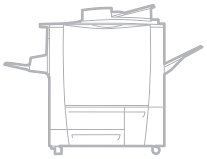
Xerox ColorQube
9301 / 9302 / 9303
Multifunction Printer
Imprimante multifonction



Xerox® ColorQube®

9301 / 9302 / 9303

System Administrator Guide

Guide de l’administrateur système

Español	Guía del administrador del sistema
Português	Guia de Administração do Sistema

Document version 1.0: April 2011

Contents

8 Faxing 137

9 Accounting 157

10 Administrator Tools 167

Introduction 1

This chapter includes:

Overview

This guide is designed for a system administrator with network administrator rights who understands networking concepts and has experience creating and managing network user accounts.

Use this guide to help you install, configure, and manage your printer on a network.

Notes:

- Network features are not available when you are connected over USB.
- Embedded fax features are not available for all printer models.

Configuration Steps

When configuring the printer for the first time, complete the following tasks:

1. Connect an Ethernet cable from your printer to the network.
2. Confirm that your printer is recognized on your network. By default, the printer is configured to receive an IP address from a DHCP server over a TCP/IP network. If you have another type of network, or want to assign a static IP address, see IP on page 25.
3. Complete the installation wizards. These wizards help you configure basic printer settings such as your location, time zone, and date and time preferences.
4. Print a Configuration Report listing the current printer configuration. Review the report and locate the printer IP address. For details, see Configuration Report on page 15.
5. Open a Web browser and type the IP address of your printer to access CentreWare Internet Services. CentreWare Internet Services is the administration and configuration software installed on the embedded Web server in the printer. For details, see Accessing CentreWare Internet Services on page 17.

   Note: Most configuration settings are located on the Properties tab in CentreWare Internet Services.

6. Print the Configuration Checklist. The Configuration Checklist provides space for you to write down important information as you go through the configuration process. Use it to record information about your network settings, including passwords, network paths, and server addresses.
7. Configure Authentication. For details, see Setting Up Access Rights on page 58.
8. Configure Security. For details, see Security on page 57.
9. Enable services in CentreWare Internet Services. For details, see Enabling Services on page 18.
10. Configure Print, Scan, and Fax features. For details, see Printing on page 99, Scanning on page 117, and Faxing on page 137.
11. Configure Accounting. For details, see Accounting on page 157.

    Note: Not all printer models support these features.

More Information

You can obtain more information about your printer from these sources:

Resource	Location
Installation Guide	Packaged with printer and at www.xerox.com/office/CQ9301_CQ9302_CQ9303docs
Quick Use Guide	Packaged with printer and at www.xerox.com/office/CQ9301_CQ9302_CQ9303docs
User Guide	Software and Documentation Disc and at www.xerox.com/office/CQ9301_CQ9302_CQ9303docs
Video Tutorials	www.xerox.com/office/CQ9301_CQ9302_CQ9303docs
Recommended Media List	United States: www.xerox.com/paper Europe: www.xerox.com/europaper
Technical support information for your printer. Includes online technical support, Online Support Assistant, and driver downloads.	www.xerox.com/office/CQ9301_CQ9302_CQ9303support
Information about printer menus or error messages.	Control panel Help (?) button
Information pages	Click **Status** > **Information Pages** in CentreWare Internet Services
CentreWare Internet Services Help	Help button in CentreWare Internet Services
Order supplies for your printer	www.xerox.com/office/CQ9301_CQ9302_CQ9303supplies
A resource for tools and information, such as interactive tutorials, printing templates, helpful tips, and customized features to meet your individual needs.	www.xerox.com/office/businessresourcecenter
Local sales and support center	www.xerox.com/office/worldcontacts
Printer registration	www.xerox.com/office/register
Xerox® Direct online store	www.direct.xerox.com/

Initial Setup 2

This chapter includes:

Physically Connecting the Printer

1. Connect the power cord to the printer, and plug it into an electrical outlet.
2. Connect one end of a Category 5 or better Ethernet cable to the Ethernet port on the back of the printer. Connect the other end of the cable to a correctly configured network port.
3. If your printer has fax installed, connect it to a correctly configured telephone line.
4. Turn on the printer.

Initial Setup at the Control Panel

Installation Wizard

The Installation wizard starts the first time you turn on the printer. The wizard prompts you with a series of questions to help you configure basic printer settings.

> Note: You can change these settings at any time.

Quick Setup Home

After the Installation wizard completes, the Quick Setup Home wizard appears. Use the Quick Setup Home wizard to configure printer settings.

> Note: You can complete the wizard at any time.

1. Use the IP Address Settings wizard to assign a static IP address or change the default dynamic addressing settings.
2. Use the Contact Numbers wizard to type phone numbers for support or supplies.

   After the Quick Setup Home wizard completes, the printer restarts and a Configuration Report automatically prints.

Configuration Report

The Configuration Report lists all current settings of the printer. A configuration report prints at startup by default.

1. In CentreWare Internet Services, click **Status** > **Configuration Report**.
2. To print the report, click **Print Configuration Page**.

To turn off automatic printing of a Configuration Report at startup, see Disabling the Configuration Report at Startup on page 16.

> Note: If the system administrator has restricted printing of the Configuration Report, you need a user name and password to print. For details, see the system administrator.

System Administrator Access at the Control Panel

1. At the printer control panel, press the **Machine Status** button, then touch the **Tools** tab.
2. Press the **Log In/Out** button.
3. Type **admin** and touch **Next**.
4. Type the **Admin Password** and touch **Enter**. The default password is **1111**.

Disabling the Configuration Report at Startup

1. In CentreWare Internet Services, click **Properties** > **Services**.
2. Click **Printing** > **General**.
3. Under Configuration Report, clear **Print at Power on**.
4. Click **Apply** to save the new settings or **Undo** to retain the previous settings.

Manually Setting the Ethernet Interface Speed

The Ethernet interface on the printer automatically detects the speed of your network. Any auto-sensing devices connected to the network, such as a hub, do not always detect the correct speed. Refer to the configuration report to ensure that the printer detects the correct network speed.

1. At the printer control panel, press the **Machine Status** button, then touch the **Tools** tab.
2. Touch **Network Settings** > **Advanced Settings**.
3. When the warning message appears, touch **Continue**.
4. Touch **Ethernet Physical Media**.
5. Select the speed to match the speed of your hub or switch.
6. Touch **Save**, then touch **Close**.

Assigning a Network Address

The printer automatically acquires a network address from a DHCP server by default. To assign a static IP address, configure DNS server settings, or configure other TCP/IP settings, see IP on page 25.

Initial Setup in CentreWare Internet Services

CentreWare Internet Services is the administration and configuration software installed on the embedded Web server in the printer. It allows you to configure and administer the printer from a Web browser.

Before you begin:

- TCP/IP and HTTP must be enabled to access CentreWare Internet Services. If you disable either of these services, enable them at the printer before accessing CentreWare Internet Services.
- Locate your printer IP address using the Configuration Report.

  Note: If your printer is locked, type the system administrator user name and password to access the Properties tab. The administrator user name is **admin** and the default password is **1111**.

Accessing CentreWare Internet Services

At your computer, open a Web browser, type the IP address of the printer in the address field, then press **Enter** or **Return**.

Locking or Unlocking the Printer

1. In CentreWare Internet Services, click **Properties** > **Security** > **Authentication**.
2. Click **Tools & Feature Access**.
3. Under Presets, select:
   - **Standard Access - Only Lock Tools** to lock the printer.
   - **Open Access - Unlock All Tools and Features** to unlock the printer.
   - **Custom Access** to select to lock or unlock individually any of the services in the list.
4. Click **Apply** to save the new settings or **Undo** to retain the previous settings.

Changing the System Administrator Password

Xerox® recommends that you change the default system administrator password after you configure the printer. Be sure to store the password in a secure location.

1. In CentreWare Internet Services, click **Properties** > **Security**.
2. Click **Admin Password**.
3. Under User Name, type the **New Password**.
4. Retype the password to verify.
5. Click **Apply** to save the new settings or **Undo** to retain the previous settings.

Using the Configuration Overview Page

The Configuration Overview page contains links to the commonly-accessed pages on the Properties tab. Use the Configuration Overview page to help you install your printer successfully.

1. In CentreWare Internet Services, click **Properties** > **Configuration Page**.
2. To configure any of the services or features, click **Settings** next to the service to open that page. You can also click **View** to open a page showing all options that you can select to create a clone file. Possible options include:
    - **SMart eSolutions**
    - **Print Protocols**
    - **Email**
    - **Workflow Scanning**
    - **Server Fax**
    - **Internet Fax**
    - **Cloning**

    Note: Not all options listed are supported on all printers. Some options apply only to specific printer models or configurations.

Assigning the Printer Name and Location

1. In CentreWare Internet Services, click **Properties** > **Description**.
2. Under **Device Name**, type a name for the printer.
3. Under **Location**, type the location of the printer.
4. Click **Apply** to save the new settings or **Undo** to retain the previous settings.

Enabling Services

Services must be enabled before they can be managed through the Tools and Feature Access page.

1. In CentreWare Internet Services, click **Properties** > **Services**.
2. Click **Service Registration**.
3. Select the services to enable or click **Enable All**.
4. Click **Apply** to save the new settings or **Undo** to retain the previous settings.

    Note: If a service is not enabled on the Service Registration page, you cannot view or manage it from the Tools and Features page. Ensure that the desired service is enabled.

Viewing Services on the Control Panel

1. At the printer control panel, press the **Machine Status** button, then touch the **Machine Information** tab.
2. Touch **Installed Options**.

    All installed options registered in CentreWare Internet Services and their status appear. Set options to Locked or Unlocked on the Tools & Services page.

Physical Connection Settings

You can specify Ethernet and USB settings, such as Ethernet Rated Speed, USB Connection Mode, and Print Timeout for USB printing.

Setting Ethernet Options

1. In CentreWare Internet Services, click **Properties** > **Connectivity** > **Physical Connections**.
2. Click **Ethernet**.
3. Under Rated Speed, click the down arrow and select the speed of your connection.
4. Click **Apply** to save the new settings or **Undo** to retain the previous settings.

   Click **Default All** to reset settings to default values.

   Note: Restart the printer for the new settings to take effect.

Setting USB Options

1. In CentreWare Internet Services, click **Properties** > **Connectivity** > **Physical Connections**.
2. Click **USB Settings**.
3. Under USB Connection Mode, select an option:
   - **Software Tools**: Select this option if you are using Xerox® Copier Assistant, or if you want to disable Direct Printing via Driver. Xerox representatives also use this option to connect directly to the printer and use diagnostic software and other software utilities.
   - **Direct Printing via Driver**: Select this option to allow users to connect to the printer using a USB cable.
4. Under Print Timeout, type the amount of time in seconds that the printer waits inactive before disconnecting from a device connected to the port. Type **0** to disable the timeout.
5. Click **Apply**.

Network Configuration 3

This chapter includes:

AppleTalk

AppleTalk is a proprietary suite of protocols developed for networking computers by Apple, Inc. An AppleTalk zone is a group of nodes or networks organized by departments or physical locations.

Before you begin:

- Verify that there is an existing operational AppleTalk network.
- Determine the AppleTalk Name you wish to assign to your printer.
- Determine the AppleTalk Zone, if used, to assign to your printer.

1. In CentreWare Internet Services, click **Properties** > **Connectivity** > **Protocols**.
2. Click **AppleTalk**.
3. Under Protocol, select **Enabled** to enable the protocol.
4. Under Printer Name, type the printer name or use the default name. The default printer name is based on the printer MAC address.
5. Under Zone Name, type a new zone name or use the default AppleTalk local zone. The default AppleTalk local zone is *.
6. Click **Apply** to save the new settings or **Undo** to retain the previous settings.
7. Click **Default All** to reset settings to default values.

NetWare

NetWare is a network operating system developed by Novell to run various services using cooperative multitasking.

Before you begin:

- Ensure an existing operational NetWare network is available.
- Verify that you have administrator rights to log in to a NetWare file server or tree.
- Ensure that the printer is connected to the network.
- Set up a print server object using the appropriate Novell utility. Refer to the Novell system documentation for help.

Configuring NetWare Settings

1. In CentreWare Internet Services, click **Properties** > **Connectivity** > **Protocols**.
2. Click **NetWare**.
3. Select **Enabled** to enable the protocol.
4. Select **IP** or **IPX** from the Filing Transport menu.
5. Select the Frame Type from the menu. Options are:
   - **Auto**
   - **Ethernet II**
   - **Ethernet 802.2**
   - **Ethernet 802.3**
6. Type a polling rate between **1–240** seconds for the print server in Queue Poll Interval. The default value is 5 seconds.
7. Type the Printer Server Name. The default name is **XRX_MAC address**.
8. Type then retype the server password in the New Print Server Password and Retype New Print Server Password fields.
9. Enable **Select to save new password**.

Service Advertising Protocol

Service Advertising Protocol (SAP) sends periodic broadcast messages to other network components about available services on the printer. SAP facilitates dynamic adding and removing of services on an IPX internetwork. As servers start up and shut down, they can advertise and remove their services using SAP.

1. Under Protocol, select **Enabled**.
2. Under SAP Frequency, type the time in seconds between **15–300**. The default time value is 60 seconds.

Configuring NetWare Bindery Settings

Bindery services are a stand-alone database system that contains user information and security data. NetWare can use Bindery services for authentication.

If you are using Bindery mode, under Bindery Settings, type the names of up to four primary file servers in the File Server fields.

> Note: When the printer uses Bindery mode, the NDS Tree and NDS Context fields are blank.

Configuring NetWare Directory Services (NDS) Settings

NetWare Directory Services (NDS) is a hierarchical, object-oriented database that represents all of the assets of an organization in a logical tree structure. Assets can include printers, servers, computers, people, organizations, and more.

1. Under NetWare Directory Services (NDS), select the preferred address type. Select **IPv4** to set a static IPv4 address or select **Host Name** to configure with an NDS server.

   Note: The NDS server is used for Workflow Scanning and Server Fax only.

2. Type a name for the NDS tree. The default entry for this field is **Xerox_DS_Tree**. If you are using bindery or bindery emulation, leave this field blank.
3. Type a name for the context. The default entry for this field is **Xerox_DS_Context**. If you are using bindery or bindery emulation, leave this field blank.
4. Click **Apply** to save the new settings or **Undo** to retain the previous settings.
5. Click **Default All** to reset settings to default values.

IP

Internet Protocol (IP) is a protocol within the Internet Protocol Suite that manages the transmission of messages from computer to computer.

Enabling TCP/IP

1. At the printer control panel, press the **Machine Status** button, then touch the **Tools** tab.
2. Touch **Network Settings** > **TCP/IP Settings**.
3. Touch **TCPIP Enablement**.
4. Touch **Enable** for IPv4 or IPv6, then touch **Save**.

   Note: By default, TCP/IP is enabled. If you disable TCP/IP, enable it at the printer control panel before you access CentreWare Internet Services.

Configuring TCP/IP Settings at the Control Panel

Manually Configuring the Network Address

1. At the printer control panel, press the **Machine Status** button, then touch the **Tools** tab.
2. Touch **Network Settings** > **TCP/IP Settings**.
3. Touch **Dynamic Addressing**.
4. Touch **Disabled**, then touch **Save**.
5. Touch **IP Address/Host Name**.
6. Touch the field under IPv4 Address, then type the static IP address using the touch screen keypad.
7. Touch the field under **Host Name**, then type the host name.
8. Touch **Save**, then touch **Close**.
9. Touch **Subnet and Gateway**.
10. Touch **Subnet Mask**, then type the subnet mask address using the touch screen keypad.
11. Touch **Save**.
12. Touch **IP Gateway**, type the gateway address using the touch screen keypad, then touch **Save**.

Configuring Dynamic Address Settings

1. At the printer control panel, press the **Machine Status** button, then touch the **Tools** tab.
2. Touch **Network Settings** > **TCP/IP Settings**.
3. Touch **Dynamic Addressing**.
4. Touch **DHCP** or **BOOTP**, then touch **Save**.

Configuring DNS/DDNS Settings at the Control Panel

Domain Name System (DNS) and Dynamic Domain Name System (DDNS) are systems that map host names to IP addresses.

1. At the printer control panel, press the **Machine Status** button, then touch the **Tools** tab.
2. Touch **Network Settings** > **TCP/IP Settings**.
3. Touch **DNS Configuration**.

   Note: If DHCP is enabled, your company DHCP server can provide the following information.

4. Touch **Domain Name**, touch the field under Domain Name, type the domain name using the touch screen keypad, then touch **Save**.
5. Touch **DNS Servers**.
   a. Touch **Primary DNS Server**, then type the server address using the touch screen keypad.
   b. Touch **Alternate DNS Server #1**, then type the server address using the touch screen keypad.
   c. Touch **Alternate DNS Server #2**, then type the server address using the touch screen keypad.
   d. Touch **Save**, then touch **Close** to exit the DNS Servers screen.
6. Touch **Dynamic DNS Registration**, and touch **Enable** under IPv4 or IPv6 if necessary.

Configuring IP Settings in CentreWare Internet Services

If your printer has a valid network address, you can configure TCP/IP settings in CentreWare Internet Services.

Configuring IPv4

You can use IPv4 or IPv6 in addition to or in place of the other.

1. In CentreWare Internet Services, click **Properties** > **Connectivity** > **Protocols**.
2. Click **IP (Internet Protocol)** > **IPv4**.
3. Under Protocol, select **Enabled** to enable the protocol.

⚠ CAUTION: If both IPv4 and IPv6 are disabled, you cannot access CentreWare Internet Services. To access IPv4 and IPv6 settings in CentreWare Internet Services, enable TCP/IP at the printer control panel. If you disable TCP/IP or change the IP address, any dependent protocols are disabled and the network controller restarts.

4. Under IP Address Resolution select an option from the drop-down list. Depending on the option you select, some or all of the fields can be disabled.
   - **STATIC**: This option disables dynamic addressing and allows you to type a static IP address. Type the Machine IP Address, Subnet Mask, and Gateway Address.
   - **BOOTP**: This option allows your DHCP server to assign an IP address to the printer. Dynamic DNS Registration is enabled.
   - **DHCP**: This option allows your DHCP server to assign an IP address to the printer. Dynamic DNS Registration is enabled.

5. Select **Enabled** under Release Registration to send a release request to the DHCP and DNS servers. If the servers grant the request, the current IP address and any dynamic DNS name are released when the printer is turned off.
6. Under Zero-Configuration Networking, select **Enabled** under Self Assigned Address. This option instructs the printer to assign itself an address if a DHCP server does not provide one.
7. Click **Apply** to save the new settings or **Undo** to retain the previous settings.
8. Click **Default All** to reset settings to default values. This option also disables FIPS 140 mode.

Configuring Settings for IPv6

IPv6 hosts can automatically configure themselves when connected to a routed IPv6 network using the Internet Control Message Protocol Version 6 (ICMPv6). ICMPv6 performs error reporting for IP along with other diagnostic functions. When first connected to a network, a host sends a link-local multicast router solicitation request for configuration parameters. If suitably configured, routers respond to this request with a router advertisement packet containing network-layer configuration parameters.

1. In CentreWare Internet Services, click **Properties** > **Connectivity** > **Protocols**.
2. Click **IP** > **IPv6**.
3. Under Protocol, select **Enabled** to enable the protocol.

⚠ **CAUTION:** If both IPv4 and IPv6 are disabled, you cannot access CentreWare Internet Services. To access IPv4 and IPv6 settings in CentreWare Internet Services, enable TCP/IP at the printer control panel. If you disable TCP/IP or change the IP address, any dependent protocols are disabled and the network controller restarts.

4. Under Stateless Addresses, enable **Use Router Supplied Prefixes** to allow the router to assign address prefixes.
5. Under Default Dynamic Host Configuration Protocol (DHCP) Settings, select how DHCP operates for IPv6. Options are:
   - **Use DHCP as directed by a router**
   - **Always enable DHCP for address assignment and other configuration data**
   - **Always enable DHCP for other configuration data only**
   - **Never use DHCP**
6. Select **Release DHCPv6 Address at Power Down** to release the current DCHP-assigned address and any DNS name when the printer is turned off.
7. Select **Enable Manual Address** to specify an address manually. Select a Router Prefix from the menu, or type a new router prefix and click **Add**.
8. Select **Prefer IPv6 Address over IPv4** to use an IPv6 address before using an IPv4 address.
9. Click **Apply** to save the new settings or **Undo** to retain the previous settings.
10. Click **Default All** to reset settings to default values.

DNS

Domain Name System (DNS) and Dynamic Domain Name System (DDNS) are systems that map host names to IP addresses.

1. In CentreWare Internet Services, click **Properties** > **Connectivity** > **Protocols**.
2. Click **IP (Internet Protocol)** > **DNS**.
3. Under Host Name, type a unique name for your printer. If the host name successfully registers to the DNS server, the host name appears under Verified Host Name. The default host name is XRX_xxx, where xxx is the MAC address of the printer.

   Note: If no host name, or a different host name appears under Verified Host Name, the host name did not successfully register to the DNS server. Ensure that your network supports direct client DNS name registration, or configure your DHCP server to perform updates on behalf of the DHCP clients. Configure your DNS server to allow dynamic updates.

4. Under Domain Name, type the name of the domain to which the printer is connected.

   If the domain name successfully registers to the DNS server, the domain name appears under Verified Domain Name.

Note: If no domain name, or a different domain name appears, the domain name did not successfully register to the DNS server. Ensure that your network supports direct client DNS name registration, or configure your DHCP server to perform updates on behalf of the DHCP clients. Configure your DNS server to allow dynamic updates.

5. Select **Enabled** under Dynamic DNS Registration of IPv4 Address, or Dynamic DNS Registration of IPv6 Address, if desired. This option allows your DDNS server to register the host name of the printer automatically. If you change the host name in CentreWare Internet Services, the registered host name is updated on your DDNS server. Clear the **Enabled** check box if your network does not support dynamic name addressing. Manage host names in the DNS server manually.
6. Under Remove this Device's IPv4 DNS Registration, select **Enabled** if necessary. This option allows the printer to send a release request to the DHCP and DNS servers. If the servers grant the request, the current IP address and any dynamic DNS name are released when the printer is turned off.
7. Under Remove this Device's IPv6 DNS Registration at power down, select **Enabled** if necessary. This option allows the printer to release the current DCHP-assigned address and any DNS name when the printer is turned off.
8. To allow users to see and connect to the printer using Bonjour, under Multicast DNS Registration, select **Enabled**.
9. If you have a DHCP server, and the printer recognizes your DNS server, the address appears under DNS Server Addresses. If you want to use other DNS servers, type the IPv4 or IPv6 server address under Additional DNS Server Addresses.
10. Under DNS Connection Timeout, type the time in seconds that the printer waits if it fails to connect to a DNS server. After the timeout period, the printer attempts to connect to any additional DNS servers.
11. If you have a DHCP server, recognized search domain names appear in a list under Domain Name Search List.The list of domain names allows the DNS server to recognize unqualified host names. If you want the printer to search for other domain names, type the domain names under Additional Search Domains.
12. Under Append Device Domain, select **Enabled** to add the domain of the printer to the Domain Name Search List.
13. Under Append Parent Domains, select **Enabled** to add the parent domains of the printer to the Domain Name Search List.
14. Click **Apply**.

SLP

Printers use Service Location Protocol (SLP) to announce and look up services on a local network without prior configuration. When SLP is enabled, the printer becomes a Service Agent (SA) and announces its services to User Agents (UA) on the network using SLP.

Directory Agents (DA) are components that cache services. They are used in larger networks to reduce the amount of traffic. DAs are optional. If a DA is present, then User Agents (UAs) and System Agents (SAs) are required to use it instead of communicating directly with the printer.

Configuring SLP

1. In CentreWare Internet Services, click **Properties** > **Connectivity** > **Protocols**.
2. Click **SLP**.
3. Under Protocol, select **Enabled**.
4. Under Directory Agent, type the IP address for the Directory Agent (DA), if one is used. This entry is optional.
5. If you use scopes to group services, type in the Scope 1, 2, and 3 names. Printers cannot see services that are in different scopes. Under Message Type, select **Multicast** to route multicast packets between subnets, or select **Broadcast** not to route packets between subnets.
6. Select the Multicast Radius value between **0–255**. This value defines how many routers the multicast packet can cross. The default value is 255.
7. Select a value for Maximum Transmission Unit (MTU) size between **484–32768** bytes. The default value is 1400 bytes.

   Note: The maximum MTU for IP over Ethernet is 1500 bytes.
8. Click **Apply** to save the new settings or **Undo** to retain the previous settings.
9. Click **Default All** to reset settings to default values.

FTP

File Transport Protocol (FTP) is a standard network protocol used to pass and manipulate files over a TCP/IP network. Several services running on your printer, including Network Scanning, Saved Jobs Backup, and Software upgrade can use FTP as a filing service.

> Note: In Active mode, data transfers over a fixed, known port from a connection made from the server. In Passive mode, data transfers over a random port number specified by the FTP server from a connection made from the printer.

Setting FTP Mode

1. In CentreWare Internet Services, click **Properties** > **Connectivity** > **Protocols**.
2. Click **FTP**.
3. Under Mode, select the FTP operational mode to use when FTP is the selected protocol for network filing. Options are **Passive** or **Active**.

SNMP

Simple Network Management Protocol (SNMP) is a set of network protocols designed to allow you to manage and monitor devices on your network.

You can use the SNMP configuration pages in CentreWare Internet Services to:

- Enable or disable Authentication Failure Generic Traps.
- Enable SNMPv3 to create an encrypted channel for secure printer management.
- Assign privacy, authentication protocols, and keys to Administrative and key user accounts.
- Assign read and write access to User accounts.
- Limit SNMP access to the printer using hosts.

Enabling SNMP

1. In CentreWare Internet Services, click **Properties** > **Connectivity** > **Protocols**.
2. Click **SNMP**.
3. Select **Enable SNMP v1/v2c Protocols** to enable the protocol.
4. Select **Enable SMNP v3 Protocols** to enable the protocol.
5. Under Authentication Failure Generic Traps, select **Enable** to prompt the printer to generate a trap for every SNMP request processed with an invalid community name.
6. Click **Apply** to save the new settings or **Undo** to retain the previous settings.

   Note: Click **Apply** after enabling the protocols and before navigating to any other pages to ensure that your settings are saved.

Configuring SNMPv1/v2c

SNMP version 1 (SNMPv1) is the initial implementation of the SNMP protocol. SNMPv1 operates over protocols such as User Datagram Protocol (UDP), IP, and Novell Internet Packet Exchange (IPX).

SNMPv2c includes improvements in performance, confidentiality, and manager-to-manager communications over SNMPv1, however it uses the simple-community based security scheme of SNMPv1.

1. In CentreWare Internet Services, click **Properties** > **Connectivity** > **Protocols**.
2. Click **SNMP**.
3. Under SNMP Properties, click **Edit SNMPv1/v2c Properties**.
4. Type a name up to **256** characters for the GET Community Name or use the default value of **public**. GET returns the password for the SNMP GET requests to the printer. Applications obtaining information from the printer using SNMP, such as CentreWare Internet Services, use this password.
5. Type a name up to **256** characters for the SET Community Name or use the default value of **private**. SET returns the password for the SNMP SET requests to the printer. Applications that set information on the printer using SNMP use this password.

⚠ CAUTION: Changes made to the GET or SET community names for this printer require corresponding changes to GET or SET community names applications using SNMP.

6. Type a name up to **256** characters for the default TRAP Community Name or use the default value of **SNMP_TRAP**.

   Note: Use the Default TRAP Community Name to specify the default community name for all traps generated by this printer. Individual Trap Community Names specified for each trap destination address can override the community name. Each Trap Community Name must be unique.

7. Click **Save** to apply the new settings or **Undo** to retain the previous settings.
   Click **Cancel** to return to the previous page.

Configuring SNMPv3

SNMPv3 is the current standard version of SNMP defined by the Internet Engineering Task Force (IETF). It provides three important security features:

- Message integrity to ensure that a packet has not been tampered with in transit
- Authentication to verify that the message is from a valid source
- Encryption of packets to prevent unauthorized access

Before you begin:

- Ensure that Secure HTTP (SSL) is enabled.
- Ensure that a certificate is installed on the printer.

Editing SNMPv3 Properties

1. In CentreWare Internet Services, click **Properties** > **Connectivity** > **Protocols**.
2. Click **SNMP**.
3. Under SNMP Properties, click **Edit SNMP v3 Properties**.
4. Under Administrator Account, select **Account Enabled** to create the administrator account.
5. Type and confirm the **Authentication Password**. The Authentication Password is used to generate a key used for authentication.
6. Type and confirm the **Privacy Password**. The Privacy Password is used for encryption of SNMPv3 data. The passphrase used to encrypt the data must match the passphrase on the Server.

   Note: The passwords must be at least 8 characters in length and can include any characters except control characters.

7. Select the checkbox to save new password.
8. Under Print Drivers/Remote Clients Account, click **Account Enabled**. To reset the default password, click **Reset**. This account allows Xerox® clients and drivers limited access to objects on the printer.
9. Click **Save** to apply the new settings or **Undo** to retain the previous settings.
10. Click **Cancel** to return to the previous page.

Configuring SNMP Advanced Settings

You can add, edit, or delete IP and IPX addresses for Network Management workstations that receive traps from the printer.

Configuring SNMP Advanced Settings

1. In CentreWare Internet Services, click **Properties** > **Connectivity** > **Protocols**.
2. Click **SNMP**.
3. Click **Advanced Settings**.
4. To add an IP trap destination address, under Trap Destination Addresses, click **Add IP Address**.
5. To add an IPX trap destination address, under Trap Destination Addresses, click **Add IPX Address**.
6. To edit an address, next to the address click **Edit**.
7. To delete an address, select the check box next to the address and click **Delete**.

Adding or Editing an IP Trap Destination Address

1. On the Advanced Settings page, click **Add IPX Address**, or select an existing address and click **Edit**.
2. Type the IP address of the host running the SNMP manager that receives traps.
3. Type the UDP Port Number. The default is 162 for traps.
4. Select the SNMP version based on what the system receiving traps supports.
5. Select the type of traps that the SNMP manager receives under Traps to be Received.
6. Click **Save** to apply the new settings or **Undo** to retain the previous settings.
7. Click **Cancel** to return to the previous page.

Adding or Editing an IPX Trap Destination Address

1. On the Advanced Settings page, click **Add IP Address**, or select an existing address and click **Edit**.
2. Type the 8-digit hexadecimal number that identifies the IPX External Network host configured to receive the trap.
3. Type the 48-bit Physical MAC Address of the computer running the SMNP manager application receiving the trap.
4. Type the IPX Socket Number of the computer running the SNMP manager application configured to receive the packets. The default IPX Socket Number is 9010.
5. Select the SNMP Version.
6. Select the type of traps that the SNMP manager receives under Traps to be Received.
7. Click **Save** to apply the new settings or **Undo** to retain the previous settings.
8. Click **Cancel** to return to the previous page.

SSDP

Simple Service Discovery Protocol (SSDP) provides processes to allow network clients with little or no static configuration to discover network services. SSDP provides multicast discovery, server-based notification, and discovery routing options.

1. In CentreWare Internet Services, click **Properties** > **Connectivity** > **Protocols**.
2. Click **SSDP**.
3. Under Protocol, select **Enabled**.
4. Under Cache Control, type a value between **1–43200** minutes. The default value is 1440 minutes.
5. Under Time to Live, type a number between **1–60** router hops for discovery advertisement. The default number of hops is 4.
6. Click **Apply** to save the new settings or **Undo** to retain the previous settings.

   Click **Default All** to reset settings to default values.

Microsoft Networking

When running WINS, the printer registers its IP address and NetBIOS Host Name with a WINS server. WINS allows the printer to communicate using host name only. Using Microsoft Networking removes significant overhead for systems administrators.

Configuring Microsoft Networking

1. In CentreWare Internet Services, click **Properties** > **Connectivity** > **Protocols**.
2. Click **Microsoft Networking**.
3. Under Protocol, select **Enabled** to enable the protocol.
4. Type the name of the workgroup in the Workgroup field.
5. Type the host name used to provide shared access and authenticate interprocess communication in the SMB Host Name field.
6. If desired, type a descriptive comment in the SMB Host Name Comment field.
7. Type the name of the share in the Share Name field.
8. If desired, type a descriptive comment in the Share Name Comment field.
9. Type the maximum number of connections allowed, between **10–30**, in Maximum Connections.
10. Type the desired number of seconds, between **1–32767**, until the connection times out.

Configuring WINS

1. Under Server Information, select **Enabled** to enable the protocol.
2. Type the IP Address for your primary server.
3. If desired, type an IP Address for a secondary server.

   Note: If DHCP is configured, WINS IP Addresses are overridden.

4. Click **Apply** to save the new settings or **Undo** to retain the previous settings.

LPR/LPD

1. The Line Printer Daemon (LPD) and Line Printer Remote (LPR) protocols provide printer spooling and network print server functionality for UNIX-based systems, such as HP-UX, Linux, and Macintosh.In CentreWare Internet Services, click **Properties** > **Connectivity** > **Protocols**.
2. Click **LPR/LPD**.
3. Under Protocol, select **Enable**.
4. Type an LPR/LPD Port Number or use the default port number of 515.
5. Under Advanced Settings, select **Enabled** to allow PDL Switching. This option allows the printer to process a single print job that contains two or more printer languages. An example is a PostScript print job with a PCL header.
6. Select **Enabled** to enable PDL banner page attributes override LPR control file attributes for job name and owner. This feature allows you to replace the standard information displayed on a banner page with the user name and job name from the print job.
7. Select the desired option from the Place temporary hold on which jobs drop-down menu. Options include:
   - **None (Use printer's default banner sheet job name if data file 1st)**: The printer does not wait to receive the job control information. This selection can cause banner page information to print incorrectly.
   - **Only those with data file received 1st**: The printer holds the job if the data file for the job is received first. This option ensures that the printer waits to receive the control file information to print banner page details correctly.
   - **All (consistent with older implementations)**: This option puts all jobs on hold. All data is received before a job begins printing. This setting can cause jobs to print slowly but results in accurate banner page information.
8. Click **Apply** to save the new settings or **Undo** to retain the previous settings.

Raw TCP/IP Printing

Raw TCP/IP is used to open a TCP socket-level connection over Port 9100, and stream a print-ready file to the printer input buffer. It then closes the connection either after sensing an End Of Job character in the PDL or after expiration of a preset timeout value. Port 9100 does not require an LPR request from the computer or the use of an LPD running on the printer. Raw TCP/IP printing is selected in Windows as the Standard TCP/IP port.

Configuring Raw TCP/IP Settings

1. In CentreWare Internet Services, click **Properties** > **Connectivity** > **Protocols**.
2. Click **Raw TCP/IP Printing**.
3. Select **Enabled** to enable the protocol.
4. Ensure that the TCP Port Number is set to **9100** for Port 1. If you want to emulate HP JetDirect EX Plus 3, set Port 2 to **9101** and Port 3 to **9102**.
5. Select **Enabled** for bidirectional communication.
6. Set the Maximum Connections per port between **1–32** for each port. The default port value is 32.
7. Set the End of Job Timeout to the desired number of seconds between **0–1800** before the job is processed with an End of Job character. The default time is 300 seconds.
8. Select **Enabled** for PDL Switching to allow the printer to switch automatically between multiple supported PDLs within a single job. PDL switching is normally disabled.
9. Click **Apply** to save the new settings or **Undo** to retain the previous settings.

   Click **Default All** to reset settings to default values.

   Note: Enable TCP/IP before enabling Raw TCP/IP printing.

Configuring Raw TCP/IP Advanced Settings

Use this page to set additional Raw TCP/IP Printing options for Ports 1, 2, and 3.

To configure Advanced Settings:

1. Under Connections, set the following:
   - Set the Maximum Connections per port between **1–32**. The default port value is 32.
   - To allow concurrent jobs to process for each port connection, type a number between **0–500** jobs in each port. Type **0** to allow unlimited concurrent jobs.
   - To limit the number of jobs that are active for each port connection, type a number between **0–32768**. Type **0** to allow unlimited number of active jobs.
2. Under Job Boundary Determination:
   - Type the End of Job Timeout between **0–1800** seconds to specify the amount of time to pass before a job processes with an End of Job character. The default time is 300 seconds. Type **0** to disable end of job detection by timeout.

3. Under Backchannel Data:
   - Enable **Backchannel Data Transmission to Client**, then, enable **Out of Order Backchannel Data** to allow data from several jobs to be interspersed.

   Note: Out of Order Backchannel Data is only available when Backchannel Data Transmission to Client is enabled.

4. Under Banner Page Printing:
   - To restrict banner pages to print for specific jobs only, select the job types from the Banner Page Enabled drop-down menu. Options are **First Job Only**, **No Jobs**, or **All Jobs**.
   - To enable banner pages to print before each PDL document within a single job, select **Enabled** for Banner Page for Each Document of Job.
   - To restrict banner pages to print for jobs that specifically request them through PJL, select **Enabled** for Banner Page for Job Containing only PJL Commands.
5. Miscellaneous
   - To allow the printer to switch between multiple PDLs within a single job, select **Enabled** for Language (PDL) Switching within PJL Job.
   - To force parsing of job data, select **Enabled** for Job Data Parsing Override.

   Note: Job data is not parsed when bidirectional communication and PDL switching are disabled.

6. Click **Apply** to save the new settings or **Undo** to retain the previous settings.
   Click **Default All** to reset settings to default values.

SMB Filing

You can specify Kerberos authentication options for features that file images to an SMB-shared network location.

Configuring Kerberos Authentication Options for SMB

1. In CentreWare Internet Services, click **Properties** > **Connectivity** > **Protocols**.
2. Under With Kerberos Tickets, for Workflow Scanning, Server Fax, and Scan to Home features, select an option:
   - **Always File with Kerberos Ticket**: The printer only attempts to use Kerberos authentication to the SMB shared network location. Configure Network Authentication or Smart Card Authentication using a Kerberos server.
   - **Prefer Filing with Kerberos Ticket**: The printer authenticates to the SMB shared network location with a Kerberos ticket if available. If a Kerberos ticket is not available, or Kerberos authentication fails, the printer attempts to authenticate using other methods, such as NT, or NTLM.
   - **Do Not File with Kerberos Ticket**: The printer attempts to authenticate to the SMB shared network location using other methods, such as NT, or NTLM. Do not select this option when Smart Card authentication is enabled. If you select this option when Smart Card authentication is enabled, SMB file transmission fails, and an error message appears on the touch screen.
3. Under WIthout Kerberos Tickets, features that use SMB, but cannot use Kerberos authentication are listed. Click the link under the feature name to navigate to the configuration page for that feature. Disable these features or configure them to use a protocol other than SMB for FIPS 140 compliance.
4. Click **Apply**.

SMTP Server

Simple Mail Transfer Protocol (SMTP) is an Internet standard used to transmit email across IP networks. Your printer uses SMTP to transmit scanned images and Internet Fax jobs through email.

Configuring SMTP Settings

1. In CentreWare Internet Services, click **Properties** > **Connectivity** > **Protocols**.
2. Click **SMTP (Email)**.
3. Under Required Information, select the desired method to locate an SMTP server.
   - Select **Use DNS to identify SMTP Server** to allow DNS automatically to find an SMTP server on the network.
   - Select **Specify SMTP Server manually** to map to a specific SMTP server.

   Note: If you select Use DNS to identify SMTP Server, ensure that DNS is configured for either IPv4 or IPv6 before you define the SMTP server.
4. Select the address type. Options include **IPv4**, **IPv6**, or **Host Name**.
5. Type the appropriately formatted address and port number. The default port number is 25.
6. Type the email address assigned to the printer by the SMTP server in the multifunction device Email Address field.
7. Click **Apply** to save the new settings or **Undo** to retain the previous settings.

Configuring SMTP Settings Optional Information

1. To define a maximum message size for messages with attachments, type a value between **512–20480** KB in the Maximum Message Size field. The default size is 10240 KB.
2. To improve transmission speed, set messages to fragment between **2–500** times. The default value for Number of Fragments is 1.
3. To set a maximum job size, type a value between **512–2000000** KB in the Total Job Size field.
4. If you selected more than 1 fragment in Number of Fragments, you can select how the email jobs are split for Email Job Splitting Boundary. Select:
   - **Page Boundary** to instruct mail client not to reassemble the job on receipt.
   - **Automatic Boundary** to instruct the mail client to reassemble the job on receipt.

5. Under Login Credentials for the multifunction device, select **System**. This option instructs the printer to authenticate itself using the Login Name and Password configured on this page. Select **None** to instruct the printer not to provide authentication credentials to the SMTP server.
6. If you select System, type the Login Name and Password used to access the server.
7. Enable **Select to save new password** to update the password for an existing Login Name.
8. If authentication is enabled, and Tools and Feature Access is configured to require users to log in before accessing email, select **Authenticated User** under Login Credentials for the Walkup User. You can also allow this field to default to the same setting that you selected for sending automated emails.
9. Click **Apply** to save the new settings or **Undo** to retain the previous settings.

LDAP

This section includes:

Lightweight Directory Access Protocol (LDAP) is a protocol used to process queries and updates to an LDAP information directory, on an external server. LDAP can also be used for network authentication and authorization. LDAP directories are heavily optimized for read performance. Use this page to define how the printer retrieves user information from an LDAP directory.

The LDAP Server page displays the current LDAP servers configured for your printer. You can configure a maximum of nine LDAP servers for your printer.

1. In CentreWare Internet Services, click **Properties** > **Connectivity** > **Protocols**.
2. Click **LDAP**.
3. To add a new LDAP server, click **Add New**.
4. To edit an LDAP server, click **Edit** next to the server you want to edit.
5. To copy an LDAP Server configuration, click **Copy From**.
6. To delete all LDAP servers configured, click **Delete All**.

Configuring LDAP Servers

1. In CentreWare Internet Services, click **Properties** > **Connectivity** > **Protocols**.
2. Click **LDAP**.
3. To add a new server, click **Add New Server**. To edit existing LDAP server settings, select the server and click **Edit**.
4. Under Server Information, select the preferred address type. Options are **IPv4**, **IPv6**, or **Host Name**.
5. Type a Friendly Name for the LDAP Server.
6. Type the appropriately formatted address and port number. The default port number is 389.
7. Select the LDAP server type from the LDAP Server menu.

Configuring LDAP Server Optional Information

1. Type the search directory root path in the Search Directory Root field using Base DN format.

   For more detail on Base DN formatting, refer to the *RFC 2849 - LDAP Data Interchange Format (LDIF) Technical Specification* on the IETF website.

2. Specify the login credentials required to access the LDAP directory. Options are:
   - **None**: The server does not require the printer to provide a user name or password.
   - **Authenticated User**: The printer uses the user name and password of the authenticated user to access the server.
   - **System**: The printer uses the information provided in the Login Name and Password fields to access the server.
3. If needed, type the Login Name and Password after you select the Login Credential type.
4. Retype the password and select **Save Password**, if needed.
5. If SSL is desired, select **Enable SSL** under SSL.
   a. Select Validate Repository SSL Certificate to allow the printer to validate certificates.
   b. Under Trusted SSL Certificates, select the certificate you want to use.
   c. To view the selected certificate details, or save the certificate to your computer, click **View/Save**.

   Note: If the LDAP Server has encryption enabled, a certificate issued from the LDAP server certificate authority must be installed on the printer.

6. Under Maximum Number of Search Results, type a number between **5–100** for the maximum number of addresses returned that match search criteria. The default number is 25. You can also type the LDAP server maximum.
7. Under Search Timeout, select **Use LDAP Server Timeout** to allow the printer use the LDAP server current settings. To specify a time, select **Wait**, and type the number of seconds between **5–100** that the printer waits before timing out. The default is 30 seconds.

   Note: If you are having trouble retrieving results from your LDAP server, use the Wait option.

8. If your primary LDAP server is connected to additional servers, select **LDAP Referrals** to include those LDAP servers in your searches.
9. Under the Perform Query on heading, select:
   - **Surname and Given Name Fields** to instruct the printer to query the configured surname and given name fields.
   - **Mapped Name Field** to instruct the printer to query the configured name field. allows you to specify how the name fields are mapped. After you apply this setting, click **User Mappings** to define the field mapping.
10. Click **Apply** to save the new settings or **Undo** to retain the previous settings.

Configuring LDAP Contexts

Contexts are a defined starting points in an LDAP database from which the search function begins searching. Contexts are used with the Authentication feature. You can configure the printer automatically to add an authentication context to the Login Name provided by the user.

Note: Contexts are only used if you configure LDAP server settings and select NDS as the server type.

Configuring Contexts for LDAP

1. In CentreWare Internet Services, click **Properties** > **Connectivity** > **Protocols**.
2. Click **LDAP**.
3. Click **Contexts** at the top of the LDAP Server page.
4. Type details in the Default Login Context field.
5. Click **Apply** to save the new settings or **Undo** to retain the previous settings.

Configuring LDAP User Mappings

LDAP servers display different results depending on how they implement mappings. Use this page to map LDAP fields to fields on your printer. Editing current map settings allows you to fine-tune server search results.

Defining User Mappings

1. Click **User Mappings** at the top of the LDAP Server page.
2. Under Search, type the user name you want to search for in the Enter Name field, then click **Search**.

   If a match occurs, the user information displays.
3. Click the drop-down menu under Imported Heading to remap fields as needed. The schema on the LDAP server defines the headings.

   Note: Internet Fax users must ensure that the Internet Fax field is not set to **No Mappings Available** in the drop-down menu. This setting prevents the Network Address Book from displaying on the Internet Fax screen on the printer control panel. If your LDAP server does not contain a unique Internet Fax address field, it can be set to match the heading for email address.

Configuring LDAP Authorization Access

If you have specified Remote Authorization as the authentication type, you can use LDAP user groups to control access to printer services and features. Access group names are defined in the LDAP server. For example, the LDAP server can contain a group of users called Admin. You can configure the Admin group on the printer so that only members of this group have administrator access to the printer. When a user belonging to the group Admin logs in to the printer, the printer performs an LDAP directory look-up to verify the user. Once authenticated, the user is allowed administrative rights to the printer.

> Note: User groups can only be configured for the first LDAP server in the list. All other servers use the same Authorization Access settings.

Configuring User Roles Access

You can assign users to specific roles groups to allow them types of access.

1. Click **Authorization Access** at the top of the LDAP Server page.
2. On the Authorization Access page, click the **User Roles** tab.
3. In the System Administrator Access field, type the name of an LDAP server group to use to grant system administrator access to the printer.
4. In the Accounting Administrator Access field, type the name of the LDAP server group to use to grant accounting administrator access to the printer.
5. Click **Apply**.
6. To verify if a user has access to either role, type the user name in the Enter User Name field, then click **Test**.

   If the pathway is locked and if the user is a member of the LDAP group, the group appears next to the user name. If the user is not a member of the group, No Access appears.
7. When completed, click **Close**.

Configuring Device Access

1. Click **Authorization Access** at the top of the LDAP Server page.
2. On the Authorization Access page, click the **Device Access** tab.
3. In the Services Pathway field, type the name of an LDAP server group to use to allow access to printer services and features.
4. Repeat the process for Job Status Pathway and Machine Status Pathway.
5. Click **Apply**.
6. To verify if a user has access to either role, type the user name in the Enter User Name field, then click **Test**.

   If the pathway is locked and if the user is a member of the LDAP group, the group appears next to the user name. If the user is not a member of the group, No Access appears.
7. Click **Close**.

   Note: Device or Service Access setup requires that Authentication is configured and Tools and Feature Access are configured to require users to log in before accessing services.

Configuring Services Access

You can specify access to the services of the printer under Service Access. Type the names of the LDAP groups for any of the services listed.

1. Click **Authorization Access** at the top of the LDAP Server page.
2. On the Authorization Access page, click the **Service Access** tab.
3. Under Access Group, type the names of the LDAP groups allowed access to each of the individual printer services.
4. Click **Apply**.
5. To verify if a user has access to either role, type the user name in the Enter User Name field, then click **Test**.
6. If the pathway is locked and if the user is a member of the LDAP group, the group appears next to the user name. If the user is not a member of the group, No Access appears.
7. When completed, click **Close**.

   Note: Device or Service Access setup requires that Authentication is configured and Tools and Feature Access are configured to require users to log in before accessing services.

Configuring Feature Access

You can set access rights to selected features on your printer using the Feature Access tab.

1. Click **Authorization Access** at the top of the LDAP Server page.
2. Click the **Feature Access** tab.
3. For each on the printer, type the name of the LDAP group allowed to access the feature.
4. Click **Apply**.
5. To verify if a user has access to either role, type the user name in the Enter User Name field, then click **Test**.

   If the pathway is locked and if the user is a member of the LDAP group, the group appears next to the user name. If the user is not a member of the group, No Access appears.
6. When completed, click **Close**.

   Note: Device or Service Access setup requires that Authentication is configured and Tools and Feature Access are configured to require users to log in before accessing services.

Configuring LDAP Custom Filters

You can edit Custom Filters so that text strings typed at the control panel are changed to match the format required by the LDAP server.

There are three types of filters that you can customize:

- **LDAP Authentication Filter**: Add text to the beginning of a User ID, or the Login Name configured as the System Login Name for the Server.
- **Email Address Book Filter**: Customize the standard filter that is used when a user types a name to search in the Network Address Book.
- **User ID Query Filter**: Customize the standard filter that the printer uses when searching for the name of the logged in user. For example, when Remote Authorization is configured, and a user logs in at the control panel, the printer searches the authorization server using this filter. The standard filter looks in the field mapped as the Login Name field. If you are using an ADS LDAP server, this

field is typically sAMAccountName. Do not use wildcard characters if you want a search for a specific person to return an exact match.

Configuring Custom Filters

1. Click **Custom Filters** at the top of the LDAP Server page.
2. To configure an LDAP Authentication filter, under LDAP Authentication, select **Prepend Domain Name**. This setting prepends the base DN to a user Relative Distinguished Name (RDN) when authenticating the user. Use the Common Name (CN) attribute to specify USERID in the base DN.

   Notes:

   - If Authenticated User is selected for Login Credentials to Access LDAP Server, some UNIX/Linux LDAP servers can require setting the Prepend Domain Name attribute.
   - For more detail on Base DN formatting, refer to the *RFC 2849 - LDAP Data Interchange Format (LDIF) Technical Specification* on the IETF website.
3. To configure an LDAP Authentication filter, under Email Address Book Filter, select **Enable Custom Filter**.
4. Type the LDAP search string or filter that you want to apply in the field. The filter defines a series of conditions that the LDAP search must fulfill to return the desired information. For example, to find people only, type **(ObjectClass=Person)&(cn=LDAP*)**.
5. To configure an LDAP Authentication filter, under User ID Query Filter, select **Enable Custom Filter**.
6. Type the LDAP search string or filter that you want to apply, where LDAP represents the string provided for the query. The filter defines a series of conditions that the LDAP search must fulfill to return the desired information. For example, to find the user with an sAMAccountName of Bob, type **(objectClass=user) (sAMAccountName=Bob)**.
7. Click **Apply** to save the new settings or **Undo** to retain the previous settings.

HTTP

Hypertext Transfer Protocol (HTTP) is a request-response standard protocol between clients and servers. Clients that make HTTP requests are called User Agents (UAs). Servers that respond to these requests for resources, such as HTML pages, are called Origin Servers. There can be any number of intermediaries, such as tunnels, proxies, or gateways between User Agents and Origin Servers.

Enabling HTTP at the Control Panel

1. At the printer control panel, press the **Machine Status** button, then touch the **Tools** tab.
2. Touch **Network Settings** > **Advanced Settings**.
3. Touch **Continue**.
4. Touch **HTTP Settings**.
5. Touch **Enable**, then touch **Save**.

Configuring HTTP Settings in CentreWare Internet Services

1. In CentreWare Internet Services, click **Properties** > **Connectivity** > **Protocols**.
2. Click **HTTP**.
3. Under Configuration, select **Enabled** to enable the protocol.
4. Change the HTTP Port Number if needed. The default is 80.
5. In Keep Alive Timeout, type the time between **1–60** seconds that the printer waits for a response from a connected user before terminating the connection. The default time is 15 seconds.

   Note: Increasing the Keep Alive Timeout can cause connections to slow down.

6. To encrypt HTTP communication using SSL, under Secure HTTPS, select **Enabled**. When SSL is enabled, all Web pages contain https:// in the URL.
   a. From the Choose Device Certificate menu, select the Device Certificate to use for SSL.
   b. To view the selected certificate details, or save the certificate to your computer, click **View/Save**.
   c. If you are using the Default Xerox® Device Certificate, you can install the Generic Xerox® Trusted CA Certificate in your Web browser. Installing the Generic Xerox® Trusted CA Certificate ensures that your browser trusts the printer. To download the certificate, click **Download the Generic Xerox Trusted CA Certificate**.
7. If necessary, change the Secure HTTP Port Number. The default is 443.
8. Click **Apply** to save the new settings or **Undo** to retain the previous settings.
9. Click **Default All** to reset settings to default values.

HTTP Web Services

This page provides a list of all available Web services on your printer and displays their configuration status.

Services are grouped into the following categories:

- Device Discovery
- Print Services
- Scan Services
- Job Management
- Security
- Remote System Management

Selecting Web Services for HTTP

1. To enable or disable individual services, select the check box next to one or more services. To enable or disable all services at one time, click **Enable All** or **Disable All**.
2. If additional settings are required for a selected service, the status column indicates the required update and a **Settings** button appears. Click **Settings** to configure the service.
3. Click **Apply** to save the new settings or **Undo** to retain the previous settings.

HTTP Advanced Settings

The Advanced Web Services page displays all services currently enabled on the printer and their port numbers.

To remove all login restrictions for web services on the printer, under Web Services IP Lockout, click **Clear Lockout**.

POP3

Post Office Protocol, version 3 (POP3) is a protocol that allows email clients to retrieve email from remote servers over TCP/IP on network port 110. This printer uses POP3 for the Internet Fax and email features to retrieve fax jobs over email. POP3 is not compatible with IPv6.

1. In CentreWare Internet Services, click **Properties** > **Connectivity** > **Protocols**.
2. Click **POP3 Setup**.
3. Under Server Information, select either **IPv4** or **Host Name** for the address type.
4. Under POP3 Server, type the appropriately formatted address and port number. The default port number is 110.
5. Type the Login Name assigned to the printer used to log in to the POP3 server.
6. Type then retype an alphanumeric Password.
7. Enable **Select to save new password**.
8. Under POP3 Settings, select **Enable receipt of Email via POP3**.
9. Type a Polling Interval value between **1–60** minutes. The default value is 15 minutes.
10. Click **Apply** to save the new settings or **Undo** to retain the previous settings.

Proxy Server

A proxy server acts as a go-between for clients seeking services and servers that provide them. The proxy server filters client requests and if the requests meet the proxy server filtering rules, it grants the request and allows the connection.

A proxy server has two main purposes:

- To keep any devices behind it anonymous for security purposes.
- To cache content from resources, such as Web pages from a Web server, to increase resource access time.

Configuring the Proxy Server

1. In CentreWare Internet Services, click **Properties** > **Connectivity** > **Protocols**.
2. Click **Proxy Server**.
3. Under HTTP Proxy Server, select **Enabled**.
4. Select the Proxy Server address type. Options are **IPv4 Address**, **IPv6 Address**, or **Host Name**.
5. Type the appropriately formatted address and port number. The default port number is 8080.
6. Click **Apply** to save the new settings or **Undo** to retain the previous settings.

NTP

The Network Time Protocol (NTP) synchronizes the internal clocks of computers over a network connection at system startup and every subsequent 24-hour period thereafter. If your printer uses DHCP and an NTP server, or if a DHCP server provides Greenwich Mean Time (GMT) offset, these settings are ignored.

1. In CentreWare Internet Services, click **Properties** > **Connectivity** > **Protocols**.
2. Click **NTP**.
3. Under Network Time Protocol, select **Enabled** to enable the protocol.
4. Select the address type. Options are **IPv4 Address** or **Host Name**.
5. Type the appropriately formatted address and port numbers for IP Address: Port and Alternate IP Address: Port. The default port number is 123.
6. Click **Apply** to save the new settings or **Undo** to retain the previous settings.

   Note: Restart your printer for the new settings to take effect.

WSD

Web Services for Devices (WSD) is technology from Microsoft that provides a standard method for discovering and using network connected devices. It is supported in Windows Vista and Windows Server 2008 operating systems. WSD is one of several supported communication protocols.

Enabling WSD

1. In CentreWare Internet Services, click **Properties** > **Connectivity** > **Protocols**.
2. Click **WSD**.
3. Under WSD Services, select **Enabled**.

Sleep Mode Network Settings

You can allow the printer to poll Novell print queues and broadcast Service Advertising Protocol (SAP) during sleep mode.

Configuring Sleep Mode Settings

1. In CentreWare Internet Services, click **Properties** > **General Setup**.
2. Click **Sleep Mode Settings**.
3. To allow the printer to poll Novell print queues, select **Resume Network Controller Briefly to Poll Novell Print Queues During Sleep Mode**.
4. Type the time in seconds to define the interval the printer uses to come out of Sleep Mode.
5. To allow the printer to broadcast SAP during sleep mode, select **Resume Network Controller Briefly to Broadcast Service Advertising Protocol (SAP) During Sleep Mode**.
6. Type the time in seconds to define the interval the printer uses to come out of Sleep Mode.
7. Click **Apply** to save the new settings or **Undo** to retain the previous settings.

See also:

NetWare on page 23.

Sleep Mode Network Settings Advanced

You can allow the printer to respond to four types of broadcast packets during sleep mode.

Notes:

- Some printers do not support this function.
- If the printer is using an IPv6 Link-Local address, enabling the IPv6 ND multicast filter brings the printer out of sleep mode.

Configuring Advanced Sleep Mode Settings

1. In CentreWare Internet Services, click **Properties** > **General Setup**.
2. Click **Sleep Mode Settings** > **Advanced Settings**.
3. In the Packet Priority list, click the **Increase Priority** and **Decrease Priority** buttons to prioritize the packet types.
4. Click **Apply** to save the priority list.

   The printer processes the list and displays the top four packet types if the corresponding protocols have been enabled. Packet types that do not have the corresponding protocol enabled are skipped.
5. Click **Return** to return to the Sleep Mode Settings page.

Security

4

This chapter includes:

See also:

www.xerox.com/security

Setting Up Access Rights

This section includes:

You can control access to services and features by setting up authentication and authorization. Personalization allows the printer to retrieve user information to customize features.

Authentication

Authentication is the process of confirming the identity of a user. When authentication is enabled, the printer compares the information that a user provides to another source of information, such as an LDAP directory. Users can be authenticated when accessing the control panel or when accessing CentreWare Internet Services.

There are several ways to authenticate a user:

- **Local**: When local authentication is configured, users log in at the control panel. The printer compares the user credentials to the information stored in the User Information Database. Use this authentication method if you have a limited number of users, or do not have access to an authentication server.
- **Network**: When network authentication is configured, users log in at the control panel. The printer compares the user credentials to the information stored on an authentication server.

  The printer can use one of the following protocols to communicate with your authentication server:

  - **Kerberos (Solaris)**
  - **Kerberos (Windows 2000/2003)**
  - **NDS**
  - **SMB (Windows 2000/2003)**
  - **LDAP**
- **Card Reader**:
  - When Xerox® Secure Access authentication is configured, users swipe a pre-programmed identification card at the control panel. The printer compares the user credentials to the information stored on the Xerox® Secure Access server. To use Xerox® Secure Access, purchase and install the Xerox Secure Access Unified ID System®.
  - When Smart Card authentication is configured, users swipe a pre-programmed identification card at the control panel. Purchase and install a Smart Card reading system before configuring Smart Card authentication.

Authorization

Authorization is the process of defining the features that users are allowed to access. For example, you can configure the printer to allow a user to copy, scan, and fax, but not email.

There are two types of authorization:

- **Local**: User login information is stored on the printer in the User Information Database.
- **Network**: User login information is stored externally in a network database, such as an LDAP directory.

Personalization

Personalization is the process of customizing services for a specific user. The printer searches an LDAP directory for the home directory and email address of a user when using Scan to Home, or Email Scanning features.

Local Authentication

When local authentication is configured, users log in at the control panel. The printer compares the user credentials to the information stored in the User Information Database. Use this authentication method if you have a limited number of users, or do not have access to an authentication server.

Setting up Local Authentication

1. In CentreWare Internet Services, click **Properties** > **Security** > **Authentication**.
2. Click **Edit**.
3. Under **Authentication method on the machine's touch interface**, select **User Name / Password Validated Locally on the Xerox Machine**.
4. Under Authorization information is stored, select **Locally on the Xerox Machine (Internal Database)**.
5. Enable personalization if you want to allow the printer to retrieve user information, such as email address or home directory, from an LDAP server. Select the check box next to **Automatically retrieve the following information for the authenticated user from LDAP**.

   Note: LDAP settings must be configured to use personalization.

6. Click **Save** to apply the new settings or **Undo** to retain the previous settings.
   Click **Cancel** to return to the previous page.

User Information

The User Information Database stores user credential information for Local Authentication.

Adding User Information to the Local Database

1. In CentreWare Internet Services, click **Properties** > **Security** > **User Information Database**.
2. Click **Setup**.
3. Click **Add New User**.
4. Type the User Name and Friendly Name of the user. Type a Password then retype the Password to verify.

   Note: If the authentication method is not set to Local Authentication, the Password field is not editable.

5. Select a User Role:
   - **System Administrator**: Users in this role are allowed to access all services and settings.
   - **Accounting Administrator**: Users in this role are allowed to access accounting settings and other services and settings that are locked.
   - **Non-Authenticated User**: Users who are not authenticated can only access features as specified in the Non-Authenticated User role.

   If you have created any user roles, they also appear in the list.
6. Click **Save** to apply the new settings or **Cancel** to return to the previous screen.

Editing User Information

1. On the **User Information Database** page, click **Edit** next to a user name to edit information about the user.
2. Update the user information.
3. Click **Save**.

Specifying Password Requirements

1. In CentreWare Internet Services, click **Properties** > **Security** > **User Information Database**.
2. Click **Password Settings**.
3. Specify the password Minimum Length and Maximum Length.
4. Select rules as desired:
   - **Cannot contain Friendly Name**
   - **Cannot contain User Name**
   - **Must contain at least 1 number**
5. Click **Apply** to save the new settings or **Undo** to retain the previous settings.

   Note: New password rules do not affect existing passwords.

Specifying Job Override Policies

Use Job Override Policies to specify what happens when a user without appropriate print permissions sends a color or 1-sided print job to the printer.

1. In CentreWare Internet Services, click **Properties** > **Security** > **Authentication**.
2. Click **Job Override Policies**.
3. Under Color Printing, select **Print Job in Black & White**, or **Delete Job**. If an unauthorized user sends a color job, the job prints in black and white, or is deleted.
4. Under 1-Sided Printing, select **Print Job 2-Sided**, or **Delete Job**. If an unauthorized user sends a 1-sided job, the job prints 2-sided, or is deleted.

Controlling Access to Tools and Features

1. In CentreWare Internet Services, click **Properties** > **Security** > **Authentication**.
2. Click **Tools & Feature Access**.
3. Under Presets, select:
   - **Standard Access** to restrict access to the Tools tab at the control panel.
   - **Open Access** to allow all users, including non-authenticated users, to access all tools and features in CentreWare Internet Services and at the control panel.
   - **Custom Access** to lock, unlock, or hide tools and features for all users.
4. If you selected Custom Access, select **Locked** or **Unlocked**.
5. Select **Hidden** to hide a service icon from the touch screen of the printer until an authorized user logs in.
6. Click **Apply** to save the new settings or **Undo** to retain the previous settings.

User Permissions

Print permissions are rules that allow you to control printing times and methods for a group of users. You can:

- Restrict color printing, requiring users to print in black and white.
- Restrict 1-sided printing, requiring users to print 2-sided.
- Restrict a Job Type, such as Secure Print.
- Restrict access to specific paper trays.
- Specify the software applications from which users are allowed to print.
- Restrict printing, color printing, and 1-sided printing from specific software applications.

Note: Users can see a list of restricted print methods in the print driver. If a user attempts to print at a restricted time or using a restricted method, the printer does not process the job. The printer sends a message to the user informing them why the job did not print.

User Roles

A role is a set of permissions associated with a group of users. To edit permissions for a group of users, you edit permissions for a role. There are two types of roles:

- **Non-Authenticated Users Role**: The Non-Authenticated Users role applies to any user who accesses the printer, but does not provide authentication credentials. This role also applies to anyone who sends a job that is not associated with a user name or Job Owner. Examples are a job sent using LPR, or a job sent from a mainframe application.

- **Authenticated Users Role**: All roles that you create apply to authenticated users only. You can assign users from the User Information Database to the role, or you can create a role that applies to all authenticated users.

Editing the Role for Non-Authenticated Users

1. In CentreWare Internet Services, click **Properties** > **Security** > **Authentication**.
2. Click **User Permissions**.
3. Click the **Non-Authenticated Users** tab.
4. Under Actions, click **Edit**.
5. On the Manage User Permissions page, under Actions, click **Edit** next to the print settings that you want to restrict.
6. A page opens, allowing you to edit settings for one of the following print permission types:

Setting Black and White and Color Print Permissions

1. On the When Users Can Print page, select:
   - **Always** to allow printing at all times.
   - **Monday - Friday from** to allow printing on weekdays. Select when users are allowed to print from the From Time and To Time menus.
   - **Time of Day (Advanced)** to allow printing on specific days during a specific time range. Select the From Time and To Time, and click **Add Time Range** next to the day. Click the trash can icon to delete.
   - **Never** to restrict printing at all times.
2. Select **Make color printing more restrictive than black & white** printing to specify permissions for Color and Black & White printing independently.
3. Click **Save**.

Setting 1-Sided Print Permissions

1. On the 1-Sided Printing page, under Role State, select **Not Allowed** to require users to print 2-sided.
2. Click **Save**.

Setting Job Type Print Permissions

1. On the Job Types page, under Presets, select one of the following options:
   - **Allow all Job Types** allows users to print any job type.
   - **Only Allow Secure Print** ensures that users only send Secure Print jobs.
   - **Custom** allows you to select the job types that users are allowed to send.
2. If you selected Custom, under Role State, next to each job type, select **Not Allowed** to restrict users from using the job type.
3. Click the **Lock** icon to lock all job types or click the **Unlock** icon to unlock all job types.
4. Click **Save**.

Setting Paper Tray Print Permissions

1. On the Paper Trays page, under Role State, next to each tray, select **Not Allowed** to restrict users from using the tray.
2. Click the **Lock** icon to lock all trays or click the **Unlock** icon to unlock all trays.
3. Click **Save**.

Setting Application Print Permissions

1. On the Applications page, click **Add New Application**.
2. Under Application List, select an application.
3. Under Role State, next to Printing, Color Printing, or 1-Sided Printing, select **Not Allowed** to restrict users from using the printing method.
4. Click **Save** to apply the new settings or **Cancel** to return to the previous screen.

Managing the List of Applications

Application Manager allows you to associate Application IDs with an Application Group. Application Group Names for common application types appear in the table at the bottom of the Application Manager page. The associated Application IDs appear next to each of the Application Group Names. An Application ID identifies the application from which the job was sent. To control print permissions for an application, the Application ID of the application must be associated with an Application Group Name. If you send a job from an application that is not in the default list, a new Application ID appears in the Custom Application ID list.

1. On the Applications page, click **Application Manager**.
2. To associate a custom Application ID with an existing Application Group, under Actions, click **Merge With**.
   a. Under Merge With the Application Group, select an application from the menu.
   b. Click **Save**.
3. To create a new Application Group, under Actions, click **Make This A Group**.
   a. Under Application Group Name, type a name for the group.
   b. Click **Save**.
4. To delete a custom Application ID, under Actions, click **Delete**.
5. To delete or disassociate a custom Application ID from an Application Group Name, under Actions, click **Manage** next to an Application Group Name.
   a. Click **Un-Merge** to disassociate the Application ID, or click **Delete** to delete the Application ID.
   b. Click **Close**.
6. To create a custom Application ID, click **Add Manually**.
   a. Under Application ID, type an Application ID.
   b. Click **Save**.
7. Click **Close** to return to the Applications page.

Creating Authenticated User Roles

To edit permissions for a specific group of users, you must first create a role.

1. In CentreWare Internet Services, click **Properties** > **Security** > **Authentication**.
2. Click **User Permissions**.
3. Click the **Authenticated Users** tab.
4. Click **Make Your Own Permission Roles** or **Add New Role**.
5. Type a name and description for the role.
6. Click **View Quick Setup Options**, and select from the following options:
   - **Remove all color printing restrictions**
   - **Start editing role with no restrictions**

   If you do not select any of these options, Print permissions are set to Allowed.
7. Click **Create**. The Assign Users to Role page appears.
8. Configure permissions and assign users to the role, or click **Save** to edit the role later.

Editing an Authenticated User Role

1. In CentreWare Internet Services, click **Properties** > **Security** > **Authentication**.
2. Click **User Permissions**.
3. Click the **Authenticated Users** tab.
4. Under Actions, click **Edit** next to a role.

   Note: You cannot edit permissions for the System Administrator or Accounting Administrator roles. Users assigned to the System Administrator Role can access all features of the printer. Users assigned to the Accounting Administrator Role can only access accounting features.
5. On the Manage User Permissions page, click **Print**.
6. Under Actions, click **Edit** next to the print settings that you want to restrict. For details, see Editing the Role for Non-Authenticated Users on page 62.

Assigning Users to a Role

If you add user information to the User Information Database and create a role, you can assign users to the role.

1. In CentreWare Internet Services, click **Properties** > **Security** > **Authentication**.
2. Click **User Permissions**.
3. Click the **Authenticated Users** tab.
4. Click **Edit** next to a role.
5. Under Methods, select one of the following options:
   - **Select Individual Users**: At the bottom of the page, select the users that you want to assign to the role.
   - **All Authenticated Users**: All users are assigned to the role.
   - **Exceptions**: At the bottom of the page, select the users that you want to remove from the role. All other users are assigned to the role.
6. Click **Save**.

Troubleshooting Conflicting Permissions

1. In CentreWare Internet Services, click **Properties** > **Security** > **Authentication**.
2. Click **Troubleshooting**.
3. Click **Permission Summary** next to a user name to see a summary of permissions for that user.

Temporarily Disabling Print Permissions for all Users

1. On the Troubleshooting page, click **Permission Enablement Options**.
2. Click **Disable Print Restrictions** to disable print restrictions for all users.
3. Click **Enable Print Restrictions** to enable print restrictions.

Network Authentication

When network authentication is configured, users log in at the control panel. The printer compares the user credentials to the information stored on an authentication server.

Setting up Network Authentication

1. In CentreWare Internet Services, click **Properties** > **Security** > **Authentication**.
2. Click **Setup**.
3. Click **Edit**.
4. Under **Authentication method on the machine's touch interface**, select **User Name/Password Validated Remotely on the Network**.
5. Under Authorization information is stored, select **Remotely on the Network**.
6. Enable personalization if you want to allow the printer to retrieve user information, such as email address or home directory, from an LDAP server. Select the check box next to **Automatically retrieve the following information for the authenticated user from LDAP**.

   Note: LDAP settings must be configured to use personalization.

7. Click **Save** to apply the new settings or **Undo** to retain the previous settings.

   Click **Cancel** to return to the previous page.

Configuring Authentication Server Settings for Kerberos (Solaris)

1. On the Xerox® Access Setup page, click **Edit** next to Authentication Servers.
2. Under Authentication Type, select **Kerberos (Solaris)**.
3. Click **Add New**.
4. Under Server Information, in the Realm field, type the realm for your authentication server.
5. Select the desired address type. Options are **IPv4 Address**, **IPv6 Address**, or **Host Name**.
6. Type the appropriately formatted address and port numbers for both the primary and backup addresses. The default port number is 88.

   Note: A backup address is optional.

7. If you want to use an LDAP server for Network Authorization or Personalization:
   a. Click **Add LDAP Mapping**.
   b. Select the LDAP server from the list and click **Add Mapping**, or click **Add New** to add a new LDAP server.
8. Click **Save Server**.
9. To specify server settings for an alternate authentication server, click **Add New**.
10. To copy the settings from another server, select a server from the list and click **Copy From**.
11. Click **Edit** to update the settings.

Configuring Authentication Server Settings for Kerberos (Windows 2000/2003)

1. On the Xerox® Access Setup page, click **Edit** next to Authentication Servers.
2. Under Authentication Type, select **Kerberos (Windows 2000/2003)**.
3. Click **Add New**.
4. Under Server Information, in the Realm field, type the realm for your authentication server.
5. Select the desired address type. Options are **IPv4 Address**, **IPv6 Address**, or **Host Name**.
6. Type the appropriately formatted address and port numbers for both the primary and backup addresses. The default port number is 88.

   Note: A backup address is optional.

7. If you want to use an LDAP server for Network Authorization or Personalization:
   a. Click **Add LDAP Mapping**.
   b. Select the LDAP server from the list and click **Add Mapping**, or click **Add New** to add a new LDAP server.I
8. Click **Save Server**.
9. To specify server settings for an alternate authentication server, click **Add New**.
10. To copy the settings from another server, select a server from the list and click **Copy From**.
11. Click **Edit** to update the settings.

Configuring Authentication Server Settings for NDS (Novell)

Before you begin:

Enable and configure Netware settings. For details, see NetWare on page 23.

1. On the Xerox® Access Setup page, click **Edit** next to Authentication Servers.
2. Under Authentication Type, select **NDS (Novell)**.
3. Click **Add New**.
4. Under Default Tree/Context, type the details in the **Tree** and **Context** fields.
5. Click **Save Server**.
6. To specify server settings for an alternate authentication server, click **Add New**.
7. To copy the settings from another server, select a server from the list and click **Copy From**.
8. Click **Edit** to update the settings.

Configuring Authentication Server Settings for SMB

1. On the Xerox® Access Setup page, click **Edit** next to Authentication Servers.
2. Under Authentication Type, select **SMB (Windows NT 4)** or **SMB (Windows 2000/2003)**.
3. Click **Add New**.
4. Under Domain, type the domain name of your authentication server.
5. If you want to specify domain controller IP addresses or host names, select **Optional Information**. Address options appear.
6. Select the address type. Options are **IPv4 Address**, or **Host Name**.
7. Type the appropriately formatted address and port number. The default port number is 137.
8. Click **Save Server**.
9. To specify server settings for an alternate authentication server, click **Add New**.
10. To copy the settings from another server, select a server from the list and click **Copy From**.
11. Click **Edit** to update the settings.

Configuring Authentication Server Settings for LDAP

1. On the Xerox® Access Setup page, click **Edit** next to Authentication Servers.
2. Under Authentication Type, select **LDAP**.
3. Click **Add New**.
4. Configure LDAP server settings and click **Apply**.
5. To configure LDAP settings for a previously added LDAP server, click **Edit** next to the LDAP server in the list.

   A book icon appears in the list next to the LDAP server that is used for Network Address Book queries.
6. To specify server settings for an alternate authentication server, click **Add New**.
7. To copy the settings from another server, select a server from the list and click **Copy From**.
8. Click **Edit** to update the settings.

Network Authorization

When Remotely on the Network is selected as the authorization method, the printer references an authorization server for authorization information for the authenticated user.

Configuring Network Authorization

When Remotely on the Network is selected as the authorization method, the printer references an authorization server for authorization information for the authenticated user.

1. On the Xerox® Access Setup page, under Action, click **Edit** next to Authorization Server.
2. Under Authorization Configuration, select **SMB** or **LDAP**.
3. If you select LDAP, click the link under Configuration to go to the configuration page for LDAP Servers.
4. If you select SMB:
   a. Under Configuration, type the Default Domain.
   b. If you want to specify domain controller IP addresses or host names, select **Optional Information**.
   c. Select **IPv4** or **Host Name**.
   d. Type the appropriately formatted address and port number. The default port number is 137.
   e. Under Login Credentials to Access SMB Server, select an option:
      - **None**: The server does not require the printer to provide a user name or password.
      - **Authenticated User**: The printer uses the user name and password of the authenticated user to access the server.
      - **System**: The printer uses the information provided in the Login Name and Password fields to access the server.

   f. If you select System, type the Login Name and Password used to access the server. Retype the password to verify.
   g. Enable **Select to save new password** to update the password for an existing Login Name.
5. Configure settings on the User Roles, Device Access, Service Access, and Feature Access tabs.
6. Click **Apply** to save the new settings or **Undo** to retain the previous settings.

For more information about the User Roles, Device Access, Service Access, and Feature Access tabs, see Configuring LDAP Authorization Access on page 46.

Authentication Using a Card Reader System

When Xerox® Secure Access authentication is configured, users swipe a pre-programmed identification card at the control panel. The printer compares the user credentials to the information stored on the Xerox® Secure Access server. To use Xerox® Secure Access, purchase and install the Xerox Secure Access Unified ID System®.

When Smart Card authentication is configured, users swipe a pre-programmed identification card at the control panel. Purchase and install a Smart Card reading system before configuring Smart Card authentication.

Before you begin:

- Enable Secure HTTP (SSL). For details, see HTTP on page 50.
- Enable the Authentication & Authorization Configuration Web Service. For details, see HTTP on page 50.
- Format and configure identification cards.

- Connect your card reader to the USB port.
- If you are using Xerox® Secure Access, install the Xerox® Secure Access authentication server software and configure it with user accounts. Refer to the Xerox® Secure Access Unified ID System documentation for help.

  Note: Accounts created on the Xerox® Secure Access server must match accounts stored in the printer local database or in another network authentication server.

Setting Up Authentication for a Smart Card System

1. In CentreWare Internet Services, click **Properties** > **Security** > **Authentication**.
2. Click **Setup**.
3. Click **Edit**.
4. Under **Authentication method on the machine's touch interface**, select **Smart Cards**.
5. You can configure an alternate authentication method to allow users to access the printer without a smart card. Under **Alternate authentication method on the machine's touch interface**, select **User Name / Password Validated Remotely on the Network**.
6. Specify a method for the printer to authenticate users who access CentreWare Internet Services from their computer. Under **Authentication method on the machine's web user interface**, select **User Name / Password Validated Locally on the Xerox Machine** or **User Name / Password Validated Remotely on the Network**.
7. Under Authorization information is used, select **Locally on the Xerox Machine**, or **Remotely on the Network**.
8. Click **Save**.
9. Type the Feature Enablement Key that is included in the Common Access Card Enablement Kit, and click **Next**.
10. Click **Next** again. A list of configuration settings appears at the bottom of the Xerox® Access Setup page.
11. Click **Edit** to configure any settings that are marked in red text as Required; Not Configured.

Configuring Domain Controller Settings

1. On the Xerox® Access Setup page, under Action, click **Edit** next to Domain Controller(s). The domain certificate on a smart card of a user must be validated on the domain controller server before they can access the printer.
2. Click **Add Domain Controller**.
3. Under Domain Controller Type, select **Windows Based Domain Controller** if you are using one.
4. Type the domain controller server address information.
5. Click **Save** to apply the new settings or **Cancel** to return to the previous screen.
6. If you have added more that one domain controller server, you can prioritize the alternate servers. Click **Change Domain Priority**.
   a. On the Change Domain Priority page, select a domain controller in the list.
   b. Click the **Up Arrow** or **Down Arrow** to change the search priority of the server.
   c. Click **Close**.
7. To configure NTP settings, under Action, click **Edit** next to NTP. The domain controller time and the time set on the printer must be synchronized. Xerox recommends that you enable NTP to ensure time synchronization.
8. Click **Close** to return to the Xerox® Access Setup page.

Configuring OCSP Validation Server Settings

If you have an OCSP server, or an OCSP certificate validation service, you can configure the printer to validate certificates installed on the domain controller.

1. On the Xerox® Access Setup page, under Action, click **Edit** next to Certificate Validation.
2. Select a validation method and click **Next**.
3. On the Required Settings page, type the URL of the OCSP server.
4. To ensure that the printer can communicate with the OCSP server and the domain controller, configure your proxy server settings if necessary.
5. Click the appropriate link to install the root CA certificates for the OCSP server and your domain controller.
6. Click **Save** to apply the new settings and return to the Xerox® Access Setup page.
   Click **Cancel** to return to the Xerox® Access Setup page.

Setting the Inactive Time Limit

1. On the Xerox® Access Setup page, under Action, click **Edit** next to Smart Card Inactivity Timer.
2. Specify the maximum amount of time before a user is automatically logged out. Type the time in minutes.
3. Click **Save** to apply the new settings and return to the Xerox® Access Setup page.
   Click **Cancel** to return to the Xerox® Access Setup page.

Configuring Email Encryption and Signing Settings

1. On the Xerox® Access Setup page, under Action, click **Edit** next to Email Encryption/Signing.
2. To enable Email Encryption, under Email Encryption Enablement, select an option:
   - **Always On; Not editable by user**: Restrict users from turning Email Encryption on or off at the control panel.
   - **Editable by user**: Allow users to turn Email Encryption on or off at the control panel.

3. If you select Editable by user, select the default setting for users at the control panel. Under Email Encryption Default, select **On** or **Off**.
4. Under Encryption Algorithm, select one of the following encryption methods:
   - **3DES**
   - **AES128**
   - **AES192**
   - **AES256**
5. To enable Email Signing, under Email Signing Enablement, select an option:
   - **Always On; Not editable by user**: Restrict users from turning Email Signing on or off at the control panel.
   - **Editable by user**: Allow users to turn Email Signing on or off at the control panel.
6. If you select Editable by user, specify the default setting for users at the control panel. Under Email Signing Default, select **On** or **Off**.
7. Click **Save** to apply the new settings and return to the Xerox® Access Setup page.

   Click **Cancel** to return to the Xerox® Access Setup page.

Displaying Your Company Logo on the Blocking Screen

You can customize the blocking screen to display your company logo. The blocking screen appears on the printer touch screen when card reader authentication or an auxiliary accounting device is configured. The screen displays a message when a user attempts to access a restricted feature, reminding users to swipe an identification card to access the feature.

1. On the Xerox® Access Setup page, under Action, click **Edit** next to Import Customer Logo.
2. Click **Browse** or **Choose File**.
3. Select a **.png** file that is not larger than 300 x 200 pixels, and click **Open**.
4. Click **Import**.
5. Click **Reboot Machine**.

Setting Up Authentication for Xerox Secure Access

1. In CentreWare Internet Services, click **Properties** > **Security** > **Authentication**.
2. Click **Setup**.
3. Click **Edit**.
4. Under **Authentication method on the machine's touch interface**, select **Xerox® Secure Access Unified ID System**.
5. Under **Authentication method on the machine's web user interface**, specify a method for the printer to authenticate users who access CentreWare Internet Services from their computer.
   - If you select **User Name / Password Validated locally on the Xerox Machine (Internal Database)**, add user information to the User Information Database.
   - If you select **User Name / Password Validated Remotely on the Network**, configure a network authentication server.

6. Under Authorization, select **Locally on the Xerox Machine (Internal Database)**, or **Remotely on the Network**.
7. Click **Save**.

   A list of configuration settings appears at the bottom of the page.
8. Under Action, click **Edit** next to Xerox® Secure Access Setup.
9. Configure the remote server. Refer to the instructions provided with your server hardware.

   After the server is configured, it communicates with the printer and automatically completes the configuration process.
10. To configure communication manually, personalize instructional windows, and review accounting options, click **Manually Configure**.
11. Click **Pending Remote Server Setup** to return to the Xerox® Access Setup page.

    In the table at the bottom of the page, click **Edit** to configure any settings that are marked in red text as Required; Not Configured.

Manually Configuring Xerox® Secure Access Settings

If you are using Xerox® Secure Access for authentication, you can manually configure remote server communication, personalize instructional windows, or review accounting options.

Before you begin:

Configure the Xerox® Secure Access authentication server.

1. On the Xerox® Access Setup page, click **Edit** next to Xerox® Secure Access Setup.
2. Click **Manually Configure**.
3. Under Server Communication, select the address type and port number. Options are **IPv4 Address** or **Host name**.
4. Type the appropriately formatted address and port number. The default port number is 443.
5. In the Path field, type the HTTP path **public/dce/xeroxvalidation/convauth**.
6. Under Device Log In Methods, select an option:
   - **Xerox® Secure Access Device Only** allows users to access the printer only using the card reader.
   - **Xerox® Secure Access Device + alternate on-screen authentication method** allows users to access the printer by logging in at the control panel.
7. When Network Accounting is configured, the printer can obtain user accounting information from the Authentication server. Select **Automatically apply Accounting Codes from the server** to reduce the number of screens that appear when a user logs in at the control panel.

   If you want users to provide an accounting code at the control panel, select **User must manually enter accounting codes at the device**.
8. Create login instructions for users by typing text in the fields under Device Instructional Blocking Window.
   a. In the Window Title field, type text that appears as a title at the top of the touch screen.
   b. In the Instructional Text field, type instructions that appear below the title.

   Note: If the Title and Prompt are configured on the Xerox® Partner authentication server, then any instructional text that you type is ignored.

9. Click **Save** to apply the new settings or **Undo** to retain the previous settings.

Secure HTTP (SSL)

You can establish an HTTP Secure(HTTPS) connection to the printer by encrypting data sent over HTTP using SSL. You can also enable SSL encryption for the following features:

- Configuring the printer in CentreWare Internet Services
- Printing from CentreWare Internet Services
- Printing using IPP
- Managing scan templates
- Workflow Scanning
- Network accounting

Note: SSL encryption is protocol-independent. You can turn SSL on or off for each protocol or scan destination as needed.

Before you begin:

- Ensure DNS is enabled and configured.
- Ensure that the date and time configured on the printer is correct. The time that is set on the printer is used to set the start time for the Xerox® Device Certificate. A Xerox® Device Certificate is installed when you enable HTTP (SSL).

Enabling HTTPS (SSL)

1. In CentreWare Internet Services, click **Properties** > **Connectivity** > **Protocols**.
2. Click **HTTP**.
3. Under Secure HTTP (SSL), select **Enabled**.

Note: When Secure HTTP is enabled, all pages in CentreWare Internet Services contain https:// in the URL for the Web page.

FIPS 140-2

You can enable the printer to check the current configuration to ensure that transmitted and stored data is encrypted as specified in Government Standard FIPS 140-2 (Level 1). If FIPS 140-2 encryption is required, all computers, serves, browser software, security certificates, and applications must comply with the standard or operate in FIPS-compliant mode.

To allow the printer to use non-FIPS compliant protocols or features when FIPS 140 mode is enabled, acknowledge the notification of non-compliance during the validation process.

> Note: Enabling FIPS 140 Mode can prevent the printer from communicating with network devices that communicate using protocols that do not use FIPS-compliant encryption algorithms.

When non-FIPS compliant protocols, such as SNMPv3 or NetWare, are enabled after FIPS mode is enabled, a message appears indicating the protocols use non-FIPS compliant encryption algorithms.

When you enable FIPS-140 mode, the printer validates the current configuration by performing the following checks:

- Validates certificates for features where the printer is the server in the client-server relationship. An SSL certificate for HTTPS is an example.
- Validates certificates for features where the printer is the client in the client-server relationship. CA certificates for LDAP, Xerox Extensible Interface Platform (EIP), and SMart eSolutions are examples.
- Validates certificates that are installed on the printer, but not used. Certificates for HTTPS, LDAP, or SNMPv3 are examples.
- Checks features and protocols for non-compliant encryption algorithms. For example, NetWare and SNMPv3 use encryption algorithms that are not FIPS-compliant.

When validation is complete, information and links appear in a table at the bottom of the page.

- Click the appropriate link to disable a non-compliant feature, or protocol.
- Click the appropriate link to replace any non-compliant certificates.
- Click the appropriate link to acknowledge that you allow the printer to use non-compliant features and protocols.

Enabling FIPS 140 Mode and Checking for Compliance

1. In CentreWare Internet Services, click **Properties** > **Security** > **Encryption**.
2. Click **FIPS 140-2**.
3. Click **Enable**.
4. Click **Run Configuration Check and Apply**.

   A pass or fail message appears:

   - If the configuration check passes, click **Reboot Machine** to save and restart the printer.
   - If the configuration check fails, the reasons for the failed test list in a table at the bottom of the page. For each reason, a link is provided. Click the appropriate link to disable the protocol, replace the certificate, or allow the printer to use the non-compliant protocol.

Note: When FIPS 140 Mode is enabled, only FIPS-compliant certificates can be installed on the printer.

Stored Data Encryption

You can encrypt user data on the printer hard drive to prevent unauthorized access to data stored on the drive.

Enabling Encryption of Stored Data

1. In CentreWare Internet Services, click **Properties** > **Security** > **Encryption**.
2. Click **User Data Encryption**.
3. Under User Data Encryption Enablement select **Enabled**.
4. Click **Apply** to save the new settings or **Undo** to retain the previous settings.

⚠ **CAUTION:** The printer restarts. This interrupts or deletes current jobs. Xerox® recommends that you back up jobs and folders before enabling User Data Encryption.

IP Filtering

You can prevent unauthorized network access by creating an IP Filter to block or allow data sent from particular IP addresses.

Creating an IP Filter Rule

1. In CentreWare Internet Services, click **Properties** > **Security**.
2. Click **IP Filtering**.
3. Click **Add**.
4. From the Protocol menu, select the protocol. Options include **All**, **TCP**, **UDP**, or **ICMP**.
5. From the Action menu, select how you want the filter to manage the incoming packet.
   - If you want the printer to reject the packet and send an ICMP message back to the source host, select **Reject**.
   - If you want the printer to ignore the packet, select **Drop**.
6. To specify the order that actions are performed, select either **End of List** or **Beginning of List** from the Move This Rule To menu. Actions are performed in the order defined in the rule list. To arrange rule execution order, go to the IP Filtering page.
7. Type the Source IP Address.
8. Type a number between **0–32** for the Source IP Mask that uses this rule. The range of 0–32 corresponds to the 32-bit binary number comprising IP addresses. For example:
   - The number 8, represents a Class A address with a mask of 255.0.0.0.
   - The number 16 represents a Class B address with a mask of 255.255.0.0.
   - The number 24 represents a Class C address with a mask of 255.255.255.0.
9. If TCP or UDP is the selected Protocol type:
   a. Type the Source Port if applicable. The Source Port is the originating port that the rule has been created to manage. If the incoming packet does not originate from this port, the rule is ignored.
   b. Type the Destination Port that the rule has been created to manage. If the incoming packet is not sent to this port, the rule is ignored.
10. If ICMP is the selected Protocol type, select which ICMP Message type the rule is meant to manage.
11. Click **Apply** to save the new settings or **Cancel** to return to the previous screen.
12. Restart your printer for the new settings to take effect.

Editing an IP Filter Rule

1. In CentreWare Internet Services, click **Properties** > **Security**.
2. Click **IP Filtering**.
3. Click an IP filter rule.
4. Click **Edit** and edit the rule.
5. Click **Apply**.

Arranging the Execution Order of IP Filter Rules

1. In CentreWare Internet Services, click **Properties** > **Security**.
2. Click **IP Filtering**.
3. Click an IP filter rule.
4. Under **Move selected rule to position**, select the position and click **Move**.

Audit Log

The Audit Log feature records events that occur on the printer. You can then download the log as a tab-delimited text file to review for potential problems or security issues.

Enabling Audit Log

Before you begin:

Ensure that Secure HTTP (SSL) is enabled.

1. In CentreWare Internet Services, click **Properties** > **Security**.
2. Click **Audit Log**.
3. Click **Enabled** under Enabling Audit Log on machine.
4. Click **Apply**.

Saving an Audit Log

1. In CentreWare Internet Services, click **Properties** > **Security**.
2. Click **Audit Log**.
3. Click **Save**.
4. Right-click the **Download Log** link and save the compressed **auditfile.txt.gz** file to your computer.
5. Extract the **Auditfile.txt** text file, and open it in a spreadsheet application that can read a tab-delimited text file.

Interpreting the Audit Log

The Audit Log is formatted into ten columns:

- **Index**: Column 1 lists a unique value that identifies the event.
- **Date**: Column 2 lists the date that the event happened in mm/dd/yy format.
- **Time**: Column 3 lists the time that the event happened in hh:mm:ss format.
- **Event ID**: Column 4 lists the type of event. The number corresponds to a unique description.
- **Event Description**: Column 5 lists an abbreviated description of the type of event.

  Notes:

  - One audit log entry is recorded for each network destination within a Workflow Scanning scan job.
  - For Server Fax jobs, one audit log entry is recorded for each Server Fax job, regardless of the number of destinations.
  - For LAN Fax jobs, one audit log entry is recorded for each LAN Fax job.
  - For Email jobs, one audit log entry is recorded for each SMTP recipient within the job.
- **Other Event Details**: Columns 6–10 list other information about the event, such as:

- **Identity**: User Name, Job Name, Computer Name, Printer Name, Folder Name, or Accounting Account ID display when Network Accounting is enabled.

Note: Authentication must be configured to record the user name in the Audit Log.

- **Completion Status**
- **Image Overwrite Status**: The status of overwrites completed on each job. Immediate Image must be enabled.

See also:

Audit Log Event Identification Numbers on page 190

IPsec

Internet Protocol Security (IPsec) is a group of protocols used to secure Internet Protocol (IP) communications by authenticating and encrypting each IP data packet. It allows you to control IP communication by creating protocol groups, policies, and actions.

You can control IP communication on the printer for the following:

- DHCP v4/v6 (TCP and UDP)
- DNS (TCP and UDP)
- FTP (TCP)
- HTTP (Scan Out, TCP port 80)
- HTTPS (Scan Out, TCP port 443)
- HTTPS (Web Server, TCP port 443)
- ICMP v4/v6
- IPP (TCP port 631)
- LPR Print (TCP port 515)
- Port 9100 Print (TCP port 9100)
- SMTP (TCP/UDP port 25)
- SNMP (TCP/UDP port 161)
- SNMP Traps (TCP/UDP port 162)
- WS-Discovery (UDP port 3702)
- Up to 10 additional services

Enabling IPsec

Before you begin:

Ensure that Secure HTTP (SSL) is enabled.

1. In CentreWare Internet Services, click **Properties** > **Security**.
2. Click **IPsec**.
3. Under Enablement, select **Enabled**.
4. Click **Apply** to save the new settings or **Undo** to retain the previous settings.

Managing Actions

Use actions to more specifically manage how IPsec controls dependent protocols.

Creating a New Action

1. Click **Actions** at the top of the IPsec page.
2. Click **Add New Action**.
3. On the Step 1 of 2 page, under IP Action Details, type in the Name. This field is required.
4. In the Description field, type a description for the action, if desired.
5. Under Keying Method, select **Manual Keying** or **Internet Key Exchange (IKE)**.

   Note: Select Manual Keying if client devices are not configured for or do not support IKE.

6. If you selected IKE, under Pre-shared Key Passphrase, type the passphrase, then click **Next**.

Configuring Manual Keying Settings

Manual Keying is used when client systems either do not support IKE or are not configured for IKE.

1. Under IPsec Mode, select **Transport Mode** or **Tunnel Mode**.

   Note: Transport mode only encrypts the IP payload, whereas Tunnel mode encrypts the IP header and the IP payload. Tunnel mode provides protection for an entire IP packet by treating it as an Authentication Header (AH), or Encapsulating Security Payload (ESP).

2. If you selected Tunnel Mode, under Enable Security End Point Address, select the address type. Options are **Disabled**, **IPv4 Address**, or **IPv6 Address**.
3. Under IPsec Security, select **ESP**, **AH**, or **BOTH**.
4. In the Security Parameter Index: IN field, type a 32-bit number larger than 256 that identifies the inbound Security Association (SA).
5. In the Security Parameter Index: OUT field, type a 32-bit number larger than 256 that identifies the outbound Security Association (SA).
6. Under Hash, select from the following:
   - **SHA1**
   - **None**
7. Under Enter Keys as, select **ASCII format** or **Hexadecimal number**.
8. Type a 20-character ASCII key, or 40-character Hexadecimal key for the following:
   - **Hash Key: IN**
   - **Hash Key: OUT**
9. If you selected ESP or BOTH for the IPsec Security type, select one or more of the following Encryption types:

   Note: If the IPsec Security type is set to AH, the Encryption type options do not appear.

   - **AES**
   - **3DES**
   - **None**
10. Type a 24-character ASCII key, or 48-character Hexadecimal key for the following:
    - **Encryption Key: IN**
    - **Encryption Key: OUT**
11. Click **Save** to apply the new settings or **Undo** to retain the previous settings.

Configuring Internet Key Exchange Settings

IKE is a keying protocol that allows automatic negotiation and authentication, anti-replay services, and CA support. It can also change encryption keys during an IPsec session. IKE is used as part of virtual private networking.

IKE Phase 1 authenticates the IPsec peers and sets up a secure channel between the peers to enable IKE exchanges. IKE Phase 2 negotiates IPsec SAs to set up the IPsec tunnel.

1. Under IKE Phase 1, in the Key Lifetime field, type the length of time until the key expires in **Seconds**, **Minutes**, or **Hours**. When a key reaches this lifetime, the SA is renegotiated and the key is regenerated or refreshed.
2. Select the DH Group from the following options:
   - **Group 2** provides a 1024-bit Modular Exponential (MODP) keying strength.
   - **Group 14** provides a 2048-bit MODP keying strength.
3. Under IKE Phase 2, select the IPsec Mode. Options are **Transport Mode** or **Tunnel Mode**.

   Note: Transport mode only encrypts the IP payload, whereas Tunnel mode encrypts the IP header and the IP payload. Tunnel mode provides protection for an entire IP packet by treating it as an Authentication Header (AH), or Encapsulating Security Payload (ESP).

4. If you selected Tunnel Mode, under Enable Security End Point Address, select the address type. Options are **Disabled**, **IPv4 Address**, or **IPv6 Address**.
5. Under IPsec Security, select **ESP**, **AH**, or **BOTH**.
6. Type the Key Lifetime, and select **Seconds**, **Minutes**, or **Hours**.
7. Under Perfect Forward Secrecy (PFS), select **None**, **Group 2**, or **Group 14**.

   Note: PFS is disabled by default. PFS allows faster IPsec setup, but is less secure.

8. Under Hash, select from the following:
   - **SHA1**
   - **None**
9. If you selected ESP or BOTH for the IPsec Security type, select one or more of the following Encryption types:

   Note: If the IPsec Security type is set to AH, the Encryption type options do not appear.

   - **AES**
   - **3DES**
   - **Null**
10. Click **Save** to apply the new settings or **Undo** to retain the previous settings.

Editing or Deleting an Action

To edit or delete an action, select the action from the list, then click **Edit** or **Delete**.

Managing Protocol Groups

Protocol Groups are logical groupings of selected protocols based on service type, service name, port number, and device type. Create a Protocol Group to apply specific security policies for selected protocols.

Creating a New Protocol Group

1. Click **Protocol Groups** at the top of the IPsec page.
2. Click **Add New Protocol Group**.
3. Type a Name and a Description for the group.
4. Under Service Name, select the protocols that you want to add to the group.
5. To control a service that is not listed, under Custom Protocols type a name for the service and select the check box under Service Name.
6. To control a service that is not listed, under Custom Protocols type a name for the service and select the check box under Service Name.
7. Select **TCP** or **UDP** from the Protocol list.
8. Type the port number, and specify if the printer is the server or client.
9. Click **Save** to apply the new settings or **Undo** to retain the previous settings. Click **Cancel** to return to the previous page.

Editing or Deleting a Protocol Group

To edit or delete a protocol group, select the protocol group from the list, and click **Edit** or **Delete**.

Managing Host Groups

Host groups are groupings of computers, servers, or other devices that you want to control using security policies.

Creating a New Host Group

1. Click **Host Groups** at the top of the IPsec page.
2. Click **Add New Host Group**.
3. Type a Name and a Description for the group.
4. Under Address List, select **IPv4** or **IPv6**.
5. Select an Address Type. Options are **Specific**, **All**, or **Subnet**.
6. Type the appropriately formatted IP address.
7. To continue to add addresses to the group, click **Add**.
8. To delete addresses, next to any address, click **Delete**.
9. Click **Save** to apply the new settings or **Undo** to retain the previous settings.

Editing or Deleting a Host Group

To edit or delete a host group, select the host group from the list, and click **Edit** or **Delete**.

Managing Security Policies

IPsec security policies are sets of conditions, configuration options, and security settings that enable two systems to agree on how to secure traffic between them. You can have multiple policies active at the same time, however, the scope and policy list order determines the overall policy behavior.

Defining a Security Policy

1. Click **Security Policies** at the top of the IPsec page.
2. Under Define Policy, select a Host Group from the menu.
3. Select a Protocol Group from the menu.
4. Select an Action from the menu.
5. Click **Add Policy**.

Prioritizing a Security Policy

To prioritize policies, under Saved Policies, select the policy you want to move, then click the **Promote** or **Demote** buttons.

Editing or Deleting a Security Policy

To delete a policy, under Saved Policies, select the policy and click **Delete**.

Security Certificates

A digital certificate is a file that contains data used to verify the identity of the client or server in a network transaction. A certificate also contains a public key used to create and verify digital signatures. One device proves its identity to another by presenting a certificate trusted by the other device. Or, the device can present a certificate signed by a trusted third party and a digital signature proving its ownership of the certificate.

A digital certificate includes the following data:

- Information about the owner of the certificate
- The certificate serial number and expiration date
- The name and digital signature of the Certificate Authority (CA) that issued the certificate
- A public key
- A purpose defining how the certificate and public key can be used

There are three types of certificates:

- **Device Certificate**: A certificate for which the printer has a private key, and the purpose specified in the certificate allows it to be used to prove identity.
- **CA Certificate**: A certificate with authority to sign other certificates.
- **Trusted Certificate**: A self-signed certificate from another device that you want to trust.

To ensure that the printer can communicate with other devices over a secure trusted connection, both devices must have certain certificates installed.

For protocols such as HTTPS, the printer is the server, and must prove its identity to the client Web browser. For protocols such as 802.1X, the printer is the client, and must prove its identity to the authentication server, typically a RADIUS server. For features that use these protocols, perform the following two tasks:

- Install a device certificate on the printer.

  Note: When you enable HTTPS, a Xerox® Device Certificate is automatically created and installed on the printer.

- Install a copy of the CA certificate that was used to sign the device certificate of the printer on the other device.

Protocols such as LDAP and IPsec require both devices to prove their identity to each other.

For features that use these protocols, perform the tasks listed under one of the following options:

Option 1

- Install a device certificate on the printer.
- Install a copy of the CA certificate that was used to sign the device certificate of the printer on the other device.
- Install a copy of the CA certificate that was used to sign the certificate of the other device on the printer.

Option 2

If the other device is using a self-signed certificate, install a copy of the trusted certificate of the other device on the printer.

Installing a Digital Certificate

There are three ways to install a certificate on the printer:

- Create and install a Xerox® Device Certificate.

  Create a Xerox® Device Certificate to allow the printer to generate a certificate, sign it, and create a public key used in SSL encryption. Install the Xerox® Device Certificate on the printer, and install the Generic Xerox® Trusted CA Certificate in the devices that the printer communicates with. Examples of other devices are client Web browsers for HTTPS, or RADIUS authentication server for 802.1X. Installing this certificate ensures that users can access the printer using CentreWare Internet Services, and certificate warning messages do not appear.

  Note: Creating a Xerox® Device Certificate is less secure than creating a certificate signed by a trusted CA. If you do not have a server functioning as a Certificate Authority, install a Xerox® Device Certificate on the printer. Then install the Generic Xerox® Trusted CA Certificate on the other devices.

- Create a Certificate Signing Request (CSR) and install the CA-signed device certificate.

  Create a CSR. Send the CSR to a CA or a local server functioning as a CA to sign the CSR and return the certificate. Install the certificate on the printer. An example of a server functioning as a CA is Windows Server 2008 running Certificate Services.
- Install trusted CA and self-signed certificates.

  Install the certificates of the root CA, and any intermediate CAs for your company. Install the self-signed certificates from any other devices in your network.

Creating and Installing a Xerox® Device Certificate

1. In CentreWare Internet Services, click **Properties** > **Security**.
2. Click **Security Certificates**.
3. Click the **Xerox Device Certificate** tab.
4. Select **Create New Xerox Device Certificate**.
5. Complete the form with the requested information.
6. Click **Finish**.

Creating a Certificate Signing Request

1. In CentreWare Internet Services, click **Properties** > **Security**.
2. Click **Security Certificates**.
3. Click the **CA-Signed Device Certificate(s)** tab.
4. Select **Create Certificate Signing Request (CSR)**.
5. Complete the form with your 2-Letter Country Code, State/Province Name, Locality Name, Organization Name, Organization Unit, and Email Address.
6. Select **Subject Alternative Name** if applicable, and type the MS Universal Principal Name.

   Note: The Subject Alternative Name is only required when using 802.1X EAP -TLS for Windows clients or servers.

7. Click **Finish**.

Uploading a CA-Signed Device Certificate

1. In CentreWare Internet Services, click **Properties** > **Security**.
2. Click **Security Certificates**.
3. Click the **CA-Signed Device Certificate(s)** tab.
4. Select **Install CA-signed Device Certificate**.
5. Click **Browse** or **Choose File**, navigate to the signed certificate in **.pem** or **PKCS#12** format, and click **Open** or **Choose**.
6. Click **Next**.
7. If the certificate is password protected, type the password then retype it to verify.
8. Type a Friendly Name to help identify the certificate in the future.
9. Click **Next**.

   Note: The signed certificate must match the CSR created by the printer.

Installing a Root Certificate

1. In CentreWare Internet Services, click **Properties** > **Security**.
2. Click **Security Certificates**.
3. Click the **Root/Intermediate Trusted Certificate(s)** tab.
4. Click **Install external Root/Intermediate trusted certificates**.
5. Click **Browse** or **Choose File**, navigate to the signed certificate **.crt** file, then click **Open** or **Choose**.
6. Click **Next**.
7. Type a Friendly Name to help identify the certificate in the future.
8. Click **Next**.
   The digital certificate appears in the list of Installed certificates.

Viewing, Saving, or Deleting a Certificate

1. On the Security Certificates page, click a certificate type tab.
2. To view or save a certificate, under Action, click **View/Save**.

   Certificate details appear on the View/Save Device Certificate page.

   a. To save the certificate file to your computer, at the bottom of the page, click **Save Base-64 encoded (PEM)**.

   b. Click **Cancel** to return to the Security Certificates page.
3. To delete a certificate, select the check box next to the certificate name and click **Delete**.

   Note: You cannot delete the Default Xerox® Device Certificate.
4. Click **Reset to Machine/Device Factory Defaults** to delete all certificates except the Default Xerox® Device Certificate.

Installing the Generic Xerox® Trusted CA Certificate

If the printer uses the Xerox® Device Certificate, and a user attempts to access the printer using CentreWare Internet Services, an error message can appear on their Web browser. To ensure that error messages do not appear, install the Generic Xerox® Trusted CA Certificate in the Web browsers for all users.

1. In CentreWare Internet Services, click **Properties** > **Security**.
2. Click **Security Certificates**.
3. Click **Download the Generic Xerox® Trusted CA Certificate**, and save the file to your computer.
4. Install the file in your Web browser certificate store location. For details, see your Web browser help.

   Note: You can also download the Generic Xerox® Trusted CA Certificate from the HTTP page at **Properties** > **Connectivity** > **Protocols** > **HTTP**.

802.1X

802.1X is an Institute for Electrical and Electronics Engineers (IEEE) standard that defines a method for port-based network access control or authentication. In an 802.1X secured network, the printer must be authenticated by a central authority, typically a RADIUS server, before it can access the physical network.

You can enable and configure the printer to be used in an 802.1X secured network from the printer control panel or in CentreWare Internet Services.

Before you begin:

- Ensure that your 802.1X authentication server and authentication switch are available on the network.
- Determine the supported authentication method.
- Create a user name and password on your authentication server.

  Note: This procedure causes the printer to restart and be unavailable over the network for several minutes.

Enabling and Configuring 802.1X at the Control Panel

1. At the printer control panel, press the **Machine Status** button, then touch the **Tools** tab.
2. Touch **Network Settings** > **Advanced Settings**.
3. Touch **Continue**.
4. Touch **802.1X**.
5. Touch **Enable**.
6. Touch **Authentication Method** and select the method used on your network. Options are:
   - **EAP-MD5**
   - **EAP-MS-CHAPv2**
   - **PEAPv0/EAP-MS-CHAPv2**

   Note: When the printer is in FIPS 140 mode, EAP-TLS authentication is required.

7. Touch **Username**.
8. Type the user name required by your authentication switch and server using the touch screen keyboard.
9. Touch **Password**, and type the password using the touch screen keyboard.
10. Touch **Save**, then touch **Save** again.
11. Touch **Close**.

Enabling and Configuring 802.1X in CentreWare Internet Services

1. In CentreWare Internet Services, click **Properties** > **Security**.
2. Click **802.1X**.
3. Under Protocol, select **Enable 802.1X**.
4. Under Authentication Method, select the method used on your network. Options are:
   - **EAP-MD5**
   - **PEAPv0/EAP-MS-CHAPv2**
   - **EAP-MS-CHAPv2**
   - **EAP-TLS**

   Note: When the printer is in FIPS 140 mode, EAP-TLS authentication is required.

5. Under User Name (Device Name), type the user name required by your authentication switch and server.
6. If you selected PEAPv0/EAP-MS-CHAPv2, EAP-MS-CHAPv2, or EAP-TLS as the Authentication Method, you can require the printer to validate certificates used to encrypt 802.1X. Under Server Validation, select the root certificate that you want to use to validate the authentication server. Select **No Validation** if you do not want to validate a certificate.

   Notes:

   - TLS authentication and server verification both require X.509 certificates. To use these features, install the necessary certificates on the Security Certificates page before configuring 802.1X.
   - The Default Xerox® Device Certificate cannot be used with EAP-TLS in Windows environments. It can be used in FreeRADIUS server environments.
7. To view or save a certificate, select the certificate from the menu and click **View/Save**.

   Certificate details appear on the View/Save Device Certificate page.

   a. To save the certificate file to your computer, at the bottom of the page, click **Save Base-64 encoded (PEM)**.

   b. Click **Cancel** to return to the previous page.
8. If you selected PEAPv0/EAP-MS-CHAPv2, EAP-MS-CHAPv2, or EAP-TLS as the Authentication Method, you can allow the printer to encrypt 802.1X communication. Under Device Certificate (TLS) - Authentication Certificate, select the certificate that you want to use.
9. To view or save a certificate, select the certificate from the menu and click **View/Save**.

   Certificate details appear on the View/Save Device Certificate page.

   a. To save the certificate file to your computer, at the bottom of the page, click **Save Base-64 encoded (PEM)**.
   b. Click **Cancel** to return to the previous page.

10. Under User Name (Device Name), type the user name required by your authentication switch and server.
11. Type the Password, then retype it to confirm.
12. To save the new password, select the check box next to Select to save new password. A password is not required for EAP-TLS authentication.
13. Click **Apply** to save the new settings or **Undo** to retain the previous settings.

System Timeout

You can specify how long the printer waits to log out an inactive user at the control panel.

Setting System Timeout Values

1. In CentreWare Internet Services, click **Properties** > **Security**.
2. Click **System Timeout**.
3. Under Web System Timer, type the inactive time from **6–6000** minutes, that the printer waits before it logs a user out of CentreWare Internet Services.
4. Under Touch User Interface System Timer, type the time that the printer waits before it logs a user out of the touch screen. Type the time, from **0–60** minutes, and select the time in seconds.
5. Under Warning Screen, select **Enabled** to require the printer to display a warning message before it logs a user out of the touch screen.
6. Click **Apply** to save the new settings or **Undo** to retain the previous settings.

Overwriting Image Data

To ensure that image data on the printer hard drive cannot be accessed, you can delete and overwrite image data. Image data is any in-process or temporary user data on the disk. Some examples include, current jobs, queued jobs, temporary scan files, saved jobs, and folders. You can select Standard or Full On Demand Image Overwrite.

Standard Image Overwrite

Standard Image Overwrite deletes all image data from the printer memory and hard drive, except:

- Jobs and folders stored in the Reprint Saved Jobs feature
- Jobs stored in the Scan to Mailbox feature
- Fax Dial Directories
- Fax Mailbox contents

Full Image Overwrite

Full Image Overwrite deletes all image data from the printer memory and hard drive, including:

- Jobs and folders stored in the Reprint Saved Jobs feature
- Jobs stored in the Scan to Mailbox feature
- Fax Dial Directories
- Fax Mailbox contents

Note: Not all options listed are supported on all printers. Some options apply only to specific printer models or configurations.

Manually Deleting Image Data

1. In CentreWare Internet Services, click **Properties** > **Security** > **On Demand Overwrite**.
2. Click **Manual**.
3. Under Standard or Full, click **Start**.
4. Click **OK** to delete image data.

Note: Depending on how many files are being deleted, the printer can be offline for up to 60 minutes during the deletion process.

Scheduling Routine Deletion of Image Data

1. In CentreWare Internet Services, click **Properties** > **Security** > **On Demand Overwrite**.
2. Click **Scheduled**.
3. To enable Scheduled On Demand Overwrite, under Frequency, select how often the printer deletes data: **Daily**, **Weekly**, **Monthly**, or **Disabled**.
4. Under Time, type the time the printer deletes data.
5. If you selected Weekly or Monthly frequency, under Day of Week or Day of Month, select the day or month that the printer deletes data.
6. Under Type, select **Full** or **Standard**.

⚠ **CAUTION:** If you select Full, the printer deletes all image data.

7. Click **Apply** to save the new settings or **Undo** to retain the previous settings.

Immediate Image Overwrite

Enable Immediate Image Overwrite to direct the printer to overwrite each job after it finishes processing.

Enabling Immediate Image Overwrite

1. At the printer control panel, press the **Machine Status** button, then touch the **Tools** tab.
2. Touch **Security Settings** > **Image Overwrite Security**.
3. Touch **Immediate Overwrite**.
4. Touch **Enable**.

PostScript Passwords

The PostScript language includes commands that allow PostScript print jobs to change the printer configuration. By default, PostScript jobs can use these commands, and a password is not required. To ensure that unauthorized changes are not made, you can require PostScript jobs to include a password.

You can enable the following passwords:

- **Run Start Job**: This password controls the execution of the Sys/Start file.
- **System Parameters Password**: Use this password to control the execution of PostScript programs that modify PostScript system parameters.
- **Start Job Password**: The Start Job password, used with the Startjob and Exitserver operators, restricts PostScript jobs from running unencapsulated to prevent them from changing default printer settings.

For more information, see the CentreWare Internet Services Help.

1. Under StartupMode, select **Enabled** to enable the Run Start job password.
2. Under System Parameters Password, type a password.
3. Retype the password to verify.
4. Under Job Start Password, type a password.
5. Retype the password to verify.
6. Click **Apply** to save the new settings or **Cancel** to return to the previous screen.

Enabling or Creating PostScript Passwords

1. In CentreWare Internet Services, click **Properties** > **Security**.
2. Click **PostScript Passwords**.
3. Under StartupMode, select **Enabled** to enable the Run Start job password.
4. Under System Parameters Password, type a password.
5. Retype the password to verify.
6. Under Job Start Password, type a password.
7. Retype the password to verify.
8. Click **Apply** to save the new settings or **Cancel** to return to the previous screen.

USB Port Security

You can prevent unauthorized access to the printer through USB ports by disabling the ports. There are three USB ports. One is in the front, and two are in the back of the printer.

Enabling or Disabling USB Ports

1. In CentreWare Internet Services, click **Properties** > **Security**.
2. Click **USB Port Security**.
3. Next to Front USB Port, select **Enabled** to enable the front USB port. Clear the check box to disable the port.
4. Next to Rear USB Ports (Pair), select **Enabled** to enable the rear two USB ports. Clear the check box to disable the ports.
5. Click **Apply** to save the new settings or **Undo** to retain the previous settings.

   Notes:

   - If USB ports are disabled, you cannot use a USB card reader for authentication, update the software, or print from a USB Flash Drive.
   - If your printer model has a cover for the USB port on the control panel, you can install or remove the cover. Installation instructions and the necessary part are stored in the compartment inside of Tray 1.

Printing

5

This chapter includes:

Saving and Reprinting Jobs

The Reprint Saved Jobs feature allows you to save your print job on the printer so that you can print it at any time.

Enabling the Reprint Saved Jobs Feature

1. In CentreWare Internet Services, click **Properties** > **Services** > **Print From**.
2. Click **Reprint Saved Jobs** > **Enablement**.
3. Under Enablement, select **Enabled**.
4. Click **Apply** to save the new settings or **Undo** to retain the previous settings.

Creating and Managing Saved Jobs Folders

By default, if Reprint Saved Jobs is enabled, jobs are saved in the Default Public Folder. To create new folders or manage folders, use the Saved Jobs page.

Creating a Folder

1. In CentreWare Internet Services, click **Jobs** > **Saved Jobs**.
2. On the Saved Jobs page, click **Create New Folder**.
3. Under Name, type the name you want for the folder.
4. Under Folder Permissions, select the type of folder you want. Options include:
   - Public Folder
   - Read-Only
   - Private
5. Click **Apply**.

   The new folder displays in the Folders list.

Managing a Folder

1. On the Saved Jobs page, click **Manage Folders**.
2. Click the pencil icon next to the name you want to edit.

   The Edit Folder Properties page appears.

   If allowed, you can rename the folder and change folder permissions.
3. Click **Apply** to save the new settings or **Cancel** to return to the previous screen.

   The updated folder appears in the Folders list.

Deleting a Folder

1. Click **Manage Folders**.

   The list of existing folders appears.
2. Select the folder you want to delete.

   The Delete Folder button activates.
3. Click **Delete Folder**.

   A warning message appears informing you that the delete is permanent.
4. Click **OK** to delete or **Cancel** to exit.

Saving and Printing Jobs

Saving a Job from Your Computer

1. With your file open, click the **File** menu in the application, then click **Print**.
2. From the application Print window, select your printer from the Printer Name menu.
3. Click **Properties** to access the print settings for the job.
4. On the Paper/Output tab, click the **Job Type** menu, then select **Saved Job**.
5. On the Save Job page, click **Save** to save the job to printer to print later. Click **Save and Print** to save the job to the printer and print it immediately.
6. Type a Job Name for the job or select **Use Document Name** to use the document file name being submitted.
7. Select the destination folder from the Folder menu. You can select **Default Public Folder** or type in a name for a new folder.
8. To save your job as a secure job, type in and retype a 4–10 digit passcode in the passcode fields, then click **OK**.
9. Click **OK** to save your settings.

Backing up Saved Jobs

1. In CentreWare Internet Services, click **Properties** > **Services** > **Print From**.
2. Click **Reprint Saved Jobs** > **Backup Jobs**.
3. Under Settings, select **FTP** as the protocol.
4. Select the address type and Port for the FTP server to use to back up jobs. Options are **IPv4 Address**, **IPv6 Address**, or **Host Name**.
5. Type the appropriately formatted address in the IP Address and Port field. The default port number is 21.
6. Type the path to the file repository in the Document Path field.
7. Type the filename for the backup file in the File Name field. This name is appended to the end of the document path.
8. Type the login name for the FTP server in the Login Name field.
9. Type and retype the Password.
10. Enable **Select to Save New Password**.
11. Click **Start** to begin the backup or **Undo** to retain the previous settings.

Restoring Saved Jobs from an FTP Repository

1. In CentreWare Internet Services, click **Properties** > **Services** > **Print From**.
2. Click **Reprint Saved Jobs** > **Restore Jobs**.
3. Under Settings, select **FTP** as the protocol.
4. Select the address type and Port for the FTP server where the saved jobs are stored. Options are **IPv4 Address**, **IPv6 Address**, or **Host Name**.
5. Type the appropriately formatted address in the IP Address: Port field. The default port number is **21**.
6. Type the path to the file repository in the Document Path field.
7. Type the name for the backup file that you want to restore In the File Name field. This name is appended to the end of the document path.
8. Type the login name of the FTP server In the Login Name field.
9. Type and retype a Password.
10. Enable **Select to Save New Password**.
11. Click **Start** to begin restoring Saved Jobs or **Undo** to retain the previous settings.

⚠ **CAUTION:** When you restore backed-up jobs, existing stored jobs are overwritten, and the Default Public Folder is emptied.

Printing Jobs from CentreWare Internet Services

You can print **.pdf**, **.ps**, **.pcl**, and **.xps** files from CentreWare Internet Services.

1. In CentreWare Internet Services, click **Print**.

   The Job Submission page appears.
2. Type the name of the file in the File Name field, or click **Browse** to select the file from a local network or remote location.
3. Under Printing, select the desired options for the job.
4. Click **Submit Job** to print the document.

   Note: To ensure that the job was sent to the queue, wait for the job submission confirmation message to appear before you close this page.

Managing Banner Page Printing Options

You can set the printer to print a banner page with each print job. The banner page contains information identifying the user and job name. You can set this option in the print driver, in CentreWare Internet Services, or at the control panel.

> Note: Enable Banner page printing in the print driver and at the control panel or in CentreWare Internet Services or a banner page does not print.

Enabling Banner Page Printing in CentreWare Internet Services

1. In CentreWare Internet Services, click **Properties** > **Services**.
2. Click **Printing** > **General**.
3. Under Print Banner Sheets, select **Yes** to allow banner pages to print or **No** to disable this option.
4. Under Allow the Print Driver to Override, select **Yes** to allow the print driver settings for banner page printing to override the setting selected on this page.
    - Under Banner Sheet Identification, select the information that prints on the banner page.
5. Click **Apply** to save the new settings or **Undo** to retain the previous settings.

Enabling Banner Page Printing at the Control Panel

1. At the printer control panel, press the **Machine Status** button, then touch the **Tools** tab.
2. Touch **Service Settings**.
3. Touch **Job Sheets** > **Banner Sheets**.
4. Under Print Banner Sheets, touch **Yes**.
5. Under Allow the Print Driver to Override, touch **Yes** to allow users to turn banner page printing on or off in the print driver.
6. Under Banner Sheet Identification, select the information that prints on the banner page:
    - **Job Owner User ID and Job Name**
    - **Xerox Network Accounting User ID and Job Name**
    - **Generic User ID and Job Number**
7. Touch **Save**.

Enabling Banner Page Printing in the Print Driver

1. With your file open, click the **File** menu in the application, then click **Print**.
2. From the application Print window, select your printer from the Printer Name menu.
3. Click **Properties** to access the print settings for the job.
4. Click the **Advanced** tab.
5. Click to expand the Paper/Output option.
6. Click **Banner Sheets**, then click the down arrow and select **Enabled** or **Disabled**.
7. Click **OK**.

   Note: If banner page printing is disabled in CentreWare Internet Services or at the control panel, setting the print driver to print banner pages is ignored.

Secure Print Settings

You can configure Secure Print settings to specify how the printer behaves when a user sends a Secure Print job to the printer.

1. In CentreWare Internet Services, click **Properties** > **Services** > **Printing** > **Secure Print**, or click **Security** > **Secure Print**.
2. Under Method, select the information that a user must type at the control panel to release a Secure Print job. Select an option:
   - **User ID**: If a user logs in at the control panel, they can release Secure Print jobs that they sent.
   - **Passcode**: User types a passcode to release a Secure Print job at the control panel.
3. Type a number from 4 through10 to specify the length of the Secure Print password.
4. When a Secure Print job is sent to the printer, by default, the job name appears in the list of jobs on the control panel touch screen. The characters in the job name are shown as asterisks to hide the the title of the document that is being printed. To reveal or hide the characters in job names with asterisks, select an option:
   - **Conceal All Job Names**
   - **Show All Job Names**
   - **Conceal Secure Print Job Names Only**
5. Click **Apply**.

Hold All Jobs

You can enable and configure the Hold All Jobs feature to require users to release print jobs manually at the control panel.

Configuring the Hold all Jobs Feature

1. In CentreWare Internet Services, click **Properties** > **Services**.
2. Click **Printing** > **Hold All Jobs**.
3. Under Enablement, select an option:
   - **Hold all Jobs in a Private Queue**: The printer holds sent jobs in a locked folder. Users must log in at the control panel to view, print, and delete jobs.
   - **Hold all Jobs in a Public Queue**: The printer holds sent jobs in an unlocked folder. Users are not required to log in at the control panel unless accessing a Secure Print job.
4. Under User Validation Policies for Releasing Jobs, select an option:
   - **Use ID Only**: The printer allows a user to release a held job by validating the user ID only. This option allows users to log in using a different domain than the one the printer is using.
   - **Use ID and Domain**: The printer allows a user to release a held job by validating both the user ID and the domain name. This option ensures that the printer distinguishes users with the same user name but different domains. For example, jobs sent by JSmith@wgc.yourcompany.com are filed separately from jobs sent by JSmith@na.yourcompany.com. Each user cannot release the job of the other person.
5. Under Unidentified Job Policies, select an option:

   Note: Unidentified jobs are jobs that are not associated with a user name. Unidentified jobs originate from a computer that does not require a user to log in. Examples are a job sent from a DOS or UNIX window using LPR, Port 9100, or from the Jobs tab in CentreWare Internet Services.

   - **Hold Jobs; All Users can Manage Jobs**: All users can view, print, and delete unidentified jobs. Users must enter a passcode to release Secure print jobs.
   - **Hold Jobs; Only Administrators can Manage Jobs**: Only system administrators can view, print, and delete unidentified jobs. System administrators must enter a passcode to release Secure Print jobs.
   - **Delete Jobs Immediately**: All unidentified jobs are deleted and are not printed. Deleted jobs appear in a list at the control panel in the Completed Jobs queue.
   - **Print Jobs Immediately**: All unidentified jobs are printed immediately except for unidentified Secure Print jobs. Users must enter a passcode to release Secure Print jobs.
6. Click **Apply**.
7. Enable authentication or configure other related settings if necessary. At the bottom of the page, under Related Configuration Settings, click **Edit** under Action next to the setting you want to configure.

UNIX, Linux, and AS/400 Printing

UNIX-based printing uses LPD/LPR port 515 or lp to port 9100 to provide printer spooling and network print server functionality. Xerox® printers can communicate using either protocol.

Xerox® Services for UNIX Systems

Xerox® Services for UNIX Systems (XSUS) is an application that allows you to manage and print to multiple printers in UNIX and Linux environments. XSUS allows you to:

- Configure and check the status of network connected printers.
- Set up a printer on your network as well as monitor the operation of the printer once installed.
- Perform maintenance checks and view supplies status at any time.
- Provide a common look and feel across the many different suppliers of UNIX and Linux operating systems.

Supported Printing Models

- **Workstation-to-printer (Peer-to-Peer)**: Print jobs are processed and spooled locally on your computer, then sent directly to the printer. XSUS must be installed on each computer.
- **Workstation-to-Server (Client-Server)**: Print jobs are processed and spooled on your computer, then sent to the printer. Install XSUS on both the server and the computer.
- **Server Based**: Print jobs are sent unprocessed from your computer, spooled on the server, then sent to the printer. Install XSUS on the server only. Individual computers can set up a generic lp or lpr queue and point to the queue on the print server.
- **Network Information Service (NIS) Based**: NIS uses a printer configuration map on the server. As new printer queues are added to a print server, only the configuration file in the master NIS server is updated. NIS clients can then print to any of the queues listed on the server map without setting up local queues.

For more information on how to set up NIS-based printing, see your UNIX or Linux operating system documentation.

Installing XSUS

Before you begin:

Ensure that you have root or superuser privileges to install XSUS.

1. From the Xerox® Drivers and Downloads website, download the following **.tgz** files to a temporary directory:
    - Printer Model Package file which contains PPD files for all printer models. The file name is PrinterPkgXPXX_20xx_xx_xx.tgz.
    - Print Driver for your operating system. The available files are:
        - XeroxAIXpowerpcxpxx_x.xx.xx.tgz for the IBM RS6000 family.

- XeroxHPUXXPXX_x.xx.xx.tgz to support HP workstations.
- XeroxLinuxi386XPXX_x.xx.xx.tgz to support Linux environments.
- XeroxSolarisXPXX_x.xx.xx.tgz for Sun Solaris systems.

Note: Each expanded **.tgz** file requires as much as four times its original size in disk space.

2. At the UNIX command line, type **gzip -dfv {filename.tgz}** then press **Return** or **Enter**. The filename must include a **.tgz** extension.
3. Type **tar -xvf {filename.tgz}** then press **Return** or **Enter**.
4. The files are expanded and two directories are created with names that match the print driver and Printer Model Package **.tgz** file names. Perform the expansion steps for both **.tgz** files.
5. Change to the directory created by the expansion of the Code **.tgz** file.
6. On the command line, type **./setup** then press **Return** or **Enter**.
7. Change to the directory created by the expansion of the Printer Definition **.tgz** file.
8. Type **./setup** then press **Return** or **Enter**.

The installation creates a Xerox directory in /usr or /opt depending on your operating system.

Launching XSUS

To launch XSUS from a terminal window prompt as root, type **xpadmin**, then press **Enter** or **Return**. XSUS automatically detects if the X server on your system is able to run in graphical mode or not and starts accordingly.

For more information on managing printers and queues through XSUS, see the *XSUS Administrator Online Help*.

Printing from a Linux Workstation

Ensure that CUPS is installed and running on your workstation. The instructions for installing and building CUPS are contained in the *CUPS Software Administrators Manual*, written and copyrighted by Easy Software Products.

For complete information on CUPS printing capabilities, refer to the *CUPS Software Users Manual* available from www.cups.org/documentation.php .

Installing the PPD on the Workstation

1. Download the Xerox® PPD for CUPS from the Drivers and Downloads page on the Xerox® Support website.
2. Copy the PPD into the CUPS ppd/Xerox folder on your workstation. If you are unsure of the location of the folder, use the Find command to locate the PPD files.
3. Follow the instructions that are included with the PPD.

Adding the Printer

1. Verify that the CUPS daemon is running.
2. Open a Web browser and type **http://localhost:631/admin**, then click **Enter** or **Return**.
3. For User ID, type **root**. For password, type the root password.
4. Click **Add Printer** and follow the onscreen prompts to add the printer to the CUPS printer list.

Printing with CUPS

CUPS supports the use of both the System V (lp) and Berkeley (lpr) printing commands.

1. To print to a specific printer in System V, type: **lp -dprinter filename**, then click **Enter**.
2. To print to a specific printer in Berkeley, type: **lpr -Pprinter filename**, then click **Enter**.

AS/400

Xerox® provides Work Station Customization Object (WSCO) files to support AS/400 or Iseries, V5R2 or later systems. The WSCO file provides printer-specific PCL codes. The host print transform uses these codes to select the correct tray, 2-sided option, font size and type, and orientation.

The XTOOLSxxxx library provides a source WSCO for each supported Xerox® printer or device. You only download and install the library once.

Notes:

- The host print transform only works on files that are of the type AFPDS and SCS. PIDS formatted printer files must be recreated as type AFPDS to use the WSCO for printing.
- You must have IOSYSCFG permissions to create a device description or a remote queue.
- For details on AS/400, refer to the *IBM AS/400 Printing V, (Red Book),* available on the IBM website.

Installing the WSCO and Setting up Print Queues

For detailed instructions on installing the library and setting up print queues, refer to the installation instructions that are included with the library.

Print from USB

This feature allows you to print a file that is stored on a USB Flash Drive from the USB port on the printer control panel.

Before you begin:

Enable USB ports. For details, see USB Port Security on page 97.

Enabling Print from USB

1. In CentreWare Internet Services, click **Properties** > **Services**.
2. Click **Print From** > **Print from USB**.
3. Under Print from USB, select **Enabled**.

Managing Copy Functions

6

This chapter includes:

Specifying Default Copy Settings

1. At the printer control panel, press the **Machine Status** button, then touch the **Tools** tab.
2. Touch **Service Settings**.
3. Touch **Copy Service Settings**.
4. Touch **Feature Defaults**.
5. Make the desired changes to the settings on the following tabs:
    - **Copy**: Update Output Color, Reduce/Enlarge settings, Paper Supply, 2-Sided Copying, and Copy Output settings.
    - **Image Quality**: Update Image Options, Image Enhancement, and Color Balance settings.
    - **Layout Adjustment**: Update Original Size, Image Shift, and Edge Erase settings.
    - **Output Options**: Set Annotations for copy jobs.
6. Touch **Save Defaults**.

Changing the Reading Order

You can change the order that pages are scanned in books, which impacts Book Copy and Book Fax features. You can also change the order that pages are printed, which impacts the Page Layout and Booklet Creation features.

To change the Reading Order options:

1. At the printer control panel, press the **Machine Status** button, then touch the **Tools** tab.
2. Touch **Service Settings**.
3. Touch **Copy Service Settings**.
4. Touch **Reading Order Options**.
5. Under Scan Order, touch either:
   - **Hide Reading Order**
   - **Show Reading Order**

   If Show Reading Order is selected, default reading order options appear.
6. Touch either **Left to Right** or **Right to Left**.
7. Under Print Order, touch either:
   - **Hide Reading Order**
   - **Show Reading Order**

   If Show Reading Order is selected, default reading order options appear.
8. Touch either **Left to Right** or **Right to Left**.
9. Touch **Save**.

Accessing Copy Presets

1. At the printer control panel, press the **Machine Status** button, then touch the **Tools** tab.
2. Touch **Service Settings**.
3. Touch **Copy Service Settings**.

Edge Erase Presets

To create an Edge Erase Preset:

1. Touch **Edge Erase Presets**.
2. Touch **Presets**, then touch **Available** in the list of presets.
3. Touch **Name** at the bottom of the window, then, using the touch screen keyboard, touch **Clear Text**.
4. Enter the name of the new preset, then touch **Save**.

To edit an existing preset:

1. Touch **Edge Erase Presets**.
2. Touch **Presets**, then touch the desired preset.
3. Touch **Side 1**, then touch the arrows to change the amount to erase from each edge.
4. Touch **Side 2**, then touch the arrows to change the amount to erase from each edge, or touch **Mirror Side 1**.
5. Touch **Save**.

Changing Image Shift Presets

1. Touch **Image Shift Presets**.
2. Touch **Presets**, then touch the desired preset.
3. Touch the arrows to change the amount of Up/Down and Left/Right shift for Side 1 and Side 2.
4. Touch **Save**.

Changing Reduce/Enlarge Presets

1. Touch **Reduce/Enlarge Presets**.
2. To change a proportional preset, touch **Proportional %**, touch the desired preset between **1–10**, then type the percentage using the touch-screen keypad.
3. To change a preset that uses an independent percentage for the width and length of the image, touch **Independent X-Y%**.
4. Touch the X and Y for the preset you want to change, then type the scale percentage using the touch-screen keypad.
5. Touch **Save**.

Scanning

7

This chapter includes:

Scanning to a Folder on the Printer

The Scan to Mailbox feature allows users to scan files to mailboxes, which are folders created on the printer hard drive. These files can then be retrieved through CentreWare Internet Services. This feature provides network scanning capability without the need to configure a separate server and is supported in Workflow Scanning.

For instructions explaining how to use this feature, see the *User Guide* at www.xerox.com/office/CQ9301_CQ9302_CQ9303docs .

Enabling or Disabling Scan to Mailbox

1. In CentreWare Internet Services, click **Properties** > **Services**.
2. Click **Scan to Mailbox** > **Enablement**.
3. Select **Enable Scan to Mailbox**.

   Note: Once you enable Scan to Mailbox, any mailboxes created display in Workflow Scanning.

4. To enable mailboxes to display on the Scan tab in CentreWare Internet Services, select **On Scan tab, view Mailboxes by default**.
5. Click **Apply** to save the new settings or **Undo** to retain the previous settings.

Setting Scan Policies

Scan policies allow you to manage how users are allowed to scan files, create folders, and assign passwords to their folders on the printer.

1. In CentreWare Internet Services, click **Properties** > **Services**.
2. Click **Scan to Mailbox** > **Scan Policies**.
3. Under Scan Policies, select or clear:
   - **Allow scanning to Default Public Folder**: Enable this option to allow users to scan files to the Default Public Folder without requiring a password.
   - **Require per job password for public folders**: Enable this option to require users to type a password for every job they scan to the public folder.
   - **Allow additional folders to be created**: Enable this option to allow users to create additional public or private folders on the printer. If **Require password when creating additional folders** is disabled, assigning a password to the folder is optional and creates a public folder. If **Allow additional folders to be created** is disabled, the **Create Folder** button does not display on the Scan tab.
   - **Require password when creating additional folders**: Enable this option to require users to type a new password every time they create a new folder. This feature only allows users to create private folders.
   - **Prompt for password when scanning to private folder**: Enable this option to require users to type the password at the control panel every time they scan a job to that private folder.

- **Allow access to job log data file**: Enable this option to allow users to print a job log containing details for any scanned image. Third-party applications can be used to search, file, and distribute jobs based on job log information.

4. Click **Apply**.

Managing Folders and Scanned Files

Creating and Editing a Folder

By default, all users are allowed to scan to the Default Public Folder. If this option has been enabled in Scan Policies, users can create and edit additional folders.

To create a folder:

1. In CentreWare Internet Services, click **Scan**.
2. Under Display, select **Mailboxes**.
3. Under Scan to Mailbox, click **Create Folder**.
4. Type a name for the folder.
5. If necessary, type a password, then retype the password again to verify.
6. Click **Apply**.

To change the folder password, click **Modify Folder**.

To edit the default scan settings for the folder, click **Personalize Settings**. Click **Edit** to edit the scan settings. For more information, see the CentreWare Internet Services Help.

Deleting Scanned Files

1. In CentreWare Internet Services, click **Properties** > **Services**.
2. Click **Scan to Mailbox** > **Files**.
3. To immediately remove files from the server, select an option:
   - **Delete all files now** to delete all files on the server.
   - **Delete all files older than** to delete files older than a specified number of days. Type how many days old files must be for deletion.
4. Click **Delete Files**.
5. Under Schedule Clean Up of Folder Files, specify the files that you want to delete. Type how many days old files must be for deletion.
6. Next to Cleanup time, select:
   - **Hourly** to have files deleted at the beginning of every hour.
   - **Daily** and specify the time of day for the delete process to run.
7. Click **Apply**.

Deleting Scan Folders

You can modify or delete scan folders from two locations in CentreWare Internet Services. Deleting folders from either location deletes them from the printer.

To delete folders from the Properties tab:

1. In CentreWare Internet Services, click **Properties** > **Services**.
2. Click **Scan to Mailbox**.
3. Select the folder to delete, then click **Modify Folder**.
4. Under Remove folder from device, click **Delete Folder**.

To delete folders from the Scan tab:

1. In CentreWare Internet Services, click **Scan**.
2. Under Display, click **Mailboxes**, then select the folder you want to delete. If the folder is private, type the password.
3. Select the folder to delete, then click **Modify Folder**.
4. Under Remove folder from device, click **Delete Folder**.

Managing Folder Passwords

You can modify folder passwords from two locations in CentreWare Internet Services. Modifying passwords from either location changes them on the printer.

To modify folder passwords from the Properties tab:

1. In CentreWare Internet Services, click **Properties** > **Services**.
2. Click **Scan to Mailbox** > **Folders**.
3. Under Created Folder Operations, select the folder from the menu.
4. Under Created Folder Operations, type a new password for **Change Folder Password**.
5. Retype the password for Confirm Folder Password, then click **Save Password**.

To modify folder passwords from the Scan tab:

1. In CentreWare Internet Services, click **Scan**.
2. Select **Mailboxes**, then select the folder you want to modify.
3. Click **Modify Folder**.
4. Under Folder Operations, type a new password for **Change Folder Password**.
5. Retype the password for Confirm Folder Password, then click **Save Password**.

Monitoring Capacity

Capacity is the total space available for all mailboxes.

> Note: If the available space is less than 100 MB or the current percentage used is above 99 % , your system requires cleanup to remove old, unneeded mailboxes and files.

To view the current capacity usage:

1. In CentreWare Internet Services, click **Properties** > **Services**.
2. Click **Scan to Mailbox** > **Capacity**.
    - **Capacity**: The total amount of space available on the printer for scanned images.
    - **Used**: The space currently used to hold scanned images.

- **Available**: The space left for scanned images.
- **Percentage Used**: The amount of space used by scanned images as a percentage of the total space.

Scanning to an Email Address

The email feature allows you to scan a document and send it to an email address as an attachment.

For instructions explaining how to use this feature, see the *User Guide* at www.xerox.com/office/CQ9301_CQ9302_CQ9303docs .

Before you begin:

- Configure SMTP settings. Note the IP Address or host name of your SMTP server. For details, see Configure SMTP Server Settings on page 42.
- Create an email account for the printer. The printer uses this address as the default text in the From: field of the email.

Editing Default Scan Settings

1. In CentreWare Internet Services, click **Properties** > **Services**.
2. Click **Email** > **Defaults**.
3. Next to Scan to Email, click **Edit**.

   Note: You can change default email message options, scan options, file format options, and others. For details, click the **Help** link in CentreWare Internet Services.

Managing the Email Address Book

To manage the email address book, see Internet Fax and Email Address Book on page 177.

Workflow Scanning

Workflow Scanning allows you to scan an original document, distribute, and archive the scanned image file. The Workflow Scanning feature simplifies the task of scanning many multi-page documents and saving the scanned image files in one or more file locations.

To specify how and where scanned images are stored, create a template. You can create, manage, and store multiple templates in a template pool repository on a network server. Xerox® software, such as SMARTsend and ScanFlowStore, is designed to help you create and manage Workflow Scanning templates.

For instructions explaining how to use this feature, see the *User Guide* at www.xerox.com/office/CQ9301_CQ9302_CQ9303docs .

Before you begin:

- Ensure that Secure HTTP (SSL) is enabled.
- Ensure that a certificate is installed on the printer.

Configuring Workflow Scanning

1. In CentreWare Internet Services, click **Properties** > **Services**.
2. Click **Workflow Scanning** > **Scanning Web Services**.
3. Next to Scan Template Management, click **Settings**.
   The HTTP page opens.
4. On the HTTP page, enable **Scan Template Management**.
5. Click **Save** to apply the new settings or **Undo** to retain the previous settings.

Configuring File Repository Settings

A file repository is a network location where scanned images are stored. Configure the file repository settings before you create a template.

Your printer supports the following transfer protocols:

- FTP
- SFTP
- NetWare NCP
- SMB
- HTTP/HTTPS

  Note: HTTP/HTTPS scans to a Web server using a CGI script.

FTP or SFTP

Before you begin:

- Ensure that FTP or SFTP services are running on the server or computer being used to store scanned image files. Note the IP address or host name.
- Create a user account and password with read and write access for the printer to use to access the repository folder. Note the user name and password.
- Create a folder within the FTP or SFTP root. Note the directory path, user name, and password. This folder is your file repository.
- Test the connection. Log in to the file repository from a computer with the user name and password. Create a folder in the directory, then delete it. If you cannot create and delete the folder, check the user account access rights.

To configure file repository settings for FTP or SFTP:

1. In CentreWare Internet Services, click **Properties** > **Services**.
2. Click **Workflow Scanning** > **File Repository Setup**.
3. Click **Add New**.
4. In the Friendly Name field, type a name for the repository.
5. From the Default Repository Protocol drop-down menu, select **FTP** or **SFTP**.
6. Select the address type. Options for FTP include **IPv4**, **IPv6**, or **Host Name**. Options for SFTP include **IPv4**, or **Host Name**.
7. Type the appropriately formatted address and port number in the Default Repository Server field for the FTP or SFTP location.
8. In the Default Repository Document Path field, type the directory path of the folder beginning at the root of FTP or SFTP services. For example: /directoryname/foldername.
9. Under Default Repository Login Credentials, select one of the following:
   - **Authenticated User and Domain**: The printer uses the domain name, user name, and password of the authenticated users to access the server.
   - **Authenticated User**: The printer uses the user name and password of the authenticated user to access the server.
   - **Prompt at User Interface**: Users type the login name and password at the control panel. Select this option if you do not have an authentication server. Select this option if your document repository requires different login credentials than the ones required to access the printer.
   - **System**: The printer uses the information provided in the Login Name and Password fields to access the server.
10. Click **Save** to apply the new settings or **Undo** to retain the previous settings.

NetWare

Before you begin:

- Enable and configure NetWare protocol settings. For details, see NetWare on page 23.
- On the NetWare server, create a folder. This folder is your file repository. Note the server name, server volume, directory path, the NDS Context and Tree, if applicable.

- Create a user account and password with read and write access for the printer to use to access the repository folder. Note the user name and password.
- Test the connection. Log in to the file repository from a computer with the user name and password. Create a folder in the directory, then delete it. If you cannot create and delete the folder, check the user account access rights.

To configure file repository settings for NetWare:

1. In CentreWare Internet Services, click **Properties** > **Services**.
2. Click **Workflow Scanning** > **File Repository Setup**.
3. Click **Add New**.
4. Type a name for the repository in the Friendly Name field.
5. Select **NetWare** from the Default Repository Protocol drop-down menu.
6. Type the server name in the Default Repository Server field.
7. Type the server volume in the Server Volume field.
8. For NetWare 4.x, 5.x, 6x, and IPX only, type the tree and context in the NDS Tree and NDS Context fields.
9. In the Default Repository Document Path field, type the directory path of the folder.
10. Under Default Repository Login Credentials, select one of the following:
    - **Authenticated User and Domain**: The printer uses the domain name, user name, and password of the authenticated users to access the server.
    - **Authenticated User**: The printer uses the user name and password of the authenticated user to access the server.
    - **Prompt at User Interface**: Users type the login name and password at the control panel. Select this option if you do not have an authentication server. Select this option if your document repository requires different login credentials than the ones required to access the printer.
    - **System**: The printer uses the information provided in the Login Name and Password fields to access the server.
11. Type the Login Name and Password if the system directly accesses the file server.
12. Click **Save** to apply the new settings or **Undo** to retain the previous settings.

SMB

Before you begin:

- Ensure that SMB services are running on the server or computer where you want to store scanned image files. Note the IP address or host name.
- On the SMB server, create a shared folder. This folder is your file repository. Note the directory path, Share Name of the folder, and the Computer Name or Server Name.
- Create a user account and password with read and write access for the printer to use to access the repository folder. Note the user name and password.
- Test the connection by logging in to the file repository from a computer with the user name and password. Create a new folder in the directory, then delete it. If you cannot do this test, check the user account access rights.

To configure file repository settings for SMB:

1. In CentreWare Internet Services, click **Properties** > **Services**.
2. Click **Workflow Scanning** > **File Repository Setup**.
3. Click **Add New**.
4. Type a name for the repository in the Friendly Name field.
5. Select **SMB** from the Default Repository Protocol drop-down menu.
6. Select the address type. Options are **IPv4** or **Host Name**.
7. Type the appropriately formatted address and port number in the Default Repository Server field for the server where the file repository is located. The default port number is 139.
8. Type the share name in the Share field.
9. In the Default Repository Document Path field, type the directory path of the folder starting at the root of the shared folder. For example, If you have a folder named **scans** in the shared folder, type **\scans**.
10. Under Default Repository Login Credentials, select one of the following:
    - **Authenticated User and Domain**: The printer uses the domain name, user name, and password of the authenticated users to access the server.
    - **Authenticated User**: The printer uses the user name and password of the authenticated user to access the server.
    - **Prompt at User Interface**: Users type the login name and password at the control panel. Select this option if you do not have an authentication server. Select this option if your document repository requires different login credentials than the ones required to access the printer.
    - **System**: The printer uses the information provided in the Login Name and Password fields to access the server.
11. Type the Login Name and Password if the system directly accesses the file server.
12. Click **Save** to apply the new settings or **Undo** to retain the previous settings.

HTTP/HTTPS

Before you begin:

- Enable HTTP or Secure HTTP (SSL). Ensure that a certificate is installed on the printer if you are using SSL.
- Configure your Web server, and ensure that HTTP/HTTPS services are running. POST requests and scanned data are sent to the server and processed by a CGI script. Note the IP address or host name of the Web server.
- Create a user account and password for the printer on the Web server. Note the user name and password.
    - Create a /home directory for the printer.
    - Create a /bin directory in the home directory.
    - Copy an executable CGI script into the /bin directory. You can create your own script, or download a sample script. For details, see CGI Scripts on page 127. Note the path to the script. The script can be defined with script_name.extension or by path/script_name.extension.
- Create a folder with read and write permissions on the Web server, or alternate server. Note the directory path, user name, and password. This folder is your file repository.
- Test the connection by logging in to the home directory of the printer on the Web server. Send a POST request and file to the Web server. Check to see if the file is in the repository.

CGI Scripts

A CGI (Common Gateway Interface) script is a program on a Web server that is executed when the server receives a request from a browser. A CGI script is required to allow files to be transferred to your HTTP server from your printer.

When a document is scanned, the printer logs in to the Web server, sends a POST request along with the scanned file, then logs out. The CGI script handles the remaining details of file transfer.

To download a sample CGI script:

1. In CentreWare Internet Services, click **Properties** > **Services**.
2. Click **Workflow Scanning** > **File Repository Setup**.
3. Click **Add New**.
4. Select **HTTP** or **HTTPS** from the Protocol menu.
5. Under Script path and filename, click **Get Example Scripts**.
6. Select a script language supported by your Web server. Right-click and save the appropriate **.zip** or **.tgz** file to your computer.
7. Extract the downloaded file to the root of the Web services home directory.

Configuring File Repository Settings for HTTP/HTTPS

1. In CentreWare Internet Services, click **Properties** > **Services**.
2. Click **Workflow Scanning** > **File Repository Setup**.
3. Click **Add New**.
4. Type a name for the repository in the Friendly Name field.
5. Select **HTTP** or **HTTPS** from the Default Repository Protocol drop-down menu.
6. Select the address type. Options include **IPv4**, **IPv6**, or **Host Name**.
7. Type the appropriately formatted address and port number for the HTTP or HTTPS server.
8. For HTTPS, click **View Trusted SSL Certificates** to verify that a digital certificate is installed on the printer.
9. To validate the SSL certificate used for HTTPS, select **Validate Repository SSL Certificate**.
10. In the Script path and filename field, type the path to the CGI script starting at the root. For example: /directoryname/foldername. Click **Get Example Scripts** to download working example scripts.
11. Type the path to the location of the scan folder in Default Repository Document Path. For Web server directories, type the path starting at root. For example: \\directoryname\foldername.
12. Under Default Repository Login Credentials, select one of the following:
    - **Authenticated User and Domain**: The printer uses the domain name, user name, and password of the authenticated users to access the server.
    - **Authenticated User**: The printer uses the user name and password of the authenticated user to access the server.
    - **Prompt at User Interface**: Users type the login name and password at the control panel. Select this option if you do not have an authentication server. Select this option if your document repository requires different login credentials than the ones required to access the printer.

- **System**: The printer uses the information provided in the Login Name and Password fields to access the server.

13. Type the Login Name and Password if the system directly accesses the file server.
14. Click **Save** to apply the new settings or **Undo** to retain the previous settings.

Configuring the Default Template

Before you can use the Workflow scanning feature, create and edit a template. A template contains scan settings, and at least one destination for the scanned image files.

Configure the default template before you create a template. After the default template is configured, all new templates created inherit the default template settings and can then be edited as required.

The default template cannot be deleted.

1. In CentreWare Internet Services, click **Properties** > **Services**.
2. Click **Workflow Scanning** > **Default Template**.
3. Under Destination Services, select:
   - **File** to add File Destinations.
   - **Fax** to add Fax Destinations.
4. Add File Destinations, Fax Destinations, Document Management Fields, and configure other scanning options.

Adding a File Destination

1. Under File Destinations, click **Add**.
2. Select the required **Filing Policy** from the drop-down menu.
3. Click **Apply** to save the new settings or **Cancel** to return to the previous screen.

Adding a Fax Destination

1. Under Fax Destinations, click **Add**.
2. Type a fax number in the Add Fax Number field and click **Add**.
3. Under Delivery, select **Delayed Send** and type a time if you want to send the fax at a specific time.
4. Click **Apply** to save the new settings or **Cancel** to return to the previous screen.

Adding Document Management Fields

1. Under Document Management Fields, click **Add**.
2. Type a name for Field Name using up to **128** characters. The Field Name text is not shown at the control panel. Third-party software uses the name to access the Document Management information. This field is required.
3. To allow users to modify the Field Label field, select **Editable** next to User Editable. The Field Label identifies the purpose of this field to the user. Select **Not Editable** to prevent users from changing the value. The field does not appear on the control panel, and the text typed for the Default Value field is used.
4. If you selected Not Editable, type a Default Value. The Default Value is optional if you selected Editable.
5. Select **Require User Input** to prompt the user to type data for this document management field before scanning.
6. Select **Mask User Input** to prevent typed input from appearing at the control panel. Select **Record User Input in Job Log** to write any masked data to the Job Log file. Consider data security issues before selecting this option.
7. Validate Data Before Scanning options can be available if validation servers are configured for the printer.
8. Click **Apply** to save the new settings or **Cancel** to return to the previous screen.

Configuring Other Default Template Scanning Options

1. Click **Edit** to edit the following settings. For details, see the CentreWare Internet Services Help.
   - Workflow Scanning
   - Advanced Settings
   - Layout Adjustment
   - Filing Options
   - Filename Extension
   - Report Options
   - Workflow Scanning Image Settings
   - Compression Capability
2. To restore the Default Template to its original settings, click **Apply Factory Default Settings**. This action deletes any custom settings applied to the Default Template.

Configuring a Template to Create a Password-Protected PDF

You can edit a template to create an encrypted PDF file, and require users to protect the scanned PDF file with a password. When a user selects the scan template at the control panel, the printer prompts the user to create a password, or accept a default password. The password is required to open the PDF file.

1. Edit the Default Template on the Default Template page, or create a template on the Scan tab.
2. Add file destinations and edit settings as needed.
3. Under Document Management Fields, click **Add**.
4. Next to Field Name, type **xrx_pdf_pswd**.
5. Next to User Editable, select **Not Editable** to set the password, or select **Editable** to allow users to create a password.
6. If you selected Not Editable, type the password in the Default Value field.
7. If you selected Editable, do the following, if necessary:
    a. Type a password in the Default Value field to suggest a default password.
    b. Type text in the Field Label field to prompt users to enter a password. For example, type **Please type a password to protect your PDF file**.
    c. Select **Require User Input** to require users to provide a password.
    d. Select **Mask User Input** to hide characters that a user types at the control panel. If you do not select this option, the printer saves the password in the Job Log. To disable the Job Log, see below.
    e. If you do not want the PDF password to appear in the Job Log, which can compromise security, ensure that the **Record User Input to Job Log** check box is cleared.
8. Click **Apply**.
9. Under Filing options, click **Edit**.
10. Next to File Format, select **PDF**.

    Note: Do not select PDF/A. If you select PDF/A, a password-protected PDF is not created.

11. Click **Apply**.
12. If you allowed users to create a password, but did not select Mask User Input, disable the Job Log. Under Report Options, click **Edit**, then next to the Job Log, clear the **Enabled** check box.
13. Click **Apply**.

Configuring Workflow Scanning General Settings

1. In CentreWare Internet Services, click **Properties** > **Services**.
2. Click **Workflow Scanning** > **General**.
3. Under Confirmation Sheet, select when you want a confirmation sheet to print.
4. A template pool repository can store templates on the network and update the printer list of available templates. You can type the time you want this update to happen in the Refresh Start Time field. To update the template list now, click **Refresh Template List Now**.
5. If you are using a template pool repository, the printer must access the repository to access the network templates. Under Login Source, select **None** to allow the printer to access the repository without authenticating, or select one of the following:
    - **Authenticated User**: The printer uses the user name and password of the authenticated user to access the server.
    - **Prompt at User Interface**: Users type the login name and password at the control panel. Select this option if you do not have an authentication server. Select this option if your document repository requires different login credentials than the ones required to access the printer.

- **Prompt if Authenticated User Does Not Match Template Owner**: Users are prompted to authenticate when their credentials do not match the template owner.
- Under Job Log, select **User Name** or **Domain** if you want these names to display in the Job Log. If you have added Document Management Fields to a template, the Job Log is filed with scanned image files.

6. Click **Apply**.

See also:

Updating the List of Templates at the Control Panel on page 132

Adding Document Management Fields

Setting Scanned Image File Naming Conventions

1. In CentreWare Internet Services, click **Properties** > **Services**.
2. Click **Workflow Scanning** > **Custom File Naming**.
3. Under File Naming, select one of the following:
   - **Auto**: Type a prefix for the scanned image file name.
   - **Custom Naming**: Under Display, select the elements you want to use to build the file name. As you select display elements, they appear in the Position field. The display elements are:
     - **Date**
     - **Time**
     - **Job ID**
     - **User ID**
     - **Custom Text**: Type any custom text you that want to appear in the file name. For example, select the first Custom Text field and type an underscore (_). The underscore displays in the Position field. You can include up to four Custom Text strings in the file name.
     - **Position**: Click an element in the Position field. Use the Up and Down Arrow buttons to move the element into the correct position for the file name. The file name generated uses all the elements in the Position field, in order, from top to bottom.
   - **Advanced**: Type a string using variables to create the file name. For more information, see the CentreWare Internet Services Help.
4. Click **Apply** to save the new settings or **Undo** to retain the previous settings.

Configuring Template Pool Repository Settings

You can store Workflow Scanning templates on your network in a template pool repository. Workflow Scanning templates contain details about scan jobs that can be saved and reused for other scan jobs.

If you use a scanning management application, such as SMARTsend or ScanFlowStore, provide information about the server that hosts the templates on this page.

1. In CentreWare Internet Services, click **Properties** > **Services**.
2. Click **Workflow Scanning** > **Advanced** > **Template Pool Setup**.
3. Under Settings, select the desired protocol from the menu.
4. Type the required information for the protocol. Follow the same steps used for setting up a file repository for the protocol.

   Notes:

   - For details, view the online help in CentreWare Internet Services for the selected protocol.
   - The format for a directory path for FTP is /directory/directory, while the format for a directory path for SMB is \directory\directory.
5. Click **Apply** to save the new settings or **Undo** to retain the previous settings.

   Click **Default All** to reset settings to default values.

See also:

FTP on page 31

NetWare on page 23

HTTP on page 50

Updating the List of Templates at the Control Panel

If you are storing templates in a template pool repository, update the list of templates that displays at the control panel when you change them.

> Note: If you are not using a template pool repository, select **Update Now** to return a partial list of templates. This option does not update workstation-based templates created using the Xerox Scan Utility (XSU).

1. Press the **Services Home** button on the control panel, then touch the **Workflow Scanning** icon.
2. Touch the **Advanced Settings** tab.
3. Touch **Update Templates**.
4. Touch **Update Now** and touch **Confirm**.

Setting Template Display Settings for the Control Panel

1. In CentreWare Internet Services, click **Properties** > **Services**.
2. Click **Workflow Scanning** > **Display Settings**.
3. To specify the template that appears at the top of the list, under Templates, select the template and click **Update**.
4. To prevent users from using the Default Workflow Scanning template, under Default Template Display, select **Hide Default Template in the Templates list**.
5. To require users to select a template before they press the Start button, under Template Selection, select **User must select template before pressing Start button**.
6. Click **Apply** to save the new settings or **Undo** to retain the previous settings.

Configuring a Validation Server

Scan metadata entered at the printer control panel can be verified against a list of valid values by a validation server.

1. In CentreWare Internet Services, click **Properties** > **Services**.
2. Click **Workflow Scanning** > **Validation Servers**.
3. Click **Add**.
4. Select **HTTP** or **HTTPS**.
5. Under Protocol, select the address type. Options are **IPv4**, **IPv6**, or **Host Name**.
6. Type the appropriately formatted address and port number in the IP Address: Port field. The default port number is 80 for HTTP and 443 for HTTPS.
7. In the Path field, type the path on the server.

   Note: The format for a directory path for FTP is /directory/directory, while the format for a directory path for SMB is \directory\directory.

8. Type a Response Timeout between **5–100** seconds.
9. Click **Apply** to save the new settings or **Cancel** to return to the previous screen.

Scan to USB

You can insert a USB Flash Drive into the printer, scan a document, and store the scanned file on the USB drive.

Before you begin:

Enable USB ports. For details, see USB Port Security on page 97.

Enabling Scan to USB

1. In CentreWare Internet Services, click **Properties** > **Services**.
2. Click **Scan to USB** > **General**.
3. Under Enablement, select **Enabled**.
4. Click **Apply** to save the new settings or **Undo** to retain the previous settings.

Scanning to a User Home Folder

Use the Scan to Home feature to scan to their home folder, as defined in your LDAP directory, or to a shared network folder.

Configuring Scan to Home

1. In CentreWare Internet Services, click **Properties** > **Services**.
2. Click **Scan to Home** > **General**.
3. Under Status, click **Enabled**.
4. Type a Friendly Name using up to 127 characters. This name is the default description of the template that appears for users when scanning at the control panel.
5. Type a Template Name using up to 127 characters. This name is the default name that appears for users when scanning at the control panel. If you leave this field blank, the template default name is @S2HOME.
6. To scan to the home folder defined in an LDAP directory:
   a. Select **LDAP Query**.
   b. To check your LDAP mapping settings, click **LDAP Mapping for Home Directory**.
7. To scan to a shared network folder:
   a. Select **No LDAP Query**.
   b. In the Network Home Path field, type the complete network path of the external server where scanned image files are stored. Example: \\servername\foldername.
8. To create a subdirectory in the network home path, select **Automatically create Subdirectory** and type a name in the Subdirectory name field.
9. If your network home path includes folders named according to each user, for example \\servername\foldername\username, and you want to store scanned images in these folders, select **Append User Name to Path**. The user name is the name used when logging in at the control panel.
10. If you want to create individual folders for each user, select **Automatically Create User Name directory if one does not exist**. Example: \\servername\foldername\username.
11. Click **Apply** to save the new settings or **Undo** to retain the previous settings.

Configuring the Printer for the Xerox Scan Utility

The Xerox Scan Utility (XSU) allows you to scan directly to your computer and helps you manage and distribute scanned image files. Before you can scan, create a template in the utility. The template is saved on the printer. XSU installs when you install scan drivers.

For instructions explaining how to use this feature, see the *User Guide* at www.xerox.com/office/CQ9301_CQ9302_CQ9303docs .

Notes:

- Ensure Secure HTTP (SSL) is enabled, and a certificate is installed on the printer before you scan using XSU.
- Ensure SMB is enabled on your computer. SMB is not enabled by default on Macintosh computers.
- You cannot delete templates created in the XSU from the printer in CentreWare Internet Services. Templates must be deleted in XSU by the user who created the template.

Faxing

8

This chapter includes:

Embedded Fax

This section includes:

When you send a fax from the printer control panel, the document is scanned and transmitted to a fax machine using a dedicated telephone line. To use the embedded fax feature, ensure that your printer has access to a functioning telephone line and has a telephone number assigned to it.

Note: Not all printer models can send faxes.

Enabling Embedded Fax

1. At the printer control panel, press the **Machine Status** button, then touch the **Tools** tab.
2. Touch **Service Settings** > **Embedded Fax Settings**.
3. Touch **Fax Setup**.
4. Touch **Enable**.
5. Touch **Save**.

Configuring Embedded Fax Settings

1. At the printer control panel, press the **Machine Status** button, then touch the **Tools** tab.
2. Touch **Service Settings** > **Embedded Fax Settings**.
3. Touch **Line 1 Setup** or **Line 2 Setup**.
4. Touch **Fax Number**, then type the fax number using the touch screen keypad.

   Note: Customers in the Czech Republic are advised to contact their Xerox representative to perform this function.

5. Touch **Line Name**, then type a Line Name for the printer using the touch screen keyboard, and touch **Save**.
6. Under Options, select fax send and receive options:
   - **Send and Receive**
   - **Send Only**

- **Receive Only**

7. If allowed, under Dial Type, select your dialing method. If you have a tone line, select **Tone**. If you have a 10-pulse-per-second line, select **Pulse**. If in doubt, touch **Tone**.

   Notes:

   - Most countries use Tone dialing.
   - The Pulse/Tone feature is not available in some countries.

8. Click **Save**.

Setting Fax Defaults

Setting Incoming Fax Defaults

1. At the printer control panel, press the **Machine Status** button, then touch the **Tools** tab.
2. Touch **Service Settings** > **Embedded Fax Settings**.
3. Touch **Incoming Fax Defaults** to open the Incoming Fax Defaults window.

Enabling Auto Answer Delay

1. On the Incoming Fax Defaults window, touch **Auto Answer Delay**.
2. Touch the field under **Automatic Answer Delay** and use the left and right arrows to select a time between **0–15** seconds for answer delay.
3. Touch **Save**.

Enabling Ring Volume

1. On the Incoming Fax Defaults screen, touch **Ring Volume**.
2. If you want the printer to ring when a fax is received, touch **Enabled**.
3. Touch a value for Ring Volume. Options are **High**, **Medium**, and **Low**.
4. Touch **Save**.

Enabling or Disabling Junk Fax Prevention

Junk fax prevention disables printing of any faxes sent from fax telephone numbers not stored in the speed dial directory.

1. On the Incoming Fax Defaults screen, touch **Junk Fax Prevention**.
2. Select one of the following:
   - **Enabled**: Prevents faxes from printing when the fax telephone numbers are not stored in the speed dial directory.
   - **Disabled**: Allows faxes to print when the fax telephone numbers are not stored in the speed dial directory.
3. Touch **Save**.

Enabling or Disabling the Secure Fax Feature

To secure fax transmissions, enable the Secure Fax feature. When Secure Fax is enabled, a password is required before a fax can be printed or deleted.

1. On the Incoming Fax Defaults screen, touch **Secure Receive Settings**.
2. Under Secure Receive, touch **Enable** to turn on Secure Receive. The default passcode is 1111. To change the passcode, touch the code field, then type the new passcode using the touch screen keypad.
3. Touch **Disable** to turn off the Secure Receive feature.
4. Under Guest Access, touch **Enable** to allow guest users to turn this feature on or off. This option appears on the Tools tab, under **Device Settings** > **Fax Secure Receive Enablement**. Guest users cannot change the passcode.
5. Touch **Disable** to hide this feature on the Tools tab.
6. Touch **Save**.

Selecting Default Paper Settings

1. On the Incoming Fax Defaults window, touch **Paper Settings**.
2. Touch **Automatic** to direct the printer to print faxes on the paper size that most closely matches the attributes of the incoming fax. If the exact paper size is not available, the printer prints to the next best match and scales the fax to fit if needed.
3. To specify exact paper attributes for incoming faxes, touch **Manual**. If the specified paper size is not available, incoming faxes are held until resources are available.
4. Touch **Save**.

Setting Default Output Options

1. On the Incoming Fax Defaults screen, touch **Default Output Options**.
2. If your printer has a finisher with a stapler, and you want documents stapled, touch **Enable** under Staple.
3. If your printer has a finisher with a hole punch, and you want documents hole punched, touch **Enable** under Hole Punch.
4. To have faxes printed on both sides of the page, touch **Enable** under 2-Sided.
5. Touch **Save**.

Fax Mailboxes

You can store faxes locally in the printer or on a remote fax machine. You can use Remote Polling to print or access a stored fax. There are 200 available fax mailboxes.

Editing a Fax Mailbox

1. At the printer control panel, press the **Machine Status** button, then touch the **Tools** tab.
2. Touch **Service Settings** > **Embedded Fax Settings**.
3. Touch the down arrow to scroll.
4. Touch **Mailbox Setup**.
5. Touch a mailbox in the Mailbox List, then touch **Edit**.
6. Touch **Mailbox Name**, type a name for the mailbox up to **30** characters using the touch-screen keyboard, then touch **Save**.
7. To assign a passcode to the mailbox, touch **Mailbox Passcode**. Touch the **C** button to delete the default values, type a 4-digit passcode using the numeric keypad, then touch **Save**. Users must type this passcode when storing faxes to, or printing faxes from the mailbox.
8. To ensure that the user receives Fax Notifications, touch **Enable**, then touch **Save**.

Deleting a Fax Mailbox

1. At the printer control panel, press the **Machine Status** button, then touch the **Tools** tab.
2. Touch **Service Settings** > **Embedded Fax Settings**.
3. Touch the down arrow to scroll.
4. Touch **Mailbox Setup**.
5. Touch the assigned mailbox that you want to delete, then touch **Delete Mailbox**.

⚠ **CAUTION:** Touching **Delete Mailbox** deletes the mailbox and all documents it contains.

6. On the Delete Mailbox confirmation screen, touch **Confirm** to delete the mailbox, or **Close** to exit.
7. Touch **Close**.

Setting Transmission Defaults

1. At the printer control panel, press the **Machine Status** button, then touch the **Tools** tab.
2. Touch **Service Settings** > **Embedded Fax Settings**.
3. Touch the down arrow to scroll.
4. Touch **Transmission Defaults**.

Automatic Redial Setup

1. On the Transmission Defaults screen, touch **Automatic Redial Setup**.
2. Use the arrows to set:
   - **Redial Time Interval**: The time interval before the fax system redials after a failed transmission. Select between **1–25** minutes.
   - **Automatic Redial Attempts**: The number of attempts the fax system makes before rejecting the job. Select between **0–14** attempts.

Send Header Text

1. On the Transmission Defaults screen, touch **Send Header Text**.
2. Using the touch-screen keyboard, type up to **30** characters of text to include in the header for the fax.
3. To delete any text, touch **Clear Text**.
4. Touch **Save**.

Automatic Resend

1. On the Transmission Defaults screen, touch **Automatic Resend**.
2. Touch the field under Set number of resends and use the arrows to select the number of resends the printer attempts between **0–5**.
3. Select the condition that prompts the printer to resend jobs automatically. Options are:
   - **Failed pages without a cover page(s)**
   - **Whole Job without a cover page**
   - **Failed page(s) with a cover page**
   - **Whole job with a cover page**
4. Touch **Save**.

Batch Send

1. On the Transmission Defaults screen, touch **Batch Send**.
2. To enable Batch Send, touch **Enabled**.
3. Touch **Save**.

Audio Line Monitor

1. On the Transmission Defaults screen, touch **Audio Line Monitor**.
2. To enable Audio Line Monitor, touch **Enable**.
3. Next to Select Line Monitor Volume, touch the desired level. Options are **High**, **Medium**, and **Low**.
4. Next to Select Line Monitor Duration, touch the Up and Down arrows to select a value between **1–25** seconds that the printer monitors the line.
5. Touch **Save**.

Fax Reports

You can configure three different reports:

- Activity Report
- Confirmation Report
- Broadcast and Multipoll Report

Setting Up Fax Reports

1. At the printer control panel, press the **Machine Status** button, then touch the **Tools** tab.
2. Touch **Service Settings** > **Embedded Fax Settings**.
3. Touch **Setup Fax Reports**. Touch the arrows to scroll if necessary.
4. Touch **Activity Report**, then touch an option:
   - **Auto Print** to always print an activity report.
   - **Off** to never print an activity report.
5. Touch **Save**.
6. Touch **Confirmation Report**, then touch an option:
   - **Always Print** prints a confirmation report every time.
   - **Off** never prints a confirmation report.
   - **Print On Error** prints a confirmation report only when a fax transmission error occurs.
7. Touch **Print Options** to specify thumbnail image printing options:
   - Touch **Reduced Image** to print a smaller thumbnail image of the first page of the fax on the confirmation report.
   - Touch **Cropped Image** to print a larger thumbnail image of the first page of the fax on the confirmation report.
   - Touch **No Image** if you do not want to print a thumbnail image of the first page of the fax on the confirmation report.
8. Touch **Save** to save and exit the Print Options screen.
9. Touch **Save**.
10. Touch **Broadcast & Multipoll Report**, then touch one of the following options:
    - **Always Print** prints a confirmation report every time.
    - **Off** never prints a confirmation report.
    - **Print On Error** prints a confirmation report only when a fax transmission error occurs.
11. Touch **Save**.

Printing a Fax Report

You can print the following fax reports from the printer control panel:

- Activity Report
- Protocol Report
- Dial Directory Report
- Group Directory Report
- Options Report
- Pending Jobs Report

To print a fax report:

1. At the printer control panel, press the **Machine Status** button, then touch the **Tools** tab.
2. Touch **Service Settings** > **Embedded Fax Settings**.
3. Touch **Print Fax Reports**, then touch the arrows to scroll if needed.
4. Touch the desired report, then touch **Print Now**.
5. Touch **Close**, then log out.

Deleting Sent Fax Jobs from Memory

1. At the printer control panel, press the **Job Status** button.
2. Touch the down arrow, then touch **Scan Jobs and Fax Sent Jobs**.
3. Touch the pending fax in the list.
4. Touch **Delete**.

Fax Forwarding

You can configure the printer to forward incoming faxes to email or file destinations by creating a Fax Forward Rule.

Creating a Fax Forward Rule

1. In CentreWare Internet Services, click **Properties** > **Services**.
2. Click **Embedded Fax** > **Fax Forward**.
3. Next to a Rule Name, click **Edit**.
4. To base the new rule on an existing rule, next to Based on Rule, select a rule from the menu.
5. Next to Rule Name, type a name for the rule.
6. Select a File Format Type from the menu.
7. Next to Print Local Copy, select **Always** to print all incoming faxes. Select **On Error Only** to print a copy only if the forwarded fax transmission fails.
8. To forward to an email address, select the check box next to Email. The Forward to Email fields activate.
9. To forward to a file location, select the check box next to SMB Protocol. The Forward to File Destination activates.
10. Click **Save**.

Adding an Email Address to a Fax Forward Rule

1. Type the email addresses of the recipients in the Address fields.
2. Type the following information:
   - From Address
   - From Name
   - Subject

3. The default Attachment Name is **Fax**. To customize the name of the attachment, click **Customize**.
   a. Under Display, select the check boxes next to Date or Time to add the date or time to the file name.
   b. Under Position, select an item, and click the arrows to arrange the items as you want them to appear in the file name.
   c. Click **Save** to apply the new settings or **Cancel** to return to the previous screen.
4. Type the following information:
   - **Message**: This text is included in the body of the email. The default text alerts the recipient that a forwarded fax document is attached to the email.
   - **Signature**: This text is included in the body of the email after the Message.
5. Click **Save**.

Adding a File Destination to a Fax Forward Rule

1. Select **IPv4 Address** or **Host Name**, and type the address or host name.
2. Type the following information:
   - Share
   - Document Path
   - Login Name
   - Password
   - Retype Password
3. To update an existing password, select the check box next to Select to save the new password.
4. The default File Name is **Doc**. To customize the name of the file, click **Customize**.
   a. Under Display, select the check boxes next to Date or Time to add the date or time to the file name.
   b. Under Position, select an item, and click the arrows to arrange the items as you want them to appear in the file name.
   c. Click **Save** to apply the new settings or **Cancel** to return to the previous screen.
5. To send an email confirmation when file transfer is complete, select **Email Notification (without Attachment)**, and type the email address in the Notification Address field.
6. Click **Save**.

Fax Polling

Fax Polling allows you to store a fax document on the printer and make it available for other fax machines to poll. You can also retrieve faxes stored on other fax machines.

> Note: Both printers must have the Fax Polling feature.

Defining Mailbox and Polling Policies

1. At the printer control panel, press the **Machine Status** button, then touch the **Tools** tab.
2. Touch **Service Settings** > **Embedded Fax Settings**.
3. Touch the down arrow to scroll.
4. Touch **Mailbox & Polling Policies**.
5. Select an option for retaining Received Documents:
   - Touch **Delete On Print** to delete the file immediately after printing.
   - Touch **Keep 1-72 hours**, then touch the number of hours between **1–72** to retain the files before deleting them.
   - Touch **Keep Forever** to keep files on the printer until you manually delete them.
6. Touch **Stored Documents**.
   - Touch **Delete On Poll** to delete the file immediately after polling.
   - Touch **Keep 1-72 hours**, then touch the number of hours between **1–72** to retain polled documents before deleting them.
   - Touch **Keep Forever** to keep polled files on the printer until you manually delete them.

   Note: The Keep Forever option is memory intensive and requires you to manually delete files to maintain printer performance. If you are unsure, select **Keep 1-72 hours**, then select **24 hours**.

For instructions explaining how to use this feature, see the *User Guide* at www.xerox.com/office/CQ9301_CQ9302_CQ9303docs .

Server Fax

Server Fax allows you to send a fax over a network to a fax server. The fax server then sends the fax to a fax machine over a phone line.

Before you can send a server fax, configure a fax filing repository, or filing location. The fax server retrieves the documents from the filing location and transmits them over the telephone network. You can also print a transmission report.

> Note: Not all printer models support this feature.

Configuring a Server Fax Filing Repository

Before you can send a server fax, configure fax repository settings. Once configured, the printer transfers faxed images to the repository. The fax server then sends the fax to its destination over the phone line.

You can set up a repository that uses one of the following protocols:

- FTP
- SFTP
- SMB
- HTTP/HTTPS: A Web server using a CGI script.
- SMTP: A mail server.
- NetWare

Configuring a Fax Repository Using FTP or SFTP

Before you begin:

- Ensure that FTP or SFTP services are running on the server or computer where images faxed by the printer are stored. Note the IP address or host name.
- Create a user account and password for the printer. When the Server Fax feature is used, the printer logs in using the account, transfers the file to the server or computer and logs out. Note the user account and password.
- Create a directory within the FTP or SFTP root to be used as a fax repository. Note the directory path.

To configure fax repository settings using FTP or SFTP:

1. In CentreWare Internet Services, click **Properties** > **Services**.
2. Click **Server Fax** > **Fax Repository Setup**.
3. Click **Add New**.
4. In the Friendly Name field, type a name for the repository.
5. From the Default Repository Protocol drop-down menu, select **FTP** or **SFTP**.
6. Select the address type. Options for FTP include **IPv4**, **IPv6**, or **Host Name**. Options for SFTP include **IPv4**, or **Host Name**.
7. Type the appropriately formatted address and port number in the Default Repository Server field for the FTP or SFTP location.
8. In the Default Repository Document Path field, type the directory path of the folder beginning at the root of FTP or SFTP services. For example: /directoryname/foldername.
9. Under Default Repository Login Credentials, select one of the following:
   - **Authenticated User and Domain**: The printer uses the domain name, user name, and password of the authenticated users to access the server.
   - **Authenticated User**: The printer uses the user name and password of the authenticated user to access the server.
   - **Prompt at User Interface**: Users type the login name and password at the control panel. Select this option if you do not have an authentication server. Select this option if your document repository requires different login credentials than the ones required to access the printer.
   - **System**: The printer uses the information provided in the Login Name and Password fields to access the server.
10. Click **Save** to apply the new settings or **Undo** to retain the previous settings.

Configuring a Fax Repository Using SMB

Before you begin:

- Create a shared folder to be used as a fax repository. Note the Share Name of the folder and the Computer Name or Server Name.
- Create a user account and password for the printer with full access rights to the fax repository. Note the user account and password.

1. In CentreWare Internet Services, click **Properties** > **Services**.
2. Click **Server Fax** > **Fax Repository Setup**.
3. Click **Add New**.
4. Type a name for the repository in the Friendly Name field.
5. Select **SMB** from the Default Repository Protocol drop-down menu.
6. Select the address type. Options are **IPv4** or **Host Name**.
7. Type the appropriately formatted address and port number in the Default Repository Server field for the server where the file repository is located. The default port number is 139.
8. Type the share name in the Share field.
9. In the Default Repository Document Path field, type the directory path of the folder starting at the root of the shared folder. For example, If you have a folder named **scans** in the shared folder, type **\scans**.
10. Under Default Repository Login Credentials, select one of the following:
    - **Authenticated User and Domain**: The printer uses the domain name, user name, and password of the authenticated users to access the server.
    - **Authenticated User**: The printer uses the user name and password of the authenticated user to access the server.
    - **Prompt at User Interface**: Users type the login name and password at the control panel. Select this option if you do not have an authentication server. Select this option if your document repository requires different login credentials than the ones required to access the printer.
    - **System**: The printer uses the information provided in the Login Name and Password fields to access the server.
11. Type the Login Name and Password if the system directly accesses the file server.
12. Click **Save** to apply the new settings or **Undo** to retain the previous settings.

Configuring a Fax Repository Using HTTP/HTTPS

Before you begin:

- Ensure that Web services are installed on the server where you want to store scanned images. Examples of Web servers include: Microsoft Internet Information Services (IIS) and Apache. Note the IP address or host name of the server.
- For HTTPS, ensure that your Web server is installed with a secure certificate.
- Create a user account and password for the printer. When a document is scanned, the printer logs in using the account, transfers the file to the server or workstation and logs out. Note the user account and password details.
- Create a directory on the HTTP/HTTPS server to be used as a scan filing location (repository). Note the directory path.
- Note any script that is required to be run.

1. In CentreWare Internet Services, click **Properties** > **Services**.
2. Click **Server Fax** > **Fax Repository Setup**.
3. Click **Add New**.
4. Type a name for the repository in the Friendly Name field.
5. Select **HTTP** or **HTTPS** from the Default Repository Protocol drop-down menu.
6. Select the address type. Options include **IPv4**, **IPv6**, or **Host Name**.
7. Type the appropriately formatted address and port number for the HTTP or HTTPS server.
8. For HTTPS, click **View Trusted SSL Certificates** to verify that a digital certificate is installed on the printer.
9. To validate the SSL certificate used for HTTPS, select **Validate Repository SSL Certificate**.
10. In the Script path and filename field, type the path to the CGI script starting at the root. For example: /directoryname/foldername. Click **Get Example Scripts** to download working example scripts.
11. Type the path to the location of the scan folder in Default Repository Document Path. For Web server directories, type the path starting at root. For example: \\directoryname\foldername.
12. Under Default Repository Login Credentials, select one of the following:
    - **Authenticated User and Domain**: The printer uses the domain name, user name, and password of the authenticated users to access the server.
    - **Authenticated User**: The printer uses the user name and password of the authenticated user to access the server.
    - **Prompt at User Interface**: Users type the login name and password at the control panel. Select this option if you do not have an authentication server. Select this option if your document repository requires different login credentials than the ones required to access the printer.
    - **System**: The printer uses the information provided in the Login Name and Password fields to access the server.
13. Type the Login Name and Password if the system directly accesses the file server.
14. Click **Save** to apply the new settings or **Undo** to retain the previous settings.

Configuring a Fax Repository Using SMTP

1. In CentreWare Internet Services, click **Properties** > **Services**.
2. Click **Server Fax** > **Fax Repository Setup**.
3. Select **SMTP** from the Protocol menu.
4. Type the domain name of your SMTP server in the **Domain Name** field.
5. In the Default "From:" Address field, type the address you want to display automatically on the fax.
6. To enable email security, select **Enable**.
7. Click **Apply** to save the new settings or **Undo** to retain the previous settings.

Configuring a Fax Repository Using Netware

Before you begin:

Enable and configure Netware settings. For details, see NetWare on page 23.

1. In CentreWare Internet Services, click **Properties** > **Services**.
2. Click **Server Fax** > **Fax Repository Setup**.
3. Select **NetWare** from the Protocol menu.
4. Type the Repository Server, Server Volume, NDS Tree, NDS Context, and Document Path in the provided fields.
5. Under Login Credentials to Access the Destination, select one of the following:
   - **Authenticated User and Domain**: The printer uses the domain name, user name, and password of the authenticated users to access the server.
   - **Authenticated User**: The printer uses the user name and password of the authenticated user to access the server.
   - **Prompt at User Interface**: Users type the login name and password at the control panel. Select this option if you do not have an authentication server. Select this option if your document repository requires different login credentials than the ones required to access the printer.
   - **System**: The printer uses the information provided in the Login Name and Password fields to access the server.
6. Type the Login Name and Password if the system directly accesses the file server.
7. Click **Apply** to save the new settings or **Undo** to retain the previous settings.

Configuring Server Fax General Settings

1. In CentreWare Internet Services, click **Properties** > **Services**.
2. Click **Server Fax** > **Defaults**.
3. Under General, click **Edit**.
4. Select the **User Name** and **Domain** fields if you want these to display on the Job Log. The Job Log is filed in the fax repository with the fax job.
5. To print a Confirmation Sheet after every Server Fax job, select **On** from the menu. The Confirmation Sheet specifies the success or failure of the Server Fax job. If the fax is successful, the location of the document on the fax server is also specified.
6. Click **Save** to apply the new settings or **Undo** to retain the previous settings.

Configuring Server Fax Settings

1. In CentreWare Internet Services, click **Properties** > **Services**.
2. Click **Server Fax** > **Defaults**.
3. Under Server Fax, click **Edit**.
4. Set the desired parameters.
5. Click **Apply** to save the new settings or **Undo** to retain the previous settings.

Configuring Server Fax Image Quality Settings

1. In CentreWare Internet Services, click **Properties** > **Services**.
2. Click **Server Fax** > **Defaults**.
3. Under Image Quality, click **Edit**.
4. Set the desired parameters.
5. Click **Apply** to save the new settings or **Undo** to retain the previous settings.

Configuring Fax Settings Layout Adjustment

1. Under Layout Adjustment, click **Edit**.
2. Set the desired parameters.
3. Click **Apply** to save the new settings or **Undo** to retain the previous settings.

Configuring Server Fax Filing Options

1. In CentreWare Internet Services, click **Properties** > **Services**.
2. Click **Server Fax** > **Defaults**.
3. Under Filing Options, click **Edit**.
4. Under Delay Start, click **Specific Time** to adjust the delay start setting.
5. Click **Apply** to save the new settings or **Undo** to retain the previous settings.

Internet Fax

Internet Fax allows you to scan documents at the control panel, send them to destination email addresses, or receive and print emails with attachments. You can also print a transmission report. A telephone line connection is not required.

Configuring Default Internet Fax Settings

Before you begin:

- Create an email address for the printer if you want it to receive Internet faxes.
- Configure POP3 settings. For details, see POP3 on page 52.

  Note: Enter a domain name before you enable Internet Fax.

Configuring Internet Fax General Settings

1. In CentreWare Internet Services, click **Properties** > **Services**.
2. Click **Internet Fax** > **Defaults**.
3. Under General, click **Edit**.
4. To have the printer print a report automatically after every 50 Internet Fax jobs, select **Enable** next to Activity Report.
5. Next to Delivery Confirmation Timeout, type the maximum number of hours between **0–72** that the printer attempts to confirm an Internet Fax job before the confirmation fails.
6. Type the subject text that you want to display in the Subject field of the email.
7. Type any text that you want to display as the first paragraph in the Message Body.
8. Select optional information fields to display in the body of the fax. Options include:
   - User information such as User Name and Email Address.
   - Attachment information, such as Number of Images attached and Attachment File Type.
   - Information about the printer, such as Device Name, Device Location, and other details.
9. In the Signature field, type any additional information that you would like included on any fax sent from the printer.
10. Next to Confirmation Sheet, select when you want a confirmation page to print. Select **On**, **Off**, or **Errors Only** from the menu.
11. Click **Save** to apply the new settings or **Undo** to retain the previous settings.

Configuring Internet Fax Advanced Settings

1. In CentreWare Internet Services, click **Properties** > **Services**.
2. Click **Internet Fax** > **Defaults**.
3. Under Advanced Settings, click **Edit**.
4. Set the desired parameters.
5. Click **Apply** to save the new settings or **Undo** to retain the previous settings.

Configuring Internet Fax Layout Adjustment

1. In CentreWare Internet Services, click **Properties** > **Services**.
2. Click **Internet Fax** > **Defaults**.
3. Under Layout Adjustment, click **Edit**.
4. Set the desired parameters.
5. Click **Apply** to save the new settings or **Undo** to retain the previous settings.

Configuring Internet Fax Filing Options

1. In CentreWare Internet Services, click **Properties** > **Services**.
2. Click **Internet Fax** > **Defaults**.
3. Under Filing Options, click **Edit**.
4. Select the desired file format. Options are **Multi-Page TIFF**, **PDF images**, or **PDF/A images**.
5. To print a report listing the delivery status for each recipient of the Internet Fax, select **Print Report** next to Acknowledgment Report.
6. Click **Apply** to save the new settings or **Undo** to retain the previous settings.

Configuring Internet Fax Image Settings

1. In CentreWare Internet Services, click **Properties** > **Services**.
2. Click **Internet Fax** > **Defaults**.
3. Under PDF & PDF/A Settings, select **Optimized for Fast Web Viewing** to optimize the structure of PDF and PDF/A files for faster Web viewing.
4. Under Searchable PDF & PDF/A Default, select **Searchable** to create searchable PDF documents.
5. Specify the language or select **Use Language Displayed on the Device User Interface**.
6. Select **Enabled (Flate Compression)** to enable text compression.
7. Click **Apply** to save the new settings or **Undo** to retain the previous settings.

Configuring Internet Fax Receive Settings

1. In CentreWare Internet Services, click **Properties** > **Services**.
2. Click **Internet Fax** > **Internet Receive Settings**.
3. Under Filter Options, select **Accept Email with no attachment** to filter out attachments.
4. Under Accept the following attachments, select what types of attachments are received.
5. Under Finishing Options, select the desired setting from the drop-down menu for **Stapling** and **2-Sided Printing**.
6. Under Receipt Options, select **Send Confirmation reply when requested (allow device to send MDN)** to send a Mail Delivery Notification (MDN) email to the requestor when the fax job completes.
7. To print a cover sheet with the requestor email message before printing the fax job, select **Print Cover Sheet with incoming Email messages**.
8. Click **Apply** to save the new settings or **Undo** to retain the previous settings.

Internet Fax Addresses

You can store Internet Fax email addresses in the internal address book of the printer. You can also configure the printer to reference a network LDAP directory.

LAN Fax

Local Area Network (LAN) Fax allows you to send faxes from the print driver on your computer to a fax machine over a telephone line.

For details about using or configuring LAN Fax, see the driver help.

> Note: Not all printer models support this feature.

Accounting 9

This chapter includes:

Xerox Standard Accounting

Xerox Standard Accounting (XSA) tracks the numbers of copy, print, scan, and fax jobs for each user. You can set limits to restrict the total number of jobs by type that a user can produce. You can then generate reports listing usage data for individual users and groups.

When XSA is enabled, users must log in to the printer before accessing services. They must also provide their account details in the print driver before printing documents from a computer.

Notes:

- If XSA is enabled, you cannot enable other accounting modes.
- Install drivers and enable accounting in the drivers for all user computers.

You can create a maximum of:

- 2499 unique XSA user IDs
- 500 General Accounts
- 499 Group Accounts

All user IDs must be assigned to one or more group accounts. XSA settings and account data are stored in the printer. Xerox recommends that you use the Cloning feature to back up settings. If XSA settings are lost or deleted, you can restore them using the cloning backup file. For details, see Cloning on page 176, on page 176.

Enabling Xerox® Standard Accounting

1. In CentreWare Internet Services, click **Properties** > **Accounting** > **Xerox Standard Accounting**.
2. Click **Enablement**.
3. Select an option:
   - **Enable tracking for all services**: The printer tracks Copies, Prints, Scans, and Faxes.
   - **Enable color tracking only**: The printer tracks color Copies and Prints.
   - **Custom**: Allows you to enable tracking for specific services.
4. If you selected Custom, select **Enabled** or **Color Tracking Only** next to the services you want to track.
5. Click **Save**.

General and Group Accounts

You can create a group account to track and limit the number of copies, prints, scans, and faxes for a group of users. The number of copies, prints, scans, and faxes of each user are tracked against the user account and the group account. You can limit the usage for each user.

You can create a general account to track the total usage for a group of users. The number of copies, prints, scans, and faxes of each user are not tracked against the user account. The usage is only tracked against the general account. You cannot specify usage limits for a general account.

If a user is associated with a group account and a general account, they can access the printer using the accounting code for either account. Individual copies, prints, scans, and faxes, are tracked against the user and group accounts if the user accesses the printer using the group account. If the user accesses the printer using a general account, the usage is only tracked against the general account and not the user account.

Creating an Account

1. In CentreWare Internet Services, click **Properties** > **Accounting** > **Xerox Standard Accounting**.
2. Click **Accounts**.
3. Click the **Group Accounts** tab or the **General Accounts** tab.
4. Type a unique Account ID number and a unique Account Name for the new group.
5. Click **Add Account**.

Editing, Viewing, or Deleting an Account

1. On the Accounts page, click **Group Accounts** or **General Accounts**.
2. To edit the account name, or assign users to an account, under Actions, click **Edit**.
   a. To assign users to the account, select the check box next to a user ID.
   b. To edit the Account Name, type a new name under Account Name.
   c. Click **Save**.
3. To view usage details for an account, under Actions, click **View Usage**.
4. To delete an account, in the table at the bottom of the page, select the check box next to the account and click **Delete Selected**.

Adding a New User and Setting Usage Limits

1. In CentreWare Internet Services, click **Properties** > **Accounting** > **Xerox Standard Accounting**.
2. Click **Users & Limits**.
3. Click **Add New User**.
4. Type a Friendly Name for the user. This name is associated with the user in the User Information Database.
5. Type a unique User ID for the new user. The user types this name to log in at the control panel.
6. Under Usage Limits, type the maximum number of impressions or sent images allowed for the user. The maximum number of impressions or images sent is 16,000,000. Cover sheets and banner pages count as impressions as do fax acknowledgment reports and scan confirmation reports.
   - **Color Impressions**
     - **Prints** includes all color print jobs and received Server Fax documents.
     - **Copies** includes all color copies.
   - **Black Impressions**
     - **Prints** includes all black and white print jobs and received Server Fax documents.
     - **Copies** includes all black and white copies.
   - **Scanned Images** includes documents sent over the network, including network scans, scans to email, server faxes, and Internet faxes.

- **Fax Images**
  - **Sent** includes faxed documents. The total number of documents is the number of faxed documents, including cover sheets, multiplied by the number of destinations. Documents sent using the Server Fax feature are not included.
  - **Black Faxed Impressions** includes received fax documents that are printed. Documents sent using the Server Fax feature are not included.

7. Click **Apply**.

Assigning Users to an Account

1. In CentreWare Internet Services, click **Properties** > **Accounting** > **Xerox Standard Accounting**.
2. Click **Users & Limits**.
3. Select the check box next to the User ID of the user that you want to add to an account.
4. Under Action, click **Access, Limits, & Accounts**.
5. Click the **Group Accounts** tab or the **General Accounts** tab.
6. Select the check box next to the User ID of the user that you want to add to an account.
7. Click **Apply**.

Maximum Usage Limits

Once a user reaches their maximum usage limit, they are no longer able to use that feature until the administrator resets their limit. When they log in to the printer, they are presented with a notification message that their limit has been reached for that feature.

Any impressions made after a user reaches their limit are subtracted from their limit once it is reset. If the user limit is reached before a print job is completed, an error report prints notifying the user that their limit has been reached. The job is deleted from the print queue, and any sheets remaining in the paper path finishes printing.

Resetting Usage Limits

1. In CentreWare Internet Services, click **Properties** > **Accounting** > **Xerox Standard Accounting**.
2. Click **Report and Reset**.
3. To reset all usage data to 0, click **Reset Usage Data**.

⚠ **CAUTION:** If you click Reset Usage Data, all XSA usage data is reset to zero.

4. Click **OK**.
5. To delete all user, group, and general accounts, click **Reset to Default**.

⚠ **CAUTION:** If you click Reset to Default, all XSA usage data, user, group, and general account records are permanently deleted from the printer.

6. Click **OK**.

Printing a Report

You can print a report that lists the number of impressions recorded for each user and each account.

To print a report:

1. In CentreWare Internet Services, click **Properties** > **Accounting** > **Xerox Standard Accounting**.
2. Click **Report and Reset**.
3. Click **Generate Report**.
4. Right-click the **Right-click to download** link and save the **.csv** file to your computer.

Network Accounting

Network Accounting allows you to manage printer usage with detailed cost analysis capabilities. Print, Scan, Fax, and Copy jobs are tracked at the printer and stored in a job log. All jobs require authentication of User ID and Account ID, which are logged with the job details in the job log. The user is prompted for accounting information when submitting a job to the printer.

The job log information can be compiled at the accounting server and formatted into reports.

Before you begin:

- Install and configure Xerox® certified network accounting software on your network. Refer to the manufacturer instructions for help.
- Test communication between the accounting server and the printer. Open a Web browser, type the IP Address of the printer in the address bar, then press **Enter**. The printer CentreWare Internet Services home page appears.
- Install print drivers on all user computers if you want to track print and LAN Fax jobs.

Enabling and Configuring Network Accounting

1. At the printer control panel, press the **Machine Status** button, then touch the **Tools** tab.
2. Touch **Accounting Settings**.
3. Touch **Accounting Mode**.
4. Touch **Network Accounting** to enable.
5. To customize the prompt that users see at the control panel, touch **Customize Prompts**, then select the required prompt option from the drop-down menu: **Display Prompt 1 and 2**, **Display Prompt 1 Only**, **Display Prompt 2 Only**, **Display No Prompts**. To set the prompt values:
    a. Touch **Prompt 1 Label**, type an ID between 1–32 characters, then touch **Save**.
    b. Touch **Prompt 2 Label**, type an ID between 1–32 characters, then touch **Save**.
    c. Touch **Prompt 1 Default Value**, type an ID between 1–32 characters, then touch **Save**.
    d. Touch **Prompt 2 Default Value**, type an ID between 1–32 characters, then touch **Save**.
    e. To prevent typed information from being displayed on the control panel, touch **Mask Entries**, then touch **Save**.
6. Touch **Code Entry Validation**, and select one of the following:
    a. Select **Enabled** to track copy, print, and scan usage information by User ID, Account ID, and resources used by each user account. Users are required to type a valid User ID and Account ID for every job.
    b. Select **Disabled** to allow the printer to accept both valid and invalid User and Account IDs. Disable code entry validation if you want to determine what the general usage baseline is for any particular printer before requiring authentication controls. Users are still required to type at least one character into the User ID and Account ID fields.
7. Touch **Save**, then touch **Save** again.
8. On your network accounting server, open the network accounting application.
9. Configure the application to define the destination for retrieval of data as the IP address or the fully qualified domain name of the printer.

Enabling Accounting in Print Drivers

Enabling Accounting in a Windows Print Driver

1. From the Start menu, select **Printers and Faxes**.
2. Right-click the printer in the list, and select **Properties** > **Configuration** > **Accounting**.
3. From the Accounting System menu, select **Xerox Standard Accounting or Auditron**, or **Xerox Network Accounting**.
4. Select **Always Prompt** to prompt users to type their User ID and Account ID each time they print. If you do not want users to log in, select **Do Not Prompt** and type the user information in the Default User ID and Default Account ID fields.Select **Mask User ID** and **Mask Account ID** to show characters as asterisks when an ID is entered.
5. Select **Remember Last Entered Codes** to show the last entered code when a user is prompted for their Account ID.
6. Select **Auxiliary Accounting Interface** if you are using XSA with an external accounting device.
7. To specify the default User ID and Account ID, type them in the Default User ID and Default Account ID fields, then select the default account type.
8. Click **OK**.
9. Click **OK** to exit.

Enabling Accounting in an Apple Macintosh Print Driver

Users must select this preset each time they print or send a LAN fax using the print driver.

1. Open a document and select **File**, then select **Print**.
2. Select the Xerox® printer.
3. Select **Accounting** from the drop-down menu.
4. Under Accounting System, select **Xerox Standard Accounting or Auditron**, or **Xerox Network Accounting**.
5. Select **Prompt for Every Job** if you want users to type their User ID and Account ID every time they print.
6. Select **Mask User ID** and **Mask Account ID** to show characters as asterisks when an ID is typed.
7. Select **Use Default Accounting Codes** if you want to specify the default User ID and Account ID. Type them in the Default User ID and Default Account ID fields, then select the default account type.
8. To use XSA with an external accounting device, select **Auxiliary Accounting Interface**.
9. To save your settings, click the **Presets** menu and select **Save As**.
10. Type a name for the preset.
11. Click **OK**.

Displaying Your Company Logo on the Blocking Screen

You can customize the blocking screen to display your company logo. The blocking screen appears on the printer touch screen when card reader authentication or an auxiliary accounting device is configured. The screen displays a message when a user attempts to access a restricted feature, reminding users to swipe an identification card to access the feature.

Displaying Your Company Logo on the Blocking Screen

1. In CentreWare Internet Services, click **Properties** > **Accounting** > **Auxiliary Access Device** > **Import Customer Logo**.
2. Click **Browse** or **Choose File**.
3. Select a **.png** file that is not larger than 300 x 200 pixels, and click **Open**.
4. Click **Import**.
5. Click **Reboot Machine**.

Administrator Tools

10

This chapter includes:

Monitoring Alerts and Status

The Description and Alerts page displays printer information, such as printer name and location, as well as a list of any current alerts. You can view alert information, such as the status code, description of the issue, and the suggested skill level required to resolve the problem.

To view alerts:

1. In CentreWare Internet Services, click **Status** > **Description & Alerts**.

   The Description and Alerts page appears.
2. Click **Refresh** to update the page.

Alert Notification

There are several ways to set the printer to send out notifications when alerts occur. Possible alert types include low supply status, paper supply status, and paper jams.

Email Alerts

You can define groups to receive email notifications when selected status alerts occur on the printer.

1. In CentreWare Internet Services, click **Properties** > **General Setup**.
2. Click **Alert Notification** > **Email Alerts**.
3. Under Recipient Group Addresses, select which group you want to enable and type up to five email addresses to receive selected alerts.
4. Under Recipient Group Preferences, for the group you created, select the type of alerts that cause email notifications to occur. You can set up to three separate groups to receive any combination of email alerts.
5. To view definitions of the alert types, click **(Glossary)** under Status Codes in the Recipient Group Preferences area.
6. In **"Reply to:" Email Address**, type the email address of the administrator or user designated to receive any replies sent by Alert Notification group members.
7. Type a number between **0–60** minutes for **Set jam timer for release of status to selected groups** to specify how long the printer waits after a jam is detected before it sends an email status message. The default time is 0 minutes.
8. Click **Apply** to save the new settings or **Undo** to retain the previous settings.

Local UI Alerts

You can specify when you want the printer to display a warning on the control panel if the printer scan disk memory is low. Low memory can cause the printer to slow down or lose jobs.

1. In CentreWare Internet Services, click **Properties** > **General Setup**.
2. Click **Alert Notification** > **Local UI Alerts**.
3. Under Scan Disk Memory Warning, select the estimated number of scanned pages that can be held in scan memory before a warning appears. Options include:
   - 10 scanned pages
   - 30 scanned pages
   - Custom: Type a number of pages between 0–75 before a notification is sent.

   Note: The higher number of pages selected, the more frequently the warnings appear.
4. Click **Apply** to save the new settings or **Undo** to retain the previous settings.

Low Supply Warning

You can set the printer to display warnings in the printer status area when supplies reach a designated low level.

1. In CentreWare Internet Services, click **Properties** > **General Setup**.
2. Click **Alert Notification** > **Low Supply Warning**.
3. From the menu under each supply, select when you want the printer to display an alert in the printer status region. The range is 0–20 days.
4. Click **Apply** to save the new settings or **Undo** to retain the previous settings.

   Notes:

   - You can view the status on the Description & Alerts page under Status.
   - To view current supplies status, click **Status** > **Supplies**.

Energy Saving Settings

Configuring Sleep Mode Settings at the Control Panel

1. At the printer control panel, press the **Machine Status** button, then touch the **Tools** tab.
2. Touch **Device Settings** > **General** > **Energy Saver**.
3. Touch an option:
   - **Intelligent Ready**: The printer wakes and sleeps based on previous usage.
   - **Job Activated**: The printer wakes when it detects activity.
   - **Scheduled**: The printer wakes and sleeps according to a schedule you specify.
4. Under Fast Resume, touch **On** to reduce the wake time. This option changes the default sleep and low-power timeout periods, and increases energy usage.
5. If you selected Scheduled as the Energy Saver Mode, touch **Scheduled Settings** to select the times that you want the printer to wake or sleep.
6. Touch a day of the week in the list.
7. Under Schedule Based On, touch **Activity** to allow the printer to wake on activity for that day. Touch **Time** to wake the printer at a certain time.
8. If you selected Time, touch **Warm Up Time**, and select the time that the printer wakes on that day. Touch **Energy Saver Time**, and select the time that the printer sleeps on that day.
9. Touch **Save**.

Setting the Date and Time

Setting the Date and Time in CentreWare Internet Services

1. In CentreWare Internet Services, click **Properties** > **General Setup**.
2. Click **Date and Time**.
3. Under Date and Time Setup, select:
   - **Automatic using NTP** to allow the NTP service to set the time automatically.
   - **Manual (NTP Disabled)** to set the date and time manually.
4. If you are using an NTP server, select the address type. Options are **IPv4 Address** or **Host Name**. Type the appropriately formatted address, alternate address, and port numbers. The default port number is 123.

   Note: Changes to these settings cause the printer to restart.
5. Select the date and time format, and type the date and time in the appropriate fields. Select the **Display 24 hour clock** check box to show the time in 24 hour format.
6. Under Time Zone, select your time zone from the drop-down menu.
7. Click **Apply**.

Setting the Date and Time at the Control Panel

1. At the printer control panel, press the **Machine Status** button, then touch the **Tools** tab.
2. Touch **Device Settings** > **General** > **Date & Time**.
3. To set the time zone, touch **Time Zone** and touch the arrows to adjust the time zone.
4. To set the date, touch **Date**, select a format and set the date.
5. To set the time, touch **Time** and set the time. Select **Display 24 hour clock** to use 24 hour format.
6. Touch **Save**.

Taking the Printer Offline

To prevent the printer from either sending or receiving jobs over the network at any given time, you can take the printer offline. Taking the printer offline allows you to perform printer maintenance without jobs being sent to the printer. When the printer is offline, any services, such as Workflow Scanning, are unavailable.

1. At the printer control panel, press the **Machine Status** button, then touch the **Tools** tab.
2. Touch **Network Settings**.
3. Touch **Online/Offline**.
4. Touch **Online** or **Offline**.
5. Touch **Close**.
6. Press the **Log In/Out** button, then touch **Logout** to exit the Tools pathway.

Restarting the Printer in CentreWare Internet Services

1. In CentreWare Internet Services, click **Status** > **Description & Alerts**.
2. At the bottom of the page, click **Reboot Machine**, then click **OK**.

   Notes:

   - If your printer is locked, type the system administrator user name and password to access the Properties tab. The administrator user name is **admin** and the default password is **1111**.
   - This procedure causes the printer to restart and be unavailable over the network for several minutes.

Restarting the Printer at the Control Panel

Using Software Resets to restart the printer is faster and wastes fewer consumables than powering the printer on and off. Restarting the printer can take up to five minutes during which time CentreWare Internet Services is not available.

1. At the printer control panel, press the **Machine Status** button, then touch the **Tools** tab.
2. Touch **Troubleshooting**.
3. Touch **Resets**.
4. Touch **Software Reset**.
5. Under Reset Options, select the type of reset you want:
   - **All Software**
   - **Network Software**
   - **Copy Software**
6. Touch **Reset**.

SMart eSolutions and Billing Information

SMart eSolutions

SMart eSolutions is a suite of features that simplifies printer ownership and administration. It provides free services to enable administration of metered billing and supplies replenishment plans for printers on a network.Before you can use SMart eSolutions, register the printer for SMart eSolutions. There are three ways to register the printer for SMart eSolutions:

- **Automatic registration**: Automatic registration is available as a standard feature on many printer models.
- **SMart eSolutions Windows Client**: The Windows client is an option for small and medium sized businesses. To download the Windows client, see www.xerox.com/smartesolutions .
- **CentreWare Web**: CentreWare Web is a browser-based software tool that installs, configures, manages, monitors, and reports on all network printers and multifunction printers regardless of manufacturer. It is suited for large enterprise businesses. For more information, see www.xerox.com/centrewareweb .

Once the software is installed, MeterAssistant automatically enables.

Note: SMart eSolutions is not available in all countries. See your Xerox representative for details.

Before you begin:

- Create an account on Xerox.com to receive your meter read information. To create an account, go to www.xerox.com/meterreads .
- Ensure that SNMP and TCP/IP are enabled.
- Ensure that the HTTP Proxy Server is configured.

Enabling SMart eSolutions

1. In CentreWare Internet Services, click **Properties** > **General Setup**.
2. Click **SMart eSolutions Setup**.
3. Under Enrollment, select **Enrolled**.
4. Under Daily Transmission Time, type the time of day that you want the printer to perform its daily communication with Xerox.
5. Click **Apply** to save the new settings or **Undo** to retain the previous settings.
6. To verify communication with the Xerox® server, click **Test Communication Now**. Under Communication Setup, a status message appears indicating if your printer is able to communicate with Xerox®.

   Note: If your network uses an HTTP Proxy Server, click **Configure** next to HTTP Proxy Server to configure the proxy settings manually.

MeterAssistant

MeterAssistant automatically submits meter reads to Xerox from network printers. This process eliminates the need to collect and report meter read information manually.

To view the last transmission of Billing Meter information for your printer:

1. In CentreWare Internet Services, click **Status** > **SMart eSolutions**.
2. Click **MeterAssistant®**.

   The number of impressions is listed in the table.

   Note: If the count is zero, no data has been transmitted to Xerox®.
3. Click **Edit** to enable Meter email alerts.

For details on setting up alerts, see Setting up Alert Notification on page 168.

Supplies Assistant

SuppliesAssistant™ proactively manages ink supplies for network equipment, and monitors actual usage.

To view the current supplies status:

1. In CentreWare Internet Services, click **Status** > **SMart eSolutions**.
2. Click **Supplies Assistant**.

   The printer supply list appears with the current **% Life Remaining** of each supply.

   Note: If the % Life Remaining is zero, no data has been transmitted to Xerox®.

Maintenance Assistant

Maintenance Assistant provides options for troubleshooting your printer. You can send detailed diagnostic information to Xerox®, start online troubleshooting sessions with Xerox®, and download usage information to your computer in **.csv** format.

1. In CentreWare Internet Services, click **Status** > **SMart eSolutions**.
2. Click **Maintenance Assistant**.
3. Click one of the following:
   - **Send Diagnostic Information to Xerox**
   - **Start an Online Troubleshooting Session at www.xerox.com**
   - **Download file to your computer**: Right-click and download the **UsageLog.csv** file to your computer.

View Usage and Billing Information

Usage Counters

The Usage Counters page displays the total number of pages printed or generated by the printer. You can see usage amounts for impressions made, sheets, images used, and images printed, copied, and faxed.

1. In CentreWare Internet Services, click **Status** > **Usage Counters**.

   The complete list of pages printed or generated by the printer appears.
2. Click **Refresh** to update the page.

Billing Information

The Billing Information page displays current readings for printer counters that are used for billing. You can view the number of impressions made in color or black and white, as well as the total number of impressions. The impression counts shown are used for billing.

1. In CentreWare Internet Services, click **Status** > **Billing Information**.

   The list of pages printed or created by the printer appears.
2. Click **Refresh** to update the page.

Cloning

Cloning allows you to save your current printer settings to a file to use as a backup and restore file for your printer. You can also use a clone file to copy your printer settings to other printers.

> Note: If you are using a clone file to copy your printer settings to another printer, both printers must be the same model. Both printers must also have the same version of software installed.

To determine the software version:

1. In CentreWare Internet Services, click **Properties** > **General Setup**.
2. Click **Configuration Report**.
3. Scroll down to **Software Versions** to verify the software information.

Creating a Clone File

1. In CentreWare Internet Services, click **Properties** > **General Setup**.
2. Click **Cloning**.
3. Under Create Clone File, select the features that you want to clone to other printers. All features are selected by default.
4. To view the specific parameters that can be cloned for any of the features, click **View Feature Details**.
5. Click **Clone**.

   The Cloning Instructions page appears.
6. Under Cloning Instructions, right-click **Cloning.dlm** to download the clone file.
7. Click **Save Link As** or **Save Target As** and select a name and the location to save the file. The default name for the file is **Cloning.dlm**. If you rename the file, use **.dlm** as the file extension.
8. Click **Save**.

Installing a Clone File

1. In CentreWare Internet Services, click **Status** > **Welcome**.
2. Click **I Have A Cloning File**.
3. Under Install Clone File, type the path and name of the clone file that you want to use or click **Browse** to locate the file.

   > Note: If View Feature Details is selected, the Install Clone File field does not appear. Click **Hide Feature Details** to see the Install Clone File field.
4. Click **Install**.

   > Note: This procedure causes the printer to restart and be unavailable over the network for several minutes.

Address Books

If your network is connected to an LDAP server, you can configure the printer to look up addresses from the LDAP directory. If you do not have an LDAP server, you can use the Fax Address Book and the Public Address Book. These address books store fax machine phone numbers and email addresses on the printer.

You can configure the printer to access both an LDAP directory and a Public Address Book. If both are configured, users are presented with the choice to use either address book.

Internet Fax and Email Address Book

An Internet Fax Address is the email address of an internet fax machine or service. Email addresses are stored in the Public Address book.

Defining Address Book Security

1. In CentreWare Internet Services, click **Address Book**.
2. Click **Access Rights**.
3. Select one of the following:
    - **System Administrators Only** to require users to log in as an administrator to edit the address book.
    - **Open to All Users** to allow anyone to edit the address book.
4. Click **Save**.

Editing the Public Address Book in CentreWare Internet Services

Adding a New Name

1. In CentreWare Internet Services, click **Address Book**.
2. On the Address Book page, click **Add New Name**.

    The Add New Name page displays.
3. Type a name using up to 253 characters with no special characters in the Friendly Name field.
4. Type the email address for the entry using standard email format.
5. Type the fax email address for the Internet Fax Address entry using the standard Internet fax address format.
6. Click **Save & New** to save the new file and prompt for the next entry.

    Click **Save & Close** to save the record and exit the window.
7. Click **Close** to discard the changes.

Deleting a Name

1. In CentreWare Internet Services, click **Address Book**.
2. Under Public Address Book, click **View All Names**.
3. Scroll to the entry you want to delete, then click **Delete**.
4. Click **OK** to delete or **Cancel** to exit.

Editing a Name

1. In CentreWare Internet Services, click **Address Book**.
2. Under Public Address Book, click **View All Names**.
3. Scroll to the entry you want to modify, then click **Edit**.
4. Type your changes in the Edit Names and Addresses fields.
5. Click **Save & Close** to confirm the delete or **Cancel**.

Deleting All Names

1. In CentreWare Internet Services, click **Address Book**.
2. Under Management, click **Delete All Names**.

   The Public Address Book dialog box appears.
3. Click **Delete All Names**.

Editing the Public Address Book as a .csv File

If you have many addresses, manage the list in a spreadsheet application, save it as a .csv file, and upload it to the printer.

Exporting an Address Book File

To make modifications or back up your current address book from your computer, you can export the file.

1. In CentreWare Internet Services, click **Address Book**.
2. Under Management, click **Export**.
3. In the File Download dialog box, click **Save**.
4. Select the location to save the file, then click **Save**.

Downloading a Sample .csv File

To back up your current address book or make modifications from your computer, you can export the file.

1. In CentreWare Internet Services, click **Address Book**.
2. Under Management, click **Download Sample**.
3. In the File Download dialog box, click **Save**.
4. Select the location to save the file, then click **Save**.

Importing

1. In CentreWare Internet Services, click **Address Book**.
2. Under Management, click **Import**.
3. Under Import Your Address Book File, type the path to your file, or click **Browse** to locate the file on an external computer.

   Notes:

   - The address book file must be in **.csv** format.
   - The printer recognizes the second row in the **.csv** file as the first data entry. The first row contains headings for the data in each column. The default column heading names are: Friendly Name, Email Address, Internet Fax Address.
4. Click **Next**.
5. Under Import Options, select the action you want to occur when the file imports:
   - **Add your new content to the existing Public Address Book**: This option merges your new file with the current file. No data is lost.
6. **Replace the existing Public Address Book with your new content**: All previously stored address book data is overwritten with the new data.

Fax Address Book

You can save fax machine phone numbers as speed dial entries at the control panel. For instructions explaining how to use this feature, see the *User Guide* at www.xerox.com/office/CQ9301_CQ9302_CQ9303docs .

LAN Fax Address Book

The LAN Fax feature has a separate directory for storing and managing addresses. For details about using or configuring the LAN Fax address book, see the driver help.

Font Management Utility

The CentreWare Font Management Utility allows you to manage fonts on one or more printers on your network. You can download the Xerox® CentreWare Font Management Utility on the Xerox® website at www.xerox.com/office/CQ9301_CQ9302_CQ9303drivers .

Use the utility to download soft fonts to your printer, such as your company branded fonts or unicode fonts to support multiple languages. You can then add, delete, or export the fonts to a file. You can add or delete printers in the utility printer list to display only those printers you want to manage.

Network Logs

Log files are text files of recent printer activity that are created and stored in the printer. Log files are used to monitor network activity or troubleshoot network problems. A Xerox customer support representative can interpret the encrypted format log files.

Downloading a Network Log Using a USB Flash Drive

1. In CentreWare Internet Services, click **Properties** > **General Setup**.
2. Touch **Network Settings** > **Network Logs**.
3. Touch **Enhanced**.

   Enhanced records a detailed list of network actions that have occurred on the printer. Only use Enhanced logging when instructed to do so by your Xerox® service or support technician as it can cause increased job processing times.

   The printer restarts.
4. Navigate back to the Network Logs screen.
5. Insert a USB memory stick in the USB port on the back of the printer, and touch **Download Enhanced Log File**. A confirmation message displays when file transfer is complete.
6. Touch **Basic** to disable Enhanced logging, and touch **Save**.
7. Remove the USB memory stick and touch **Restart**.

   The printer restarts.

Downloading a Network Log from CentreWare Internet Services

1. In CentreWare Internet Services, click **Properties** > **General Setup**.
2. Click **Network Logs**.
3. Under Information Level, select an option:
   - **Basic** records a minimum list of network actions that have occurred on the printer.
   - **Enhanced** records a detailed list of network actions that have occurred on the printer. Only use Enhanced logging when instructed to do so by your Xerox® service or support technician as it can cause increased job processing times.
4. Under Download Files > Additional Content, select the log types that you want to download.
5. Click **Start Download**.
6. Click **Download File Now** after the information processes.

   The File Download dialog box appears.
7. Select whether you want to Find or Save the file.
8. Click **Close** to return to the Network Logs page.

Customizing Printer Contact Information

The support page In CentreWare Internet Services displays contact information for service and supplies as well about the system administrator. You can customize this information to display your company contact information for printer users.

To add your own custom information:

1. In CentreWare Internet Services, click **Support**.
2. Click **Edit Settings**.
3. Update the fields with your information and click **Save**.

Updating the Printer Software

You can update your printer when Xerox® releases a new version of printer software or firmware.

Before you begin:

- Determine the current software version of your printer.
- Download the latest software update file in **.dlm** format from the Xerox® support website at www.xerox.com/office/CQ9301_CQ9302_CQ9303support .

To determine the software version:

1. In CentreWare Internet Services, click **Properties** > **General Setup**.
2. Click **Configuration Report**.
3. Scroll down to **Software Versions** to verify the software information.

Enabling Upgrades

1. In CentreWare Internet Services, click **Properties** > **General Setup**.
2. Click **Machine Software**.
3. Click **Upgrades**.
4. Under Upgrades, select **Enabled**.
5. Click **Apply**.

Manually Upgrading Printer Software

1. In CentreWare Internet Services, click **Properties** > **General Setup**.
2. Click **Machine Software**.
3. Click **Manual Upgrade**.
4. Under Manual Upgrade, click **Browse** to locate and select the software upgrade file in **.dlm** format.
5. Click **Open**.
6. Click **Install Software**.
   After the software file is submitted, the printer restarts.

   Note: CentreWare Internet Services is unavailable while the software is installing.
7. Check the configuration report to verify that the software has updated.

Manually Updating the Software Using a USB Flash Drive

1. Create a directory folder on your USB Flash Drive called **UPGRADE**.
2. Copy the software **.dlm** file to this directory.
3. Insert the USB Flash Drive into the USB host port of the printer.
   The software upgrade process begins.

4. When the software update completes, the printer restarts.

Configuring Automatic Updates

You can configure the printer to connect routinely to an FTP directory on your network to update printer software automatically. First, manually download the latest software file and copy it to the location on the FTP server. The printer retains all configured network settings and installed options after the software upgrade processes.

1. In CentreWare Internet Services, click **Properties** > **General Setup**.
2. Click **Machine Software** > **Auto Upgrade**.
3. Click **Upgrades**.
4. Under Upgrades, select **Enabled**.
5. Click **Apply**.
6. Click **Auto Upgrade** in the navigation pane.
7. Under Auto Upgrade, select **Enabled**.

   The Auto Upgrade page expands.
8. Under Refresh Start Time, select **Hourly** or **Daily**.

   If you select Daily, type the time in hours and minutes.
9. Under Protocol, select the address type. Options are **IPv4 Address**, **IPv6 Address**, or **Host Name**.
10. Type the appropriately formatted address and port number of the server where the upgrade software is located in the address field. The default port number is 21.
11. In the Directory Path field, type the full path to the software upgrade file in **.dlm** format located on the server.
12. Type the **Login Name** to access the server.
13. Type the password, then type the password again to verify.
14. Click **Apply**.

    Note: Software installation begins several minutes after the software is submitted to the printer. Once installation begins, CentreWare Internet Services is disabled. You can monitor the installation progress from the printer control panel.

11 Customization and Expansion

This chapter includes:

Xerox Extensible Interface Platform

Xerox Extensible Interface Platform® (EIP) allows independent software vendors and partners to develop personalized and customized document management solutions. These solutions can be integrated and accessed directly from the printer control panel. These solutions can leverage existing printer infrastructure and databases. Examples of applications include ScanFlow Store, Scan to PC Desktop, Equitrac Office, and others. For more information on EIP applications for your printer, contact your Xerox representative or see www.office.xerox.com/eip/enus.html on the Xerox® website.

Enabling Extensible Services

Before you begin:

Ensure that Secure HTTP (SSL) is enabled.

1. In CentreWare Internet Services, click **Properties** > **General Setup**.
2. Click **Extensible Services Setup**.
3. Under Browser Settings, select **Enable the Extensible Services Browser**.
4. Select **Verify server certificates** to check the certificates on the remote server.

   Note: If you allow the printer to verify server certificates, the EIP browser can display warning messages that the user can ignore.

5. Under Enable Extensible Services, select **Export password to Extensible Services** if your EIP application requires the user password. See your EIP application instructions for details.
6. Configure Proxy Server settings if necessary.
   a. Under Proxy Server, select **Manual Configuration** from the list.
   b. Select **Enabled** under HTTP, HTTPS, or HTTP.
   c. Select the type of address, **IPv4 Address**, **IPv6 Address**, or **Host Name** and type the address or host name in the provided field.
   d. Under Bypass Proxy Rules, type the required values, and separate them with commas.
7. Click **Apply** to save the new settings or **Undo** to retain the previous settings.

Auxiliary Interface Kit

An Auxiliary Interface Kit, or a Foreign Device Interface kit, is a third-party access and accounting device. These kits, such as a coin operated printer accessory or a card reader, can be attached to the printer. Installation instructions are included with the Foreign Device Interface Kit. After the kit is installed, enable Auxiliary Access at the control panel.

1. At the printer control panel, press the **Machine Status** button, then touch the **Tools** tab.
2. Touch **Accounting Settings**.
3. Touch **Accounting Mode** > **Auxiliary Access**.
4. Touch **Auxiliary Device Type** and select your printer type.
5. Touch **Save** twice.

See also:

Accounting on page 157

Local Authentication on page 59

Driver Download Link

The driver installation link appears on the CentreWare Internet Services Welcome, Print, and Support pages. This link goes to the default driver and downloads page for your printer on the Xerox Support website. You can hide or customize this link to go to a location on your network where you post driver installation files for users.

Customizing or Hiding the Driver Download Link

1. In CentreWare Internet Services, click **Properties** > **General Setup**.
2. Click **Configure Driver Links**.
3. Under Display Option, select **Hide Link** to hide the link.
4. Under Software Links, select **Custom Link** and type a link to direct users to the location for drivers on your network.
5. Click **Apply** to save the new settings or **Undo** to retain the previous settings.

Audit Log Event Identification Numbers

A

This appendix includes:

Audit Log Event Identification Numbers

Event Identification Number	Description
1	System startup
2	System shutdown
3	Manual ODIO (On-Demand Image Overwrite) Standard started
4	Manual ODIO Standard complete
5	Print job
6	Network scan job
7	Server fax job
8	IFAX
9	Email job
10	Audit Log Disabled
11	Audit Log Enabled
12	Copy
13	Embedded fax
14	LAN Fax Job
15	Data Encryption enabled
16	Manual ODIO Full started
17	Manual ODIO Full complete
18	Data Encryption disabled
20	Scan to Mailbox job
21	Delete File/Dir
22	USB Flash Drive
23	Scan to Home
24	Scan to Home job
26	PagePack® login
27	PostScript Passwords
29	Network User Login
30	SA login
31	User Login
32	Service Login Diagnostics
33	Audit log download
34	IIO feature status
35	SA pin changed

36	Audit log Transfer
37	SSL
38	X509 certificate
39	IPsec
40	SNMPv3
41	IP Filtering Rules
42	Network Authentication (Enable/disable/configure)
43	Device clock
44	SW upgrade
45	Cloning
46	Scan Metadata Validation
47	Xerox® Secure Authentication (Enable/disable/configure)
48	Service login copy mode
49	Smartcard (CAC/PIV) access
50	Process terminated
51	ODIO scheduled
53	CPSR Backup
54	CPSR Restore
55	System Administrator Tools admin access
58	Session timer log out
59	Feature Access Control (Enable/disable/configure)
60	Device clock NTP (Enable/disable)
61	Grant/revoke admin rights
62	Smartcard (CAC/PIV) (Enable/disable/configure)
63	IPv6 (Enable/disable/configure)
64	802.1X (Enable/disable/configure)
65	Abnormal system termination
66	Local authentication (Enable/disable)
67	Web User Interface authentication (Enable network or local)
68	FIPS 140 (Enable/disable/configure)
69	Xerox® Secure Access login
106	SA PIN reset