Xerox® ColorQube® 8580 / 8880
Color Printer
Imprimante couleur
System Administrator Guide
Guide de l'administrateur système

Contents

Contents

Contents

Introduction

1

This chapter includes:

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 configure and manage your printer on a network.

Note: Network features are not available when you are connected over USB.

Configuration Overview

When you configure the printer for the first time, complete the following tasks. For details, see Initial Setup on page 11, on page 13.

1. Ensure that your printer is connected physically to your network.
2. Confirm that your network recognizes your printer. By default, the printer receives an IP address from a DHCP server over a TCP/IP network. If you have a different type of network or want to assign a static IP address, see IP on page 23.
3. To view the printer IPv4 or IPv6 address, print a Configuration Page. For details, see Configuration Page on page 13
4. To access most configuration settings for the printer, use CentreWare Internet Services.

   Note: You can access most configuration settings in CentreWare Internet Services on the Properties tab.

5. Create a host name for the printer. For details, see DNS/WINS on page 27.
6. Configure network protocols. For details, see Network Connectivity on page 21.
7. Configure security features and set administrative accounts. For details, see Security on page 47, on page 49.
8. Configure job accounting. For details, see Job Accounting on page 53.

More Information

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

Resource	Location
Installation Guide	Packaged with the printer.
Quick Use Guide	Packaged with the printer.
Other documentation for your printer	- Xerox® ColorQube 8580 Color Printer: www.xerox.com/office/CQ8580docs - Xerox® ColorQube 8880 Color Printer: www.xerox.com/office/CQ8880docs
Recommended Media List	United States: - www.xerox.com/printer-supplies/recommended-paper/enus European Union: - www.xerox.com/europaper
Technical support information for your printer; including online technical support, Online Support Assistant, and driver downloads.	- Xerox® ColorQube 8580 Color Printer: www.xerox.com/office/CQ8580support - Xerox® ColorQube 8880 Color Printer: www.xerox.com/office/CQ8880support
PhaserSMART Technical Support automatically diagnoses problems on your network printer and proposes solutions.	www.phasersmart.com
Information about menus or error messages	Press the control panel Help (**?**) button.
Information Pages	Print from the control panel or from CentreWare Internet Services.
CentreWare Internet Services documentation	To access CentreWare Internet Services, open a Web browser, then type the IP address for your printer. In CentreWare Internet Services, click **Help**.
Order supplies for your printer	- Xerox® ColorQube 8580 Color Printer: www.xerox.com/office/CQ8580supplies - Xerox® ColorQube 8880 Color Printer: www.xerox.com/office/CQ8880supplies
A resource for tools and information, including 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 to the Network

Use a Category 5 or better Ethernet cable to connect the printer to the network. An Ethernet network is used for one or more computers and supports many printers and systems simultaneously. An Ethernet connection provides direct access to printer settings using CentreWare Internet Services.

To connect the printer:

1. Connect the power cord to the printer, and plug the cord into an electrical outlet.
2. Connect one end of a Category 5 or better Ethernet cable to the Ethernet port on the printer. Connect the other end of the Ethernet cable to a correctly configured network port on a hub or router.
3. Turn on the printer.

Initial Setup at the Control Panel

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 23. If the printer does not detect a DHCP server, then it uses an IPv4 self-assigned address.

> Note: You can view the printer IP address on the printer control panel or on the Configuration Page.

Viewing the Printer IP Address

You can view the printer IP address on the printer control panel or on the Configuration Page.

To view the IP address on the control panel:
1. At the printer control panel, to navigate to the Information Menu, use the arrows, then press **OK**.
2. Navigate to Printer Identification, then press **OK**.
3. To view the IP address, navigate to TCP/IPv4 Address or TCP/IPv6 Address.

Printing the Configuration Page

The configuration page lists printer information such as default settings, installed options, network settings including IP address, and font settings.

To print the Configuration Page:
1. At the printer control panel, to navigate to the Information Menu, use the arrows, then press **OK**.
2. Navigate to Information Pages, then press **OK**.
   The Configuration Page is highlighted by default.
3. To print the Configuration Page, press **OK**.
4. On the Configuration Page, under General Information, locate the current firmware version.

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:
- Locate your printer IP address using the Configuration Report. For details, see Printing the Configuration Page on page 13.
- Ensure that CentreWare Internet Services and TCP/IP are enabled. If you disabled either of these protocols, enable them at the control panel before accessing CentreWare Internet Services.

Accessing CentreWare Internet Services

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

Setting an Administrator Password

Xerox recommends that you set a system administrator password when you configure the printer. Store your password in a secure location.

To create an administrator password:
1. In CentreWare Internet Services, click **Properties > Security**.
2. Click **Administrative Security Settings**.
3. For Administrator Settings, type your user name, then type and retype a password that contains.
4. To grant or remove authorization to printer features, for Feature Authorization, select or clear the check boxes.
5. Click **Save Changes**.

⚠️ **CAUTION:** If you lose the Administrator password, a Fee-For-Service call is required to reset the password.

Accessing CentreWare Internet Services as an Administrator or Key User

Once an Administrator or Key User password is configured for the printer, to access CentreWare Internet Services pages, use the password to log in.

To access CentreWare Internet Services:

1. At your computer, open a Web browser, in the address field, type the IP address of the printer, then press **Enter** or **Return**.
2. Type the Administrator or Key User password.
3. Enter the password.
4. Click **OK**.

Locking the Control Panel

To prevent unauthorized users from changing settings at the printer control panel, you can lock some of the control panel menus.

If you lose the Administrator password, a Fee-For-Service call is required to reset the password.

