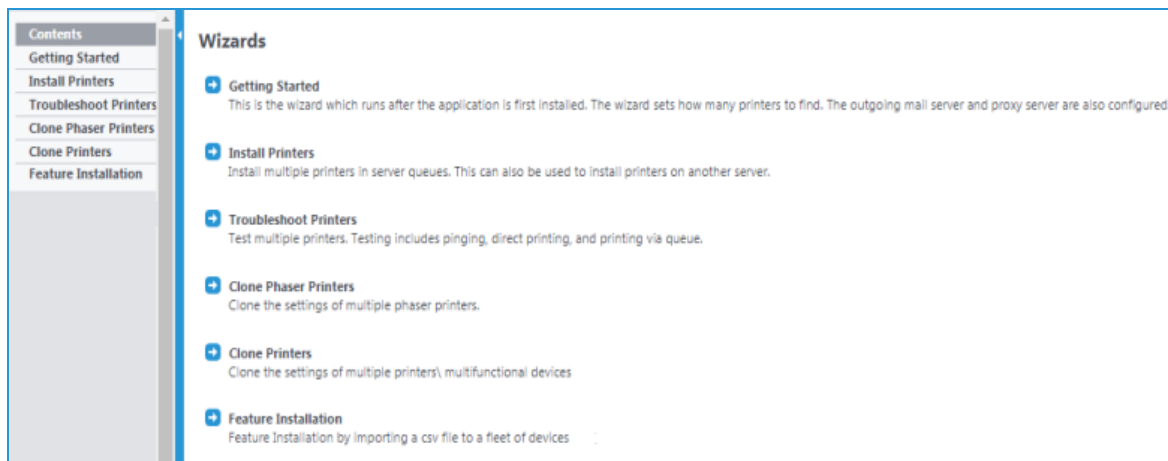
Using the Getting Started Wizard

The Getting Started wizard runs after the application is first installed. It sets how many printers to find and configures the outgoing mail and proxy servers.

Using the Install Printers Wizard

The Install Printers wizard installs one or more printers in the server queues or on a server.

To install printers:

1. From the Wizards Menu screen, select Install Printers. The installation begins.
2. Select the printer group to install from the drop-down menu.
3. Click **Continue**.
4. Select the printer(s) to be installed from the drop-down menu.
5. Click **Continue**.
6. Select the server to install the printer on from the drop-down menu.

7. Click **Continue**.
   Note: Verify the queue and printer driver settings and then click **Continue**. You might be prompted with a security warning.
8. The Install Results screen displays, showing that the printer was successfully installed.
9. Click **OK**.

Using the Troubleshoot Printers Wizard

The Troubleshoot Printers wizard tests one or more printers for pinging, direct printing, or printing via the queue.

The Troubleshooting Wizard helps triage network printing related problems for multiple print servers/multiple printers; up to 25 print servers/printers at one time. Once the desired printers are selected for analysis, the Troubleshooting Wizard automatically pings those printers and any associated print servers.

The Troubleshooting Wizard queries two printer status-related OIDs and makes a Remote Procedure Call (RPC) to any associated print server to retrieve the latest print queue status. The results of the ping test and the status queries then display on the screen. You can initiate additional testing on an individual printer from the printer's web page, if desired.

You can click Manage Queues to access the Print Server's Windows® Internet Print Service web page to submit a test page directly to the:

- Printer via Port 9100 to verify a print path

- Associated print queue via an RPC

To test the Troubleshooting Wizard:

1. Initiate a fault into your favorite printer (e.g., open a cover when running a print job, open a paper tray, pull out the printer cartridge, etc.).
2. Insert a related fault on another printer's associated print server. (e.g., pause the queue, select the printer Properties screen to change the security settings, etc.).
3. Select Troubleshoot Printers from the Wizards tab.
4. Select All from the Group drop-down menu. Available printers are queried.
5. Select the faulted printer and the printer with the associated print server fault for troubleshooting.

6. After several moments, CentreWare Web displays the troubleshooting results.

7. Click Details/Test for further details and available actions.

Using the Upgrade Android Tablets Wizard

In order to use this feature, Upgrade Android Tablet must be enabled under **Administration > Advanced > Preferences & Properties**.

This enables an administrator to upload and schedule the software package. The multifunction printer must be discovered by CentreWare Web for it to access package upgrades. CentreWare Web supports more than one Android Upgrade package.

Adding an Android Tablet Upgrade File

Follow the steps below to add a new Android tablet upgrade file

1. Go to **Wizards>Upgrade Android Tablets**.

2. Click **Add / Delete Files** in the Upgrade File Actions menu.

3. Under File Actions click **Add**.

4. Complete the fields on the Add Android Tablet Upgrade File page.
   - Upgrade Type: Choose Printer or Android.
   - Upgrade File: Browse to the file you want to upgrade.
   - Attachment: If applicable, upload relevant documentation for the upgrade. Word, (.doc). text (.txt), PowerPoint,(.ppt), and Adobe (.pdf) files are supported.

5. Click **Save**. The file is uploaded and displays in the list of upgrade files.

You may overwrite this file with a new file or delete it from the Upgrade Android Tablet page. To edit, click the pencil icon and then upload new files to overwrite the current files. To delete select the file and click **Delete** from the File Actions menu.

Scheduling an Android Tablet Upgrade File

Administrators can create a new schedule to upgrade software for multifunction printers. Administrators can select one or more android enabled printers to upgrade using the schedule. The uploaded software package will be available for the android device at the scheduled time.

The device can report the installation status to CentreWare Web, and CentreWare Web can record the installation status. Administrators can also see the progress in a detailed view of the schedule.

Follow the steps below to schedule an upgrade.

1. Go to **Wizards>Upgrade Android Tablets**.
2. Click **Schedule Upgrade**.
3. Either select an upgrade file and click Continue, or click **Add/Delete Files** if there is not an upgrade file available. Follow the steps in the Adding an Android Tablet Upgrade File section above. Click Back to return to the scheduling workflow.
4. In the Group drop-down, choose the printer group to have its tablets upgraded. Click Continue.
5. In the next screen select the printers that have an attached Android tablet to upgrade. Only Android tablets display. If you have not done so already, you should go to Table Preferences and make sure that the Android Device and Android Firmware columns display in the grid. Click Continue.
6. Set a task name and schedule you time. You may opt to upgrade now or enter a future time and date to upgrade. Click Finish.
7. The task displays on the Upgrade Android Tablets screen. The default task status is Pending.

Stopping or Restarting an Upgrade

Administrators can stop an upgrade task, so that upgrades are not available to the Android tablets. Upgrade tasks can be stopped while their status is Running or Pending.

Follow the steps below to stop an upgrade.

1. Select a task and click **Stop Upgrade**.
2. The task status and individual printer status change to Stopped. Tasks with a status of Completed, Error, or Completed with Errors cannot be stopped.

Though a task is stopped, an Android tablet can report the status of the installation if the upgrade package has already been downloaded before the task was stopped. CentreWare Web accepts this request and each corresponding status is updated.

You may also restart an upgrade task. All tasks, regardless of their status, can be restarted. A restarted task works the same way a newly scheduled task works. The task status changes to pending after restart.

Follow the steps below to restart an upgrade:

1. Select a task and click **Restart Upgrade**.
2. The task status and printer status change to Pending.
3. If the upgrade package has been downloaded before the task is restarted, the tablet can still report the status using the Report Software Update Status.

Deleting an Upgrade

You may delete an upgrade regardless of task status. However, please be aware that once you delete an upgrade task all the information related to the upgrade will be removed from the application.

Using the Clone Phaser Printers Wizard

The Clone Phaser Printers wizard clones the settings of one or more printers. This option is used by some Phaser devices. To clone AltaLink® or WorkCentre® devices with software versions 073.xxx.147.07400 or later, go to Using the Clone Printers Wizard. To clone all other devices use the Upgrade Wizard.

The Clone Phaser Printers Wizard simplifies the printer configuration process that System Administrators (SA) perform each time a printer is deployed across a corporation. This feature enables the SA to copy the configuration settings from one printer to a maximum of 25 printers of the same model running at the same firmware level.

Examples of Xerox® printers that support the Cloning Wizard, are: DocuPrint models N17/24/32/40, C55, NC60, N2025/2825, N2125, N3225/4025, N4525, Phaser 1235/5400

The Clone Phaser Printers Wizard does not transfer firmware/software to the target printers; it only transfers the printer configuration settings.

Note: This operation requires that HTTP be enabled on clone capable Xerox® printers.

To use the Clone Phaser Printers Wizard:

1. Select Clone Phaser Printers from the Wizards tab.
2. Select All printers from the Group drop-down menu to query for available source printers.
3. Select the printer configured as the source printer. CentreWare Web checks to confirm that the printer supports a compatible type of cloning.
4. Select All printers from the Group drop-down menu to query for available target printers.

5. Select the target printers from the list of qualifying target printers and then click Finish. CentreWare Web clones the settings from the source printer to the selected target printers. The results of the cloning process display when the operation is complete.

6. Generate another configuration page at the target printer and then compare similar attributes to the original target printer's configuration page. Configuration values should now be different from the original target printer's configuration page. However, similar attributes from the newly cloned printer's configuration page should be identical, in most cases, to the source printer's configuration page.

Note: Cloning may be disabled for a device from the Devices tab. Select the device you want to modify. In the Action menu choose **Edit Properties**. Go to **Security>Disable Services**. In the Disable Services section in the Cloning field, choose Yes from the drop menu.

Using the Clone Printers Wizard

Use this wizard to clone ConnectKey® devices by communicating with the device and receiving a status back. To clone AltaLink® or WorkCentre® devices with software versions 073.xxx.147.07400 or later, go to Using the Clone Printers Wizard. To clone all other devices use the Upgrade Wizard.

Follow the steps below to add a clone file.

1. Select Clone Printers from the Wizards tab.
2. Click **Add/Delete Files** from the Clone File Actions menu.
3. In the File Actions menu select **Add**.
4. On the Add File complete the following fields
    -   Choose a Model from the drop-down list.
    -   Browse to the Clone File (.DLM).This is the file that contains all the settings for the model you are cloning.
    -   Add an Attachment if you want to include instructions.

- Enter a Description.

- Click **Save**. This clone file is now available on the Add / Delete Clone Files page.

To delete a clone file, simply select the file you wish to delete in the Add / Delete Clone Files page and click **Delete**. Please note, if the clone file is associated with any tasks you will not be allowed to delete it.

Follow the steps below to clone a printer.

1. Select Clone Printers from the Wizards tab.
2. In the Clone Tasks menu select **Schedule Clone**.
3. Step 1 displays a list of clone files. Although deleted clone files still display in the list, you may not select them. Choose a clone file and click **Continue**.
4. In Step 2 select the group that contains the printers you want to clone. (You will choose the specific printers later). Click Continue.
5. In Step 3 select the devices you want to clone and click Continue. There is a filter to choose the model of the clone file; the model of the clone file must match the target device model.
6. In Step 4 schedule the clone process. Complete the following fields.
   - Enter a name for the Clone Task Identity.
   - Choose to run the clone process as a device administrator or a network user. If you select network user, because it is a more secure option, you will need to enter your user credentials.
   - Schedule the cloning. Click Clone Now to run the clone process immediately. or click Clone Later and enter a date and time.
7. Click **Finish**.
8. Check your progress in the View Clone Task Details page.

Performing Administration Functions

Overview

This section describes the various tasks performed from the Administration screen. You can:

- Specifying the Site /Administrator Information
- Set up Network Information
- Use Advanced Features
- Configure the Xerox Services Manager Suite

Those features are described in the following sections.

Specifying the Site / Administrator Information

The Administrator screen enables you to enter system administrator or support contact information for this CentreWare Web installation. The information is then available to all users from the Home screen.

Prior to establishing operation of the CentreWare Web application, you should specify the Site/Administrator information for your installation.

The Administrator setup information fields identifies this server to users. The Site Name and Identify information are displayed on the CentreWare Web Home screen.

1. Enter the appropriate settings.
   - Site Name: Descriptive name for location of this site.
   - Account Name: The account name is the same for service and contract requirements.
   - Name: The name of the administrator for this instance of the CentreWare Web server.
   - E –Mail: The e-mail for this administrator. Status messages regarding the server or external contacts can reference the administrator through this e-mail.
   - Phone: The phone for this administrator.
   - URL: An appropriate URL (beginning with http://), if required.
   - Location: Location for this server.
   - Comment: Text comment.

2. When completed, the Site / Administrator information displays on the Home screen for the CentreWare Web server. Links on the left side (Site Name, Account, etc.) link to the Administrator tab, Site / Administrator screen. The name links to the URL, if supplied above. The e-mail is a mail to link, and starts an e-

mail message if e-mail is configured on the client.

3. Click **Save** to save your changes, or Cancel to exit without making changes.

Setting Up Network Information

The Network screens enable you to set configuration options for CentreWare Web to specify how the application will work on your network.

Configuring E-Mail & External Servers

The E-Mail & External Servers screen allows you to configure the Outgoing Mail Server, Incoming Mail Server, and Proxy Server information.

The Outgoing Mail Server option specifies which Simple Mail Transport Protocol (SMTP) mail server to use when reports are e-mailed from CentreWare Web, and the e-mail address to use as the sender of reports. The Mail Server option also allows you to specify which Message Encoding standard is supported (e.g., UTF-8, etc.), the Maximum Attachment Size, Attachments Options for Reports, and the User Name and Password, if required, for SMTP security. You can also determine whether the specified server is listening on the defined port (Test Connection), and whether the specified e-mail address is correct (Send Test).

Proxy Server settings are required if you intend to use the Auto Driver Download feature and your network uses a proxy server for Internet access. For convenience purposes, CentreWare Web attempts to determine the proxy settings from your browser during the installation process. If CentreWare Web can determine the proxy settings, they automatically populate the Proxy Server Name and Proxy Server Port fields.

After defining the e-mail and server settings, click **Save** to save the settings (or changes) and exit the screen, or **Cancel** to exit the screen without saving the settings.

Configuring Network Usage

The Network Usage Configuration screen allows you to restore default settings and enable, disable, or configure various device or feature-specific functions related to data extraction.
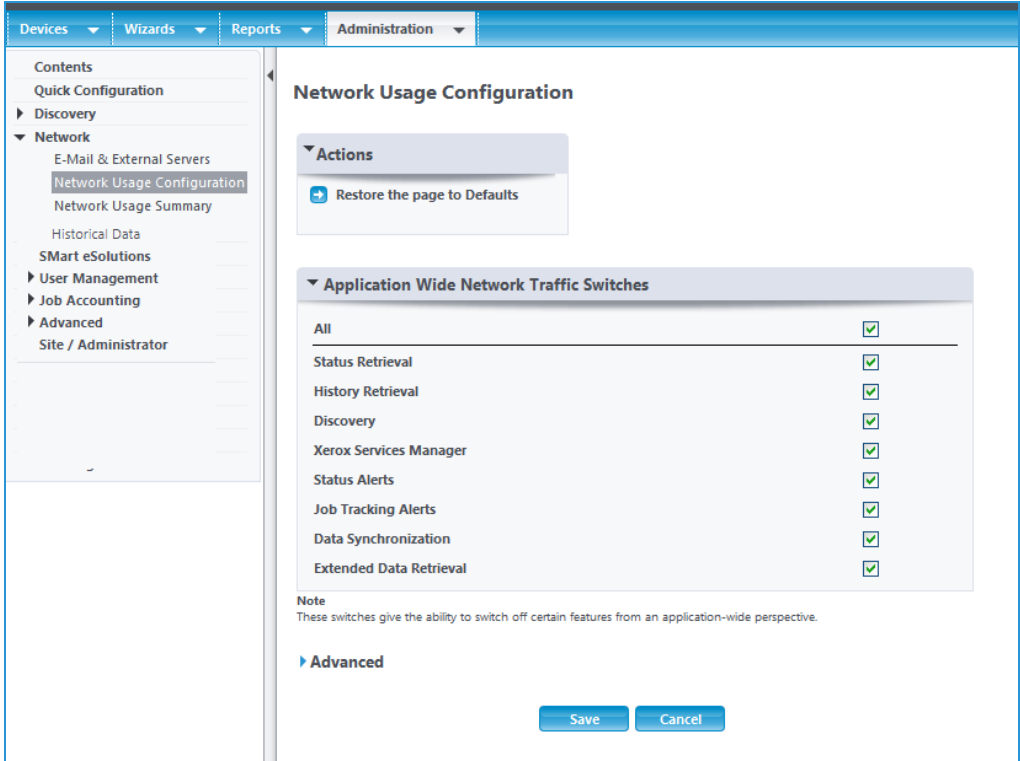
From the Actions menu you can restore the screen to the default settings .

You can individually enable/disable features from an application-wide perspective from the Application Wide Network Traffic Switches pane. Features are enabled when the corresponding box is checked. Checking All enables all of the listed features. Features are disabled when both the feature check box and the All check box are unchecked. For example, removing the check marks from All and Discovery disables the Discovery feature and prevents you from running any discovery methods, as shown in the Discovery screen below.
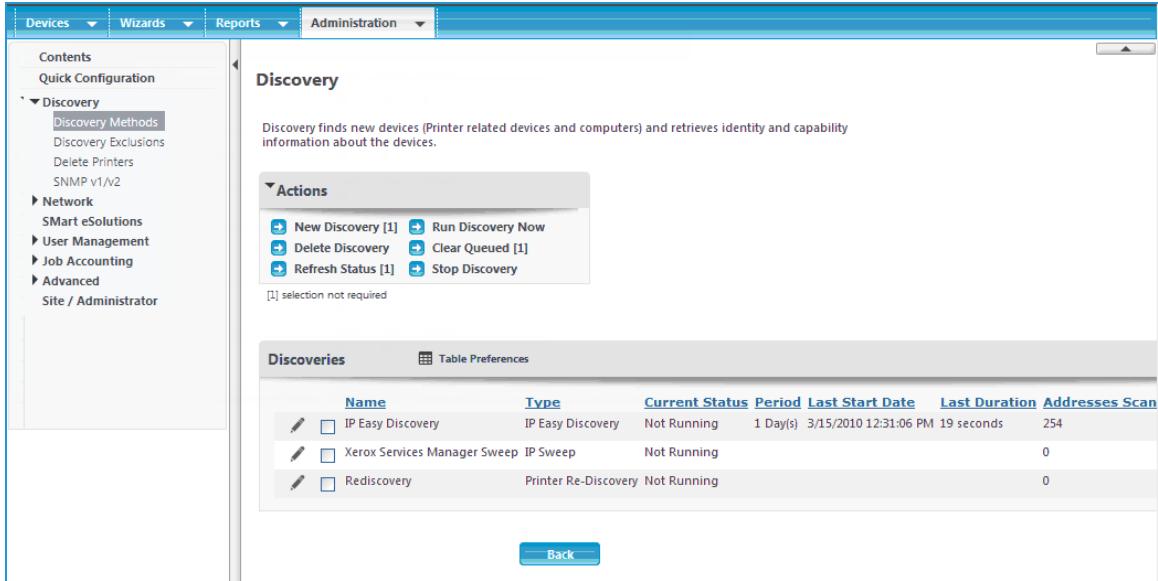
From the Network Usage Configuration screen, you can:

- Select Advanced to present or hide further Network Usage Configuration selections.

- Reset all groups and discoveries to the system defaults in the Group and Discovery Actions.

- Restrict when status retrieval occurs to only certain hours for the entire week, e.g., between 8:00PM and 1:00AM or to certain times for specific weekdays, e.g., Monday between 8:00AM and 12:00 PM, Tuesday 1:00PM and 6:00PM, etc., with Operational Hours for Status Retrieval

- Allows the time to wait for a reply and the number of retries to be defined, for retrieving printer status and adding individual printers, with the Communications Settings.

- Control when the application retrieves printer status information. Under Status Retrieval you can set the application to never retrieve this information or to retrieve it regularly at a specified interval.

- Specify whether scheduled discoveries include all printers or only Xerox® printers with Manufacturer Applicability. This setting does not apply to directly connected printers or printers added manually. Additionally, it does not apply when adding a managed print server or an Active Directory®.

- Set when power usage data is retrieved. By default, this option is enabled. We recommend you schedule the retrieval during an off period for the company, as this process can become more resource intensive as the fleet grows.

- Enable/disable reverse DNS name lookup, with DNS Names. If available, DNS names is used for printer management when performing HTTP network requests. The DNS name is used in environments that block HTTP requests to IP addresses.

Note: After defining the Network Usage Configuration settings, click **Save** to save the settings or Cancel to exit the screen without saving.

Gathering Historical Data

Historical data gathering enables the capture of page count and alert data for use in the Page Count History and Alert History reports. This information can be gathered at a specified time and for selected groups of printers. Historical data is kept in CentreWare Web's database for one year. Any historical data older than two years is automatically deleted.

This feature can evaluate using either the Page Count History or the Alert History Report. For the purpose of this evaluation, the Page Count History report is used. A more detailed evaluation of the Page Count History and Alert History reports is covered in Generating CentreWare Web Reports.

The History Retrieval option specifies if and when historical data gathering is to occur.

To enable data collection

1. Select the Every radio button.
2. Set the retrieval interval and the start date and time using the Next Scheduled Date and Next Scheduled Time settings.
3. Select the Collect Page Count History and Collect Alert History radio buttons to enable the collection of this data.
4. Specify how long the historical data should be retained in the Retain Historical Data section.
5. You can manually clear historical data by selecting your desired date range and clicking Clear Historical Data Now.
6. Click **Save**, or **Cancel** to exit without making changes.

The SMart eSolutions must be enabled by the CWW User from Administration > Smart eSolutions. There are a couple of steps the users must complete in order to enable SMart eSolutions. Once these steps are completed the SMart eSolutions are presented as a new group within the Printer file menu tree.

SMART ESOLUTIONS ACTIONS

Restore SMart eSolutions Group – Status

Registered printers are restored to this group if the application becomes corrupt, is uninstalled, or a printer is removed or deleted from the group and is added prior to next communication with Xerox Communication Server.

Transaction Log Set Up

1. Action, Clear Log.
2. Select the Clear Log link to launch a window with clear log options.
3. Discard non data export radio button for transactions older than 2 years. Date range is 1-99 days, weeks, months, years.
4. Discard Transactions older than with a date range of 1-99 days, weeks, months, years.
5. Discard all non data export transactions.
6. Discard All Transactions.

The Transaction log captures SMart eSolutions events. These events can be sorted in the following categories:

- All – displays all the events for SMart eSolutions

- Device Register – occurs when a device is registered with the Xerox Communication Server for the SMart eSolutions service

- Server Register – identifies a server that has been registered

- Xerox Server Communication – verifies a communication register with the Xerox Server

Note: Transaction Log is a log view of SMart eSolutions events. The only Actions associated with this field are to sort by different categories or to clear the log. At initial setup when SMart eSolutions is first enabled there are no log files to clear.

Smart eSolutions feature set up:
1. Check the Enabled radio button located within pull down box Enable SMart eSolutions and Register with Xerox Communication Server.
2. Check the Automatic Device Registration option, if unchecked. The user Requests Registration for each printer device at the SMart eSolutions group configuration Printer page.
   a. Select Communication Suspended Temporarily: Use to take a printer offline.
   b. Disabled and No Printers Registered: Disables the SMart eSolutions feature. and it will not appear in Printer group file menu tree.
3. Select the e-mail link to configure the SMart eSolutions Information window. The user can configure the e-mail notification when registration requests are made and transmitted.
4. Recipient(s) can be added or deleted. A total of 3 e-mail addresses can be added in the recipient list.

5.   Go to the E-Mail & External Servers page. Enable Status Alerts, configure the Outgoing Mail Server if not done during install, proxy server settings and then save the settings. If a proxy server is used then the proxy must be configured in order to cross the firewall to Xerox Communication Server.

6.   Set up Alert Notifications to email a recipient for the following SMart eSolutions events. These are enabled by default.

- Failure to Communicate with Xerox Communication Server. Date range equals 1-30 days.

- Failure to Read Data from Device for a date range that equals 1-30 days.

- Devices Deleted from SMart eSolutions Group

7.   Select **Save** at the bottom of SMart eSolutions Administration page.

8.   Upon saving this page SMart eSolutions attempts to register with the Xerox Communication Server. If successful, a status of Registered and Passed is displayed in the Xerox Communication Server Status Window on SMart eSolutions.

9.   SMart eSolutions is now set up and is available in the Printer menu file as the group SMart eSolutions.

Using Advanced Features

The Advanced section enables you to modify several more advanced features.

- Preferences and Properties
- Useful References
- Trellix Embedded Control
- Import Device Passwords
- Xerox Device Manager Updates
- Device Audit Log Settings
- Initial Android Tablet Upgrade File

These features are described in further detail in this section.

Modifying Preferences & Properties

The Preferences & Properties section allows modification to some of the basic behaviors in CentreWare Web.

- User Interface Customization: Esthetic choices for CentreWare Web.

- Detailed Device Page: Refresh device status as soon as you select the device screen or only when the device status is [xx] minutes old. You can select between 1 and 60 minutes.

- Group Level Permissions: Controls access to functionality based on user group.

- Specialized Printer Features: Specific CentreWare Web options for view to enable or disable. This includes options to clone printers, upgrade Android$^®$ tablets and more.

- Firmware Upgrade Window: By default this is disabled. When enabled you can set a time range when firmware policies run. Policies set outside of this time range will start running the next time the range is reached.

- Maximum Concurrent Firmware Upgrade: Set how many upgrades may run simultaneously. This is capped at 25.
  Recommendation: How many files can transfer over the network at one time depends on your network. For initial upgrades, you may want to run fewer than 10 upgrades until you know what your network can handle.

- Printer Password History Check Limit: Set a value between 0 and 25 to indicate how many previous passwords are checked during password reset.

- Icon Origin: Device status (warning, OK, error) furnished by the device or set for the site.

- Define Error/Warning Icon: Based on site requirements, re-prioritizing individual statuses in the display.

- Status Sort Order: CentreWare Web's status sort order.

- Define Custom Property: User-defined fields for an CentreWare Web device attribute which is visible to Xerox Services Manager.

- Scheduled Task Settings: You may set the duration of the configuration policy. You can also set the rate at which a firmware file transfers.

Defining Useful References

The Useful References screen allows you to define up to five printer references, consisting of a device manufacturer and Web site. The links to these resources display on the Printer Properties screens.

Trellix Embedded Control

The Trellix Embedded control security email notifications can be configured from this screen. Specify recipients and the message contented.

Import Device Passwords

Administrators can import a CSV file of devices and their assigned passwords. This can also be accessed from the **Devices > Password Policies**.

Using the Initial Android Tablet Upgrade File

Administrators can upload and deploy Android Software Packages as the Initial Android Tablet Upgrade File. The initial android package is available for any Multifunction Printer. The printer does not have to be discovered for the multifunction printer to download the package.

Unlike the other schedules, CentreWare Web does not track the progress of Initial Software upgrade. This status is stored in CentreWare Web as an Android Event log.

1. Go to **Administration > Advanced > Initial Android Tablet Upgrade File**.
2. In the Upgrade File field click **Browse...** to upload the Initial Software package to deploy.
3. Click **Save**. This will upload the initial software package in the CentreWare Web server. The Tablet can download these files. Only one initial software package file is allowed at a time.

You may overwrite this file with a new file or delete it from the Initial Android Tablet Upgrade File page.

Updating CentreWare Web

The CWW updates menu adds support for the latest devices. Simply click on **Xerox® CentreWare® Web Updates** and a new browser window opens where you can download the latest version of CentreWare Web.

Device Audit Log Settings

This setting allows an administrator to configure the number of days to maintain Device Audit Logs. The default is 5 days.

Security Configurations, Settings, and Considerations

Overview

In order to maintain a secure installation and operating environment, CentreWare Web is constantly adding and enhancing functionality to provide access to the latest security options.

Configuring security settings can include:

- Utilizing Trellix Embedded Controls
- Configuring and using TLS and SNMP v3
- Device based security
- Application settings
- Job Data Export modification

These features are described in the following sections.

Utilizing Trellix Embedded Controls

Trellix embedded controls add Trellix scanning and security capabilities to a device. Devices with this capability block unauthorized applications and changes on fixed-function, point-of-service infrastructures and office equipment. Violations will generate notifications that are forwarded to the configured users.

Configuration of notifications is done via the Trellix configurations pages under Administration.

Administrators can:

- Configure the recipients of email notifications.
- Define the subject and body text of the email.

Device Based Security

Administrators use secure methods of device communication, including SNMP V3 in their deployment. Prior to establishing operation of the CentreWare Web application, you should specify the Site/Administrator information for your installation.

SNMP v3 includes two important services: authentication and privacy.

Authentication

The authentication mechanism in SNMP v3 assures that a received message was, in fact, transmitted by the principal whose identifier appears as the source in the message header. In addition, this mechanism assures that the message was not altered in transit and that it was not artificially delayed or replayed.

In order to retrieve data from the device, a username is required. Administrators may set up as many user names as necessary, on a device by device basis.

Privacy Using Encryption

The SNMPv3 USM privacy module enables the application to encrypt messages to prevent eavesdropping by third parties. Privacy encrypts the contents of the SNMP message, ensuring that it cannot be read by unauthorized users. Any intercepted messages will be garbled and unreadable. The encryption is handled based on the type of encryption you have configured the system to use.

Administrators can also manage the local aspects of security on devices using CentreWare Web.

Local Administration Accounts

Local Administration accounts on the device can also be managed using the Password Management feature of CentreWare Web. Administrators can configure a policy to automatically update the local passwords for the device on a scheduled basis. Policies will also report on any devices that are using the factory default passwords. See Password Policies for more information.

USB Ports

Some devices include USB ports to allow users to print from and scan to a local device. These ports can be disabled if the device supports it.

Navigate to Devices > Edit Printer > Security > Disable USB Port. From this screen you can disable the front and rear USB ports (if available).

Service Disablement

Many services are available on devices. The exact list depends on the model. Examples include LPR, NFC, IPP, AppleTalk, etc. Specific services can be enabled and disabled by the administrators via the Printer Security details tab. Careful consideration and research should be taken before modifying the available services. Changes to this configuration can result in system instability or erratic behavior.

Console Lockout

When enabled, the Console Lockout option will disable the local console, preventing access to the device from non-authenticated users.

Appendix

Terms & Abbreviations

Terms and Abbreviations used in this document.

Abbreviation	Description
CAL	Client® Access License
CD-RW	Compact Disk- Read/write
CRU	Customer Replaceable Unit (typically toner cartridges, and the like)
DNS	Domain Naming System
DSN	Data Source Name (reference ODBC compliant DB)
HTML	Hypertext Markup Language
https	HyperText Transfer Protocol, Secure. For Xerox® Office Services hosting this is 128-bit encryption.
ICMP	Internet Control Message Protocol
IIS	Internet Information Server/Services [Microsoft®]
IP	Internet Protocol
ISP	Internet Service Provider
IPX	Internetwork Packet Exchange (Novell connectionless datagram)
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LPR	Line Printer Remote
MFD	Multifunction device, refers to Printers also capable of FAX, Scan, and Copy functions
MIB	Management Information Base (as in Printer MIB for SNMP management)
MS	Microsoft® Corporation
NIC	Network Interface Card (Like PIN number and UPC code, "NIC card" is redundant)
OID	Object Interface Definitions (as in Printer MIB for SNMP management)
ODBC	Open Database Connectivity (SQL Access Group, 1992)
OS, O/S	Operating System
POP3	Post Office Protocol [Internet]
RFC	Request For Comments [Internet]
RPC	Remote Procedure Call
SAP	Service Advertising Protocol [Novell IPX]
SMB	Server Message Blocks
SMTP	Simple Mail Transfer Protocol [Internet]
SNMP	Simple Network Management Protocol [Internet]
TCP/IP	Transmission Control Protocol/Internet Protocol

Abbreviation	Description
WAN	Wide Area Network
XP	Windows®: The Experience [Microsoft®]
WSDL	Web Services Description Language
XML	Extensible Markup Language

Abbreviations

Wildcard Definitions

Operator	Operations
%	Any string of zero or more characters.
_	Any single character, letter or numeral
[ ]	Any single character within the specified range (for example, [a-f]) or set [abcdef]). If a single character is enclosed, it is an exact match for that character.
[^]	Any single character not within the specified range or set [^a-f] or [^abcdef] would evaluate as all lowercase letters g through z
-	(dash) Through; as in the numbers 2 through 7: [2-7]
/	Escape for [,] or % operators to be used as explicit characters
Sample Expressions using Wildcards	
co%	Searches for all strings that begin with the letters co, such as copier, console, color.
%er	Searches for all strings that end with the letters er, such as power, paper, printer, scanner.
%an%	Searches for all strings that contain the letters an anywhere in the string, such as scanner, panel, ocean.
[c-z]old	Searches for all strings ending with the letters old that begin with any single letter from c through z, such as cold, sold; but not bold.
p[^a]%	Searches for all strings beginning with the letter p that do not have the letter a as the second letter, such as power, picture; but not paper, or panel.
5[%]	
5%	
[[]	Searches for the [character.
[]]	Searches for the] character.
[_]n	
_n	Searches for two letter words with any first character and n for the second character.
[a-cdf]	
%//%	Searches for a forward slash (/) anywhere in a string.

The following table lists printer status messages. Some of these statuses are generated by the application itself; others are the responses from RFC 2790 Device Status, Printer Status, and Printer Detected errors.

Status	Description of Condition
Communication Error External	A communication error has occurred with the network controller or communication has been lost. A machine power off/power on might help. If the problem persists, service might be required. Printing has stopped.
Communication Error Internal	An internal communication error has occurred with one or more printer components. A machine power off/power on might help. Printing might be disabled.
Consumable Missing	A consumable that is involved with the generation of images on paper (e.g., fuser, waste collection, photo drum, print cartridge, xerographic module, etc.) has been removed from the machine. This state is only generated on those printers that comply w/ RFC 2790 Host Resources MIBv2.
Door Open	A cover or an interlock has been opened on the machine, which caused the machine to stop print operations. (Typically for safety reasons)
Drum Invalid	The machine has detected an invalid photo conductor drum. User intervention is required to verify the make and model of the installed drum. Printing cannot start.
Drum Missing	The machine cannot detect the photo conductor drum. User intervention is required to re-seat the drum module. Service might be required if the problem persists. Printing cannot start.
Drum Reorder	The machine has detected that its photo conductor drum is nearing the end of its useful life. A new drum module should be ordered soon. Printing can continue.
Drum Replace	The machine has detected that photo conductor drum has reached the end of its useful life. A new drum module should be installed now to maintain image quality and ensure that print operations are not interrupted.
Finisher Failed	The machine has detected a failure within the finisher module. Service is required to repair the finisher. Printing can continue but the finisher is disabled.
Finisher Full	The finisher is full. User intervention is required. Unload the finisher. Printing has stopped for the current job.
Fuser Invalid	The machine has detected an invalid fuser module. User intervention is required to verify the make and model of the fuser module. Printing cannot start.
Fuser Overtemp	The fuser has exceeded its normal operating temperature. User intervention is required to power off/power on the machine. The fuser should be replaced if the problem persists. Printing is disabled.
Fuser Reorder	The machine has determined that it is time to reorder a fuser module. User intervention is required to reorder the fuser module to avoid an interruption of print service. Printing can continue.
Fuser Replace	The fuser module has reached its end-of-life and must be replaced. User intervention is required to replace the fuser module. Printing has stopped.
Fuser Undertemp	The fuser module has failed to reach the proper operating temperature in the appropriate amount of time. Replace the fuser. Printing has stopped.
Hard Disk Missing	The machine cannot detect the hard disk. It might have been removed or has failed. User intervention is required to verify that the disk is present and operational. Printing is disabled.
Hole Punch Waste Full	The machine has detected that the finisher's hole punch waste container is full. User intervention is required to empty/replace the hole punch waste container. Printing can continue.
Image Disk Error	The printer has detected either an image disk read/write problem or has received bad data from the image disk. Xerox service is required. Printing has stopped.
Input Tray Empty	One of the machine's paper trays has exhausted its supply of paper. However, printing can continue if media is available from other paper trays.

Status	Description of Condition
Input Tray Missing	One of the trays that supply paper to the printer has been removed from the machine. This state is typically used for low-volume printers that require a paper tray to be removed in order to load paper. This state is only generated on those machines that comply w/ RFC 2790 Host Resources MIBv2.
Intervention Required	There is either a critical or non-critical condition in a printer that requires either simple user intervention (e.g., to close a door or paper tray, confirm a local UI setting, etc.) or a field service technician (e.g., replace a faulted board, run intrusive diagnostics to calibrate image quality, etc.)
Job Accounting Log Corrupted	
Job Accounting Log Full	The machine's accounting log is full. An account administrator needs to retrieve the accounting data from the machine in order to restore machine operation. All machine functions are disabled.
Low Paper	The supply of paper has reached a level where it will soon need to be replaced to ensure the print operations are not interrupted. The number of images that the printer can generate during this state varies among printer vendors
Machine Configuration Incorrect	A hardware configuration mismatch was detected during power up. Service is required. The machine is unavailable for any printing.
No Answer From Device	A printer was queried for status, but that printer has not responded to the request due to one of any number of reasons (e.g., communications problem, device turned off, SNMP routing disabled, etc.)
No Toner / Ink	The machine has exhausted its supply of dry ink/solid ink and can no longer generate images on paper.
Non-Compliant Error Received	The printer's MIB instrumentation has incorrect values exposed for a critical machine state. The printer-alert table must be used to determine the true status of the printer.
Non-Compliant Warning Received	The printer's MIB instrumentation has incorrect values exposed for a non-critical machine state. The printer-alert table must be used to determine the true status of the printer.
Offline	A generic state that is typically used to indicate when a machine has stopped printing. This state is usually accompanied by another more critical fault state. (e.g., door open + offline; service requested + offline; etc.)
Offline & Intervention Required	Represents other unique machine fault conditions that are not specifically enumerated by the industry standard MIB implemented by printers (e.g., intrusive diagnostic mode active, a board has failed within the imaging module, a job handling process has died within the network controller, etc.)
Offline Only	Depending on the printer's MIB implementation, this might indicate; A) a machine's input queue might be disabled from receiving jobs because an Admin has entered the configuration screens within the machine's local UI; or, B) a machine is recovering from a fault condition that has stopped printing; or C) a machine is in the process of powering-up.
Out of Memory	The machine has run out of memory while performing the current operation. User intervention is required to Power OFF/On the machine; otherwise an SA is required to install additional memory if the problem persists. Printing is disabled.
Out of Paper	The machine has completely exhausted its supply of paper, which has caused the print operation to stop.
Output Bin Full	The tray that collects finished documents produced by the printer cannot accept any additional documents and has caused printing to stop. This state is only generated on those printers that comply w/ RFC 2790 Host Resources MIBv2.
Output Bin Near Full	The tray that collects finished documents needs to be emptied; the machine will even-

Status	Description of Condition
	tually stop printing. This state is only generated on those printers that comply w/ RFC 2790 Host Resources MIBv2.
Output Tray Missing	One of the trays that collect finished documents produced by the printer has been removed. This state is typically used for those printers that have removable output trays. This state is only generated on those printers that comply w/ RFC 2790 Host Resources MIBv2.
Overdue Preventative Maintenance	The machine has detected that the interval between maintenance checks has been exceeded. This state is only generated on those printers that comply w/ RFC 2790 Host Resources MIBv2.
Paper Jammed	Paper has become lodged in some portion of the machine's image path, which prevents printing.
Scanner Failed	The machine has detected a failure in the scanner that disables printing and scanning services. User intervention is required to power off/power on the machine. Service is required if the problem persists.
Scanner Feed Roller Reorder	The machine has determined that it is time to reorder a scanner feed roller. User intervention is required to reorder the feed roller to avoid an interruption of scanning services. Printing can continue.
Scanner Feed Roller Replace	The machine has determined that the scanner feed roller has reached the end of its life. User intervention is required to replace the feed roller to avoid an interruption of scanning services. Printing can continue.
Stapler Malfunction	A malfunction has occurred in the finisher's stapler unit. User intervention is required to correct the malfunction. Printing can continue but stapling is disabled.
Staples Empty	The finisher's stapler cartridge is empty. User intervention is required to replace the cartridge. Printing can continue but stapling is disabled.
Staples Invalid	The finisher's stapler cartridge is not correct for the device. User intervention is required to remove the cartridge and replace it with the correct unit. Printing can continue, but stapling is disabled.
Staples Low	The finisher's stapler cartridge is low on staples; only 19 more sets can be stapled. User intervention is required to replace the cartridge. Printing can continue.
Staples Missing	The finisher's stapler cartridge is missing or incorrectly installed. User intervention is required to replace the Cartridge. Printing can continue but stapling is disabled.
Technician Dispatch Required	A critical condition in a printer requires a field service technician (e.g., replace a faulted board, run intrusive diagnostics to calibrate image quality, etc.)
Toner level: 10% Low Black	A printer's black toner is depleted to a level of 10% of capacity for devices that comply with RFC-1759, Marker Supplies and Marker Colorant tables.
Toner level: 10% Low Cyan	A printer's cyan toner/ink is depleted to a level of 10% of capacity for devices that comply with RFC-1759, Marker Supplies and Marker Colorant tables.
Toner level: 10% Low Magenta	A printer's magenta toner/ink is depleted to a level of 10% of capacity for devices that comply with RFC-1759, Marker Supplies and Marker Colorant tables.
Toner level: 10% Low Yellow	A printer's yellow toner/ink is depleted to a level of 10% of capacity for devices that comply with RFC-1759, Marker Supplies and Marker Colorant tables.
Toner level: 20% Low Black	A printer's black toner/ink is depleted to a level of 20% of capacity for devices that comply with RFC-1759, Marker Supplies and Marker Colorant tables.
Toner level: 20% Low Cyan	A printer's cyan toner/ink is depleted to a level of 20% of capacity for devices that comply with RFC-1759, Marker Supplies and Marker Colorant tables.
Toner level: 20% Low	A printer's magenta toner/ink is depleted to a level of 20% of capacity for devices that

Status	Description of Condition
Magenta	comply with RFC-1759, Marker Supplies and Marker Colorant tables.
Toner level: 20% Low Yellow	A printer's yellow toner/ink is depleted to a level of 20% of capacity for devices that comply with RFC-1759, Marker Supplies and Marker Colorant tables.
Toner level: 30% Low Black	A printer's black toner/ink is depleted to a level of 30% of capacity for devices that comply with RFC-1759, Marker Supplies and Marker Colorant tables.
Toner level: 30% Low Cyan	A printer's cyan toner/ink is depleted to a level of 30% of capacity for devices that comply with RFC-1759, Marker Supplies and Marker Colorant tables.
Toner level: 30% Low Magenta	A printer's magenta toner/ink is depleted to a level of 30% of capacity for devices that comply with RFC-1759, Marker Supplies and Marker Colorant tables.
Toner level: 30% Low Yellow	A printer's yellow toner/ink is depleted to a level of 30% of capacity for devices that comply with RFC-1759, Marker Supplies and Marker Colorant tables.
Toner level: 40% Low Black	A printer's black toner is depleted to a level of 40% of capacity for devices that comply with RFC-1759, Marker Supplies and Marker Colorant tables.
Toner level: 40% Low Cyan	A printer's cyan toner/ink is depleted to a level of 40% of capacity for devices that comply with RFC-1759, Marker Supplies and Marker Colorant tables.
Toner level: 40% Low Magenta	A printer's magenta toner/ink is depleted to a level of 40% of capacity for devices that comply with RFC-1759, Marker Supplies and Marker Colorant tables.
Toner level: 40% Low Yellow	A printer's yellow toner is depleted to a level of 40% of capacity for devices that comply with RFC-1759, Marker Supplies and Marker Colorant tables.
Toner level: 50% Low Black	A printer's black toner/ink is depleted to a level of 50% of capacity for devices that comply with RFC-1759, Marker Supplies and Marker Colorant tables.
Toner level: 50% Low Cyan	A printer's cyan toner/ink is depleted to a level of 50% of capacity for devices that comply with RFC-1759, Marker Supplies and Marker Colorant tables.
Toner level: 50% Low Magenta	A printer's magenta toner/ink is depleted to a level of 50% of capacity for devices that comply with RFC-1759, Marker Supplies and Marker Colorant tables.
Toner level: 50% Low Yellow	A printer's yellow toner/ink is depleted to a level of 50% of capacity for devices that comply with RFC-1759, Marker Supplies and Marker Colorant tables.
Toner level: Low Black	Black toner/ink is depleted to the low level defined within the machine. User intervention is required to order replacement toner/ink. Printing can continue.
Toner level: Low Cyan	Cyan toner/ink is depleted to the low level defined within the machine. User intervention is required to order replacement toner/ink. Printing can continue.
Toner level: Low Magenta	Magenta toner/ink is depleted to the low level defined within the machine. User intervention is required to order replacement toner/ink. Printing can continue.
Toner level: Low Yellow	Yellow toner/ink is depleted to the low level defined within the machine. User intervention is required to order replacement toner. Printing can continue.
Toner level: No Black	Black toner/Ink is completely depleted. User intervention is required to replace the toner/ink cartridge. Printing is stopped.
Toner level: No Cyan	Cyan toner/ink is completely depleted. User intervention is required to replace the toner/ink cartridge. Printing is stopped.
Toner level: No Magenta	Magenta toner/ink is completely depleted. User intervention is required to replace the toner/ink cartridge. Printing is stopped.
Toner level: No Yellow	Yellow toner/ink is completely depleted. User intervention is required to replace the toner/ink cartridge. Printing is stopped.
Toner / Ink Low	The machine's supply of dry ink/solid ink has reached a level where it will need to be reordered and/or replaced to ensure the print operations are not interrupted. The number of images that the printer can generate during this state varies among printer

Status	Description of Condition
	vendors.
Tray Configuration Incorrect	Tray settings conflict with those required for the current job. User intervention is required to confirm the paper size settings of the tray for the current job at the local UI. Printing has stopped for the current job.
Waste Bottle Full	The waste bottle/developer collector is either missing or full. User intervention is required to replace the waste bottle/developer collector.
Waste Bottle Near Full	The waste bottle/developer collector is nearly full. User intervention is required to reorder the waste bottle/developer collector.
Xerographic Module Invalid	The machine has detected an invalid Xerographic module. User intervention is required to verify the make and model of the installed Xerographic module. Printing cannot start.
Xerographic Module Missing	The machine cannot detect the Xerographic module. User intervention is required to reseat the Xerographic module. Service might be required if the problem persists.
Xerographic Module Reorder	The Xerographic module is nearing the end of its useful life. A new Xerographic module should be ordered soon.
Xerographic Module Replace	The Xerographic module has reached the end of its useful life. A new Xerographic module should be installed now to maintain image quality and ensure that print operations are not interrupted.

This table shows direct printer errors.

Status	Description of Condition
Direct Printer Access Denied	Network, Server or Credential error
Direct Printer Initializing	The printer fuser/marking engine is warming up or the print engine is restarting.
Direct Printer Manual Feed Required	Human intervention required for special paper or job requirements.
Direct Printer Out of Memory	Upper printer memory limit has been reached
Direct Printer Page Punt	Page is ejected from the printer after some event caused it not to print or not complete; e.g., not receiving a formfeed from the application.
Direct Printer Paper Problem	Paper has become lodged in some portion of the machine's image path, which prevents printing.
Direct Printer Paused	The printer queue has been suspended.
Direct Printer User Intervention Required	A condition in the printer has forced an error that requires human intervention.
Direct Printer Waiting	Idle