1. In CentreWare Internet Services, click **Properties > Security**.
2. Click **Control Panel Lockout**.
3. For each control panel menu option that you want to lock, select the corresponding check box.
4. Click **Save Changes**.

Assigning a Printer Name and Location

1. In CentreWare Internet Services, click **Properties > General**.
2. Click **Printer Defaults**.
3. For Printer Name (SNMP System Name), type a name for the printer.
4. For Printer Location (SNMP System Location), type the location of the printer.
5. Click **Save Changes**.

Setting Up Printer Defaults

You can set printer defaults in CentreWare Internet Services for user preferences, local printer location, timeout settings, and print mode settings. You can override settings in the print driver on an individual basis as needed.

To set printer defaults in CentreWare Internet Services:

1. In CentreWare Internet Services, click **Properties > General**.
2. Click **Printer Defaults**.
3. Configure as needed.
4. Click **Save Changes**.

Identifying the Printer Configuration Automatically

During installation, the print driver identifies the configuration of the printer automatically. The print driver identifies optional features that are installed, such as automatic 2-sided printing, optional paper trays, or a solid-state hard drive. The print driver displays available installation settings. You can set the print driver to hide settings that are unavailable.

Using a Startup Network Configuration File

You can create a startup network configuration file to configure settings, load fonts, color tables, and job patches. When the printer is turned on or reset, it retrieves and processes the configuration file from a TFTP server.

Before You Begin

- The configuration file must be a valid PostScript or PCL file with appropriate PostScript, PCL. or PJL commands. For a list of PCL and PJL commands, see Printer Commands on page 87.
- The configuration file must be stored on a TFTP server that the printer can access over the TCP/IP network.

Specifying the Location of the Configuration File

To specify the location of the configuration file in a DHCP/BOOTP environment:

- For the TFTP server IP address or host name, use DHCP option 66.
- For the path name of the configuration file, use DHCP option 67.

  Notes:

  - For instructions on how to set parameters, refer to DHCP or BOOTP server documentation.
  - If other devices on your network use TFTP, Xerox recommends that you disable TFTP on the printer. To disable TFTP, in CentreWare Internet Services click **Properties > Protocols > TFTP**, then for TFTP, select **Off**.

To specify the location of the configuration file in a non-DHCP environment:

1. In CentreWare Internet Services, click **Properties > Protocols**.
2. Click **TFTP**.
3. For TFTP, select **On**.
4. For TFTP Server Name, type the IP address or hostname for the TFTP server.
5. For Boot File Name, type the path name of the configuration file.
6. Click **Save Changes**.

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 Speed

You can select the Ethernet connection speed for your network. You can select speed settings based on full duplex or half duplex modes.

- **Full Duplex speed**: The connection sends and receives data simultaneously.
- **Half Duplex speed**: The connection sends data in one direction at a time only.

To set the ethernet speed:

1. In CentreWare Internet Services, click **Properties > Interfaces**.
2. For Speed, select an option.
3. Click **Save Changes**.

USB Port Security

You can prevent unauthorized access to the printer through USB ports by disabling the ports.

Disabling the USB Port from CentreWare Internet Services

1. In CentreWare Internet Services, click **Properties > Interfaces**.
2. For USB Port, to disable, select **Off**.
3. Click **Save Changes**.

Disabling the USB Port at the Printer Control Panel

1. At the printer control panel, use the arrows to navigate to Printer Setup, then press **OK**.
2. Navigate to Connection Setup, then press **OK**.
3. Navigate to USB Setup, then press **OK**.
4. To disable, for USB Port, press **OK**.

Configuring USB Port Settings

1. In CentreWare Internet Services, click **Properties > Interfaces**.
2. To enable, for USB Port, select **On**.
3. For USB Port Timeout, type the number of seconds to wait before the port times out.
4. For Page Description Language, select an option. To configure the printer to detect the language of the print job automatically, select **AutoSelect**.
5. Click **Save Changes**.

Network Connectivity

3

This chapter includes:

Network Protocols

You can configure network protocols to enable printer discovery and network communications. You can configure protocols in CentreWare Internet Services and enable or disable them at the printer control panel.

You can prevent unauthorized access to the printer. For example, if you require a secure printing channel, you can enable the Internet Printing Protocol. If you do not use the Port 9100 and LPR protocols, you can disable the two protocols.

To disable a protocol:

1. At the printer control panel, use the arrows to navigate to Printer Setup, then press **OK**.
2. Navigate to the protocol.
3. Press **OK**.

Note: If you disable a protocol, some printer functions such as printer discovery, can be disabled.

IP

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

About TCP/IP and IP Addresses

Computers and printers primarily use TCP/IP protocols to communicate over an Ethernet network. Generally, Macintosh computers use either TCP/IP or the Bonjour protocol to communicate with a network printer. For Macintosh OS X systems, TCP/IP is preferred. Unlike TCP/IP, however, Bonjour does not require printers or computers to have IP addresses.

With TCP/IP protocols, each printer and computer must have a unique IP address. Many networks and cable and DSL routers have a Dynamic Host Configuration Protocol (DHCP) server. A DHCP server automatically assigns an IP address to every computer and printer on the network that is configured to use DHCP.

If you use a Cable or DSL router, see the documentation for your router for information on IP addressing.

Accessing TCP/IP Settings

You can access IPv4, IPv6, and DNS/WINS settings in CentreWare Internet Services.
1.   In CentreWare Internet Services, click **Properties** > **Protocols**.
2.   Click **TCP/IP**.
3.   To edit IPv4 settings, click **TCP/IP (v4)**.
4.   To edit IPv6 settings, click **TCP/IP (v6)**.
5.   To edit DNS/WINS settings, click **DNS/WINS**.
6.   For the new settings to take effect, restart your printer.

Enabling or Disabling TCP/IP at the Printer Control Panel

You can enable or disable IPv4 and IPv6 independently.

> Note: 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.

To enable or disable TCP/IP:

1. At the printer control panel, use the arrows to navigate to **Printer Setup** > **Connection Setup** > **Network Setup** > **Network Services**.
2. Select an option.
   - Navigate to TCP/IPv4, then press **OK**.
   - Navigate to TCP/IPv6, then press **OK**.
3. To enable or disable the protocol, press **OK**.

IPv4

This section includes:

You can configure IPv4 with or without BOOTP/DHCP. To enable the printer to acquire TCP/IP information automatically, configure IPv4 with BOOTP/DHCP. To enter TCP/IP information manually, configure IPv4 without BOOTP/DHCP. Without BOOTP/DHCP, the printer does not issue BOOTP or DHCP requests on startup.

Before you assign an IP address, ensure that no other device on the network is using the address. If another device is using the same IP address, the printer goes offline until the conflict is resolved.

Notes:

- To use BOOTP, set up a reservation for the printer on the BOOTP server.
- If you change the BOOTP/DHCP setting, the connection to the printer can be lost.

Configuring IPv4 With BOOTP/DHCP

1. In CentreWare Internet Services, click **Properties** > **Protocols**.
2. Click **TCP/IP (v4)**.
3. To enable TCP/IP v4, select the check box.
4. For Auto IP Enable, select an option.
   - **On**: This option assigns the IP address automatically.
   - **Off**: This option allows you to configure the IP address manually. This setting is recommended for enterprise networks.
5. For BOOTP/DHCP, select **On**.
6. Click **Save Changes**.

Configuring IPv4 Without BOOTP/DHCP

1. In CentreWare Internet Services, click **Properties** > **Protocols**.
2. Click **TCP/IP (v4)**.
3. To enable TCP/IP v4, select the check box.
4. For Auto IP Enable, select an option.
   - **On**: This option assigns the IP address automatically.
   - **Off**: This option allows you to configure the IP address manually. This setting is recommended for enterprise networks.
5. For BOOTP/DHCP, select **Off**.
6. Click **Save Changes**.
7. Click **Close** to return to the previous page.
8. To view the updated settings, select **Properties** > **TCP/IP**.

9. To enter the TCP/IP settings manually, type the printer IP Address.

    The format is x.x.x.x, where x represents a decimal number from 0 through 255. The value entered must be a valid IP address. It cannot be 0.0.0.0, 255.255.255.255, or any address starting with 127 or a number from 224 through 254.

10. For Network Mask, type the network mask.

    The format is x.x.x.x, where x represents a decimal number from 0 through 255.

11. For Router/Gateway Address, type an address.

    This address serves as the host that retransmits the packets from the current network segment to another network segment.

12. Click **Save Changes**.

TCP/IPv6 Settings

Use TCP/IPv6 to configure an IPv6 network address for the printer. You can have multiple IPv6 addresses.

Configuring IPv6

1. In CentreWare Internet Services, click **Properties > Protocols**.
2. Click **TCP/IP**.
3. Click **TCP/IP (v6)**.
4. To enable TCP/IP v6, select the check box.
5. For Interface ID, select an option.
    - To compute the interface identifier from the MAC address associated with the interface, select **Use Interface ID derived from MAC address**.
    - To configure the Interface ID manually, select **Use this Interface ID**, then type the interface identifier. Only use valid hexadecimal digits 0–9, a–f, or A–F.

    Note: If you change the Interface ID, the printer prompts you to restart before the changes take effect.

6. To enable automatic router address assignment, for Automatic Address Assignment, select **Use router supplied prefixes**.
7. To specify how IPv6 uses DHCP, for DHCPv6, select an option.
8. For Manual Address Assignment, select **Use this address**, then type the IPv6 address and prefix length.
9. To set the priority when both IPv6 and IPv4 addresses are available, for Address Precedence, select **Prefer IPv6 addresses** or **Prefer IPv4 addresses**.
10. Click **Save Changes**.

DNS/WINS

This section includes:

Domain Name System (DNS) is a system that maps host names to IP addresses. Windows Internet Name Service (WINS) allows the printer to register its IP address and NetBIOS Host Name with a WINS server. When WINS is configured, the printer uses only the host name to communicate.

You can obtain DNS/WINS settings from the DHCP or BOOTP server when enabled.

> Note: Before you change the DNS/WINS settings, contact your network administrator.

DNS/WINS Configuration Options

Name/Domain Name

The hostname is the printer name registered with DDNS and WINS that identifies it on the network. The domain name is the server location that the printer uses to communicate with other devices.

- The default hostname derives from the printer Ethernet address.
- You can set the hostname and the domain name, however if BOOTP/DHCP is enabled, BOOTP/DHCP can override these values.

DNS Configuration

You can use DNS configuration to define up to four name servers that are detectable by an IPv4 or IPv6 server.

- DNS configuration requires a name server.
- The format is x.x.x.x, where x represents a decimal number from 0 through 255.
- A value of all zeros indicates that no server is configured. If both primary and secondary name servers are undefined, the printer broadcasts (peer-to-peer) name recognition.
- BOOTP/DHCP can override the IPv6 name server information.

When Dynamic DNS is enabled, the printer can update the DNS server.

- If your DNS server supports dynamic address updates, for Dynamic DNS Registration, select the check box.
- To release the assigned hostname and IP address so that the server can use it for another device, select **Release Hostname Now!**.

> Note: If you select Release Hostname Now, the connection to the printer can be lost.

WINS Servers

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.

- DNS configuration requires the primary server address.
- The secondary server address is optional.
- The format is x.x.x.x, where x represents a decimal number from 0 through 255.
- If DHCP is configured, WINS IP addresses are overridden.

Multicast DNS (Bonjour)

When you enable Multicast DNS (Bonjour) on the printer, the printer responds to mDNS calls. Any computer that runs the Apple Macintosh OS Bonjour technology can discover the printer on a network.

To enable computers on a network to locate the printer with Multicast DNS (Bonjour), select **On**.

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. If Directory Agents (DA) exist on the network, they provide a cache for services information. When Directory Agent Discovery is enabled, the printer attempts SLP Directory Agent Discovery.

1. In CentreWare Internet Services, click **Properties > Protocols**.
2. Click **SLP**.
3. For SLP Enable, select **On**.
4. To configure the printer to search for discovery agents, for Directory Agent Discovery Enable, select **On**.
5. For Directory Agent, type the name of the directory agent. To discover one or more directory agents, leave the field blank.
6. For Scope 1, 2, and 3, type a name as needed. When scope fields are empty and DHCP Option 79 is configured on the DHCP server, the printer uses scopes that are specified in Option 79.
7. For SLP Multicast Enable, select an option.
   - **On**: The printer uses multicast to communicate as needed.
   - **Off**: The printer uses broadcast instead of multicast to communicate.
8. To specify the multicast radius, for SLP Multicast TTL, type a value from 0–255. Multicast radius is also referred to as hop count or time-to-live (TTL).
9. To specify the maximum packet size that the printer can transmit for UDP, for SLP MTU, type a value from 484–1400. When packets exceed the maximum size, the printer uses TCP/IP.
10. Click **Save Changes**.

UPnP

Universal Plug and Play (UPnP) is a method to obtain an IP address for a printer. UPnP uses Simple Service Discovery Protocol to locate and display devices on the network. 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 > Protocols**.
2. Click **UPnP**.
3. For SSDP Enable, select **On**.
4. For SSDP TTL, type a value for the multicast radius from 0–255.

   Multicast radius is also referred to as hop count or time-to-live (TTL).
5. Click **Save Changes**.

TFTP

Trivial File Transfer Protocol (TFTP) is a simplified protocol used to automated transfers of configuration or boot files between devices in a local environment. For example, you can use TFTP to retrieve a configuration file during setup of the printer.

1. In CentreWare Internet Services, click **Properties** > **Protocols**.
2. Click **TFTP**.
3. For TFTP, select **On**.
4. For TFTP Server Name, type the IP address or hostname for the TFTP server.
5. For Boot File Name, type the path name of the configuration file.
6. Click **Save Changes**.

Port 9100

Before you disable Port 9100, ensure that network users do not have their print driver configured to print to Port 9100.

1.   In CentreWare Internet Services, click **Properties > Protocols**.

2.   Click **Port 9100**.

3.   For Port 9100, select **On**.

4.   For Page Description Language, select the desired language that you want the printer to receive at Port 9100. To configure the printer to detect the language of the print job automatically, select **AutoSelect**.

5.   To enable the printer to respond to control characters included in a file, for Filtering, select **InterpreterBased**.

6.   Click **Save Changes**.

Note: IBM and legacy mainframes can generate control characters to manage jobs sent to the printer. The printer accepts PS and PJL files with embedded control characters.

LPR

LPR is an application-level printing protocol that uses TCP/IP to establish connections between printers and workstations on a network.

Before you disable LPR, ensure that network users do not have their print driver configured to print to LPR.

1. In CentreWare Internet Services, click **Properties** > **Protocols**.
2. Click **LPR**.
3. For LPR, select **On**.
4. To print a banner page with each job, for Banners, select **On**.

   If you select Off, but banner page printing is set to On at the file server, the file server setting overrides your selection.
5. To enable the printer to respond to control characters included in a file, for Filtering, select **InterpreterBased**.
6. Click **Save Changes**.

IPP

Internet Printing Protocol (IPP) is a standard network protocol that allows you to print and manage jobs remotely. IPP supports authentication and encryption for secure printing.

Before you disable IPP, ensure that network users do not have their print driver configured to print to IPP.

There are two authentication schemes.

- **Basic**: The printer authenticates the user who sends the print job.
- **Digest**: The printer uses a single checksum password scheme to authenticate the user who sends the print job. When you specify digest authentication, the required password is secured before it is sent to the printer. To enter the user name and password information and to enable digest authentication, in CentreWare Internet Services, click **Properties > Protocols > IPP**.

  Notes:

  - These options comply with official standards for basic and digest authentication, however, not all IPP clients support these authentication methods.
  - If you configure IPP for Windows, specify a user name, password, and digest authentication.

To configure IPP:

1. In CentreWare Internet Services, click **Properties > Protocols**.
2. Click **IPP**.
3. For IPP, select **On**.
4. For Page Description Language, select the desired language that you want the printer to receive at Port 9100. To configure the printer to detect the language of the print job automatically, select **AutoSelect**.
5. To enable the printer to respond to control characters included in a file, for Filtering, select **InterpreterBased**.
6. For Authentication Scheme, select an option.
7. For User Name, type a user name.
8. Type the password.
9. Type the password again to verify.
10. Click **Save Changes**.

    Note: IBM and legacy mainframes can generate control characters to manage jobs sent to the printer. The printer accepts PS and PJL files with embedded control characters.

Mopria

Mopria is a software feature that enables users to print from mobile devices without requiring a print driver. You can use Mopria to print from your mobile device to Mopria-enabled printers.

Notes:

- Mopria and all of its required protocols are enabled by default.
- Only Mopria-enabled devices support Mopria printing.
- Wireless devices must join the same wireless network as the printer. A system administrator can connect the printer by its wired network interface.
- The device that submits the Mopria job must be on the same subnet as the printer. To allow devices to print from different subnets, configure your network to pass multicast DNS traffic across subnets.
- The name and location of your printer appears in a list of Mopria-enabled printers on connected devices.

To configure Mopria:

1. In CentreWare Internet Services, click **Properties > Protocols**.
2. Click **Mopria**.
3. For Protocol, select **Enabled**.
4. To modify IPP, click **Edit Settings**.
5. To modify Multicast DNS (Bonjour), click **Edit Settings**.
6. Click **Save Changes**.

AirPrint

Use AirPrint to print directly from a wired or wireless device without using a print driver. AirPrint is a software feature that allows for driverless printing from Apple iOS-based mobile devices and Mac OS-based devices. AirPrint-enabled printers let you print directly from a Mac or from an iPhone, iPad, or iPod touch.

If you specify the geographical latitude and longitude of the printer, use decimal form. For latitude, type a coordinate value from –90 through 90. For longitude, type a coordinate value from –180 through 180. For example, use coordinates such as 45.325026, -122.766831.

Notes:

- When HTTP, IPP, and Bonjour mDNS protocols are enabled, AirPrint is enabled by default. If you disable HTTP, IPP, or Bonjour, AirPrint is disabled.
- Not all iOS applications support printing using AirPrint.
- Wireless devices must join the same wireless network as the printer. A system administrator can connect the printer by its wired network interface.
- The device that submits the AirPrint job must be on the same subnet as the printer. To allow devices to print from different subnets, configure your network to pass multicast DNS traffic across subnets.
- AirPrint-enabled printers work with all models of iPad, iPhone (3GS or later), and iPod touch (3rd generation or later), running the latest version of iOS.
- The Mac OS device must be Mac OS 10.7 or later.

To configure AirPrint:

1. In CentreWare Internet Services, click **Properties** > **Protocols**.
2. Click **AirPrint**.
3. To enable AirPrint, select **Enabled**.
4. To change the printer name, in the Name field, type a new name.
5. To enter a physical location for the printer, in the Location field, type the location.
6. To enter a geographic location for the printer, for Geographic Location, enter the latitude and longitude in decimal form.
7. To modify IPP, click **Edit Settings**.
8. To modify Multicast DNS (Bonjour), click **Edit Settings**.
9. To add or delete certificates on the printer, click **Manage Certificates**.
10. Click **Save Changes**.
11. For the new settings to take effect, restart your printer.

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.

SNMP v1/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.

To access SNMP v1/v2c:
1. In CentreWare Internet Services, click **Properties > Protocols**.
2. Click **SNMP**.
3. Click **Configure SNMP v1/v2c**.

To configure SNMP v1/v2c community names:
1. For community names, type each name.
2. Click **Apply**.

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

To configure SNMP v1/v2c traps:
1. Click **Configure Traps**.
2. To edit or delete a trap, click **Edit** or **Delete**. To add a trap address, click **Add Destination**.
3. For Trap Destination Address, type an IP address.
4. For DNS Name, type a domain name.
5. Type the UDP Port Number.
6. For SNMP Version, select the trap version for the specified address.
7. For Traps Community Name, type the name of the destination device.
8. For Traps to be received, for at least one trap, select the corresponding check box.
9. Click **Apply**.

SNMP v3

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

SNMP v3 configuration requires an SSL certificate. In most cases, a certificate is established automatically when the printer is first turned on and no other action is required.

To edit SNMP v3 properties:

1. In CentreWare Internet Services, click **Properties** > **Protocols**.
2. Click **SNMP**.
3. For SNMP v3 Protocol, click **Configure SNMP v3**.
4. Click **Configure Accounts**.
5. Configure as needed.

Configuring SNMP for Maximum Security

You can configure SNMP for maximum security.

1. To access CentreWare Internet Services, open a Web browser, then type the IP address for your printer.
2. To configure SSL, click **Properties** > **Security** > **HTTPS**.
3. For Use SSL, select **To Secure Pages and Passwords**.
4. Click **Save Changes**.
5. To restrict access to configuration pages, click **Properties** > **Administrative Security Settings**.
   a. To remove user access, for **View Configuration Web Pages** and **Modify Configuration Web Pages**, clear the check boxes.
   b. Click **Save Changes**.
6. Configure Administrative and Key User accounts as needed.

Configuring the Administrative User Account

You can require passwords or keys for administrative or key user account authentication.

Note: For privacy, to hide passwords as they are typed, select **Hide Typing**.

To set an authentication password:
1. Click **Properties > SNMP > Configure SNMP v3**.
2. Click **Create Account(s)**.
3. Click **Configure using Passwords**.
4. For User Name, type the Administrator user name.
5. For Authentication Protocol, select an option.
6. Type and confirm the Authentication Password. The Authentication Password is used to generate a key used for authentication.
7. For Privacy Protocol, select an option.
8. 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.
9. Click **Create**.
10. Click **Next**.

To set an authentication key:
1. Click **Properties > SNMP > Configure SNMP v3**.
2. Click **Configure Account(s)**.
3. Click **Configure Using Keys**.
4. For User Name, type the Administrator user name.
5. For Authentication Protocol, select an option.
6. Type and confirm the Authentication key.
7. For Privacy Protocol, select an option.
8. Type and confirm the Privacy key.
9. Click **Create**.

Configuring the Key User Account

You can require passwords or keys for administrative or key user account authentication.

Note: For privacy, to hide passwords as they are typed, select **Hide Typing**.

To set an authentication password:

1. On the SNMP v3 Key User Account page, select **Configure Using Passwords**.
2. For User Name, type the Key user name.
3. For Authentication Protocol, select an option.
4. Type and confirm the Authentication Password. The Authentication Password is used to generate a key used for authentication.
5. For Privacy Protocol, select an option.
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.
7. Click **Create**.
8. Click **Next**.

To set an authentication key:
1. On the SNMP v3 Key User Account page, select **Configure Using Keys**.
2. For User Name, type the Key user name.
3. For Authentication Protocol, select an option.
4. Type and confirm the Authentication key.
5. For Privacy Protocol, select an option.
6. Type and confirm the Privacy key.
7. For MIB Access, select an option.
8. Click **Create**.
9. Click **Next**.

Configuring the Other Account Settings

1. On the SNMP v3 Other Account Settings page, to enable all users, select **Any User Enabled**.
2. For MIB Access, select an option.
3. To enable print driver account access for the Any User Account, for Driver Account, select **Driver Account Enabled**.

   Note: If Driver Account is disabled, communication is lost between the printer and any applications that use SNMP v3, such as a Xerox print driver.

4. Click **Finish**.

Configuring the SNMP Access Control List

You can use the SNMP Access Control List to set up a list of hosts that are authorized to access the printer.

To configure the Host Access List:

1. In CentreWare Internet Services, click **Properties > Protocols**.
2. Click **SNMP**.
3. For Host Access List, type up to 10 host IP addresses. Separate Host Access List entries with a blank or a comma, or to specify a range, use a hyphen. To represent a group of addresses, for example 13.62.156.*, use an asterisk.
4. Separate Host Access List entries with a blank or a comma, or to specify a range, use a hyphen.
5. Click **Save Changes**.

Disabling and Enabling SNMP

If SNMP is not needed, to prevent unauthorized access to the printer, you can disable it in CentreWare Internet Services.

If you disable SNMP, the following print driver features are also disabled.

*   Walk-Up Installer
*   Smart Trays
*   PhaserSMART
*   Automatic supplies ordering
*   Consumable levels
*   Warning and error status
*   Synchronization with installed options, including a hard drive, memory, or extra trays

To disable or enable SNMP:

1. In CentreWare Internet Services, click **Properties > Protocols**.
2. Click **SNMP**.
3. For SNMP Enable/Disable, click **Disable SNMP Now** or **Enable SNMP Now**.
4. Click **OK**.

FTP

File Transport Protocol (FTP) is a standard network protocol used to pass and manipulate files over a TCP/IP network.

1. In CentreWare Internet Services, click **Properties > Protocols**.
2. Click **FTP**.
3. For FTP, select **On**.
4. Type the password.
5. For Page Description Language, select the desired language that you want the printer to receive at Port 9100.
6. To configure the printer to detect the language of the print job automatically, select **AutoSelect**.
7. To enable the printer to respond to control characters included in a file, for Filtering, select **InterpreterBased**.
8. Click **Save Changes**.

   Note: IBM and legacy mainframes can generate control characters to manage jobs sent to the printer. The printer accepts PS and PJL files with embedded control characters.

Email Server or SMTP

Simple Mail Transfer Protocol (SMTP) is an Internet standard used to transmit email across IP networks. You can specify your SMTP server or use DNS to identify the SMTP server automatically.

To configure email server settings:

1. In CentreWare Internet Services, click **Properties > Protocols**.
2. Click **Email Server**.
3. Select an identification method for your SMTP server.
   - To identify the SMTP email server automatically, select **Use DNS to Identify SMTP Server (Automatic)**, then type the corresponding primary and secondary IP addresses.
   - To identify the SMTP email server manually, select **Specify SMTP Server Manually**, then type the name or IP address for the SMTP server.
4. For Return Email Address, type the email address that you want to use to send emails from the printer.
   If you do not specify a return address, undeliverable email is sent to the system postmaster.
5. As needed, select **Use Authentication**, then type the login information.
   a. Type the user name.
   b. Type a Password for the user, then retype it to verify.
   c. Type the SMTP service name.
6. Click **Save Changes**.

Configuring MaiLinX

MaiLinX is a feature that sends printer status updates to specified email recipients.

You can configure the printer to send MaiLinX email alerts automatically for specified conditions.

- When the printer requires attention or encounters an error, a MaiLinX alert is sent to specified recipients.
- When the printer encounters a condition specified in the MaiLinX trigger settings, a MaiLinX alert is sent.

To configure MaiLinX alerts:

1. In CentreWare Internet Services, click **Properties**.
2. Click **Mail Alerts**.
3. For MaiLinX (and Usage Profile Properties), select **On**.
4. To specify recipients of MaiLinX alerts, type their corresponding email addresses.
5. To configure Advanced Settings, click the corresponding links.
   a. To specify a return email address for undeliverable MaiLinX alerts, click **Email Server Settings**.
   b. To format MaiLinX messages, click **MaiLinX Message Settings**.
   c. To set conditions and recipients for triggered MaiLinX alerts, click **MaiLinX Trigger Settings**.
6. Click **Save Changes**.

To configure MaiLinX message settings:

1. In CentreWare Internet Services, click **Properties**.
2. Click **Mail Alerts**.
3. For Advanced Settings, click **MaiLinX Message Settings**.
4. For Printer Name, Printer Location, and Printer Contact, type the corresponding information.
5. To set default text for the subject line, for Subject Text, type simple text, variables, or a combination of both. For example, to add the printer name to the default subject text, type **MaiLinx Alert from \$**.
6. To set default text for the message body, for Message Text, type simple text, variables, or a combination of both. For example, to create a default message that includes the printer name, location, serial number, and error message, type **Printer \$ (\%) (\#) ***.
7. Click **Save Changes**.

To configure MaiLinx trigger settings:

1. In CentreWare Internet Services, click **Properties**.
2. Click **Mail Alerts**.
3. For Advanced Settings, click **MaiLinX Trigger Settings**.
4. For each trigger, to select recipients to receive email when the trigger occurs, select the corresponding check boxes.
5. Click **Save Changes**.

EtherTalk

EtherTalk is a protocol that redirects AppleTalk packets from the printer port to the EtherTalk card. These packets are then encapsulated in Ethernet Link Access Protocol and sent out onto the network.

The printer requires a unique location name or identifier. IBM and legacy mainframes can generate control characters to manage jobs sent to the printer. The printer accepts PS and PJL files with embedded control characters.

1. In CentreWare Internet Services, click **Properties > Protocols**.
2. Click **EtherTalk**.
3. To enable EtherTalk, select **On**.
4. Type a name and description.
5. For Zone, type the location of the printer. This field cannot be blank and cannot contain null characters.
6. For Page Description Language, select the desired language that you want the printer to receive at Port 9100. To configure the printer to detect the language of the print job automatically, select **AutoSelect**.
7. To enable the printer to respond to control characters included in a file, for Filtering, select **InterpreterBased**.
8. Click **Save Changes**.

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, Windows Server 2008, and newer operating systems. WSD is one of several supported communication protocols.

Configuring WSD

1. In CentreWare Internet Services, click **Properties > Protocols**.
2. Click **WSD**.
3. To enable a service, select the corresponding check box.
4. Click **Save Changes**.

Security

4

This chapter includes:

See also:

www.xerox.com/security

Optimizing Printer Security in a High-Risk Environment

You can optimize printer security to reduce the risk of unauthorized access in a high-risk environment.

1. Create or add a digital certificate. For details, see About Certificates on page 54.
2. Configure HTTPS and SSL. For details, see Configuring HTTPS and SSL on page 58.
3. Create an Administrator account. For details, see Administrative Security Settings on page 49.
4. Set user and group access levels. For details, see Setting Access Control Levels on page 65.
5. Specify the computers that can access the printer. For details, see Access Control Lists on page 49.
6. Configure security protocols. For details, see SNMP on page 37.
7. Disable unused protocols. For details, see Network Protocols on page 22.
8. Disable job accounting. For details, see Job Accounting on page 53.
9. Schedule the automatic removal of stored print jobs. For details, see Configuring the Removal of Print Jobs on page 51.
10. Disable access to printer menus. For details, see Locking the Control Panel on page 15.

Administrative Security Settings

You can configure Administrative Security Settings to prevent unauthorized access or changes to printer features. The default settings provide all users access to all printer features. After you set up an administrator account, you can grant access to printer features based on user roles. Administrator and Key User accounts require a password to access controlled printer features.

There are three types of roles:

- **Administrator**: The Administrator role has access to all features and tools on the printer.
- **Key User**: This user class has some administrative responsibilities for printer functions.
- **Any User**: This user class has no responsibility for managing the printer and is the average user sending print jobs to the printer.

    Note: Until you limit access and set permissions, all computers and host systems can access the printer.

Access Control Lists

You can use access control lists to specify computers that are allowed to access the printer. The printer has four access control lists that are configured in CentreWare Internet Services.

- **Print Host Access List**: The printer uses this list to grant access to computers that are authorized to print to the printer.
- **Administrator Host Access List**: The printer uses this list to grant access to administrator computers that can change printer settings.
- **Key User Host Access List**: The printer uses this list to grant access to computers with key user access that can change printer settings.
- **SNMP Host Access List**: The printer uses this list to grant access to devices that can access the printer using SNMP.

    Note: The host access list can include up to 10 host IP addresses or names. To represent a group of addresses, for example 13.62.156.*, use an asterisk.

    See also:

Configuring Administrative Security Settings

1. In CentreWare Internet Services, click **Properties** > **Security**.
2. Click **Administrative Security Settings**.
3. For Administrator Settings, configure the settings.
   a. To specify computers that are allowed to change printer settings, for Host Access List, type the IP addresses or host names.
   b. For User Name, type a user name.
   c. Type a Password for the user, then retype it to verify.
4. For Key User Settings, configure the settings.
   a. To specify computers that are allowed to change printer settings, for Host Access List, type the IP addresses or host names.
   b. For User Name, type a user name.
   c. Type a Password for the user, then retype it to verify.
5. To grant or remove authorization to printer features, for Feature Authorization, select or clear the check boxes. To remove user access, for **View Configuration Web Pages** and **Modify Configuration Web Pages**, clear the check boxes.
6. For PostScript and PJL Configuration Password, type then retype a password.
7. Click **Save Changes**.

Printing Security Settings

This section includes:

Setting the Print Host Access List

1. In CentreWare Internet Services, click **Properties > Security**.
2. Click **Printing Security Settings**.
3. To specify computers that are allowed to change printer settings, for Host Access List, type the IP addresses or host names.
4. Click **Save Changes**.

Configuring the Removal of Print Jobs

You can configure the printer to remove personal, secure, or proof print jobs. This feature prevents access to unprinted data.

Notes:

- This feature does not remove saved or protected print jobs.
- To use this feature, you must have the optional solid-state drive installed.
- The printer uses a solid-state drive in place of a hard drive that encrypts and stores data in random memory locations. Since this printer does not have a hard drive, there is no need for a drive overwrite feature.

To configure the removal of print jobs in CentreWare Internet Services:

1. In CentreWare Internet Services, click **Properties > Security**.
2. Click **Printing Security Settings**.
3. For Remove Unprinted Personal, Secure, and Proof Jobs, select one or more options.
   - To remove all unprinted jobs when you click Save Changes, select **Upon Save Changes**.
   - To specify the removal of unprinted jobs automatically each day, select **At this time each day (24 hr)**, then select the hour and day.
   - To specify the removal of unprinted jobs automatically based on a length of time, select **When jobs are**, then type the number of hours.
4. Click **Save Changes**.

To configure the removal of print jobs at the printer control panel:

1. At the printer control panel, use the arrows to navigate to Printer Setup, then press **OK**.
2. Navigate to File Security, then press **OK**.
3. To remove all secure, personal, and proof print jobs, for Remove Job Files, press **OK**.
4. For Remove Job Files NOW, press **OK**.
5. To specify the removal of print jobs automatically at a certain time each day, perform the following steps.
    a. Navigate to Daily Removal, then press **OK**.
    b. Navigate to Remove at HH:MM, then press **OK**.
    c. Press **OK**.
    d. To select a value, use the arrow buttons, then press **OK**.
    e. Navigate to Minute, then press **OK**.
    f. To select a value, use the arrow buttons, then press **OK**.
    g. To exit the menu, press **Back/Return**.
6. To specify removal of print jobs automatically based on the age of the document, perform the following steps.
    a. Navigate to Age Based Removal, then press **OK**.
    b. Navigate to Remove at Age, then press **OK**.
7. To select a value, use the arrow buttons, then press **OK**.

Deleting Secure Jobs

To prevent unauthorized access to confidential print jobs stored on the printer, you can delete all Secure Print jobs.

1. In CentreWare Internet Services, click **Jobs**.
2. Click **Delete Secure Jobs**.
3. To delete all secure jobs that are stored on the printer, select **Delete All Secure Jobs**.
4. To delete secure jobs that are linked to a user account, select **Delete Secure Jobs with the Following**, then type the user name and numeric password.
5. Click **Delete Job(s)**.

Job Accounting

The Job Accounting feature records print jobs that occur on the printer. You can download the print job log as a tab-delimited text file to review for potential problems.

The printer can store approximately 500 print jobs in RAM. If the printer is reset, the data is lost. The printer can store approximately 5000 print jobs on the optional solid state drive. If the printer is turned off or reset, the data is deleted.

Enabling Job Accounting

1. In CentreWare Internet Services, click **Properties > Security**.
2. Click **Printing Security Settings**.
3. For Job Accounting Record, select **Enabled**.
4. Click **Save Changes**.

Downloading Job Accounting Records

1. In CentreWare Internet Services, click **Jobs**.
2. Click **Job Accounting**.
3. Click **Download All Job Accounting Records (CSV)** or **Download All Accounting Records (XML)**. Select the XML option if you intend to import the Job Accounting Records into the Usage Analysis Tool (UAT).
4. Click **Save** to save the **.csv** or **.xml** file to your computer.

Clearing Job Accounting Records

1. In CentreWare Internet Services, click **Jobs**.
2. Click **Job Accounting**.
3. Click **Clear Job Accounting Records**.
4. Click **OK**.

Accessing the Job Accounting File Using FTP

You can use FTP to access the job accounting file from your computer and transfer it to your printer.

To access the job accounting file using FTP:
1. Open a command window.
   – For Windows, open a Command Prompt.
   – For Macintosh, open a Terminal Window.
2. Type **ftp xxx.xxx.xxx.xxx**, where xxx.xxx.xxx.xxx is the IP address of the device, then press **Enter** or **Return**.
3. At the User prompt, type your user name and password, or for none, press **Enter** or **Return**.
4. To retrieve the job accounting file, at the ftp prompt, type **get jobacct.log**.

   Note: You cannot use the dir/Is commands to display the files on the printer.

About 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

The printer supports three types of certificates. You can create a self-signed certificate, or install a root certificate or a certificate signed by a certificate authority (CA).
- A Device Certificate is a certificate for which the printer has a private key. The purpose specified in the certificate allows it to be used to prove identity.
- The printer generates a default self-signed certificate during its first startup.
- A CA Certificate is a certificate with authority to sign other certificates. The device certificate signed by a CA validates the identity of the printer to the network.
- A Root or Trust Point Certificate is a self-signed certificate from another device that you want to trust.

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.

Adding or Creating a Certificate

1. In CentreWare Internet Services, click **Properties > Security**.
2. Click **Certificates**.
3. Click **Add/Create**.
4. Select an option.
   - **Install a new Root or other Trust Point Certificate**: This option adds a certificate that is required to validate the authentication server certificate when using 802.1X EAP authentication.
   - **Install a CA signed Device Certificate**: This option adds a device certificate signed by a certificate authority (CA) that validates the identity of the printer to the network.
   - **Create Certificate Signing Request (CSR)**: This option creates a CSR that you can send for signing to a trusted CA. When the certificate is returned, you can install the CA signed device certificate on the printer.
   - **Create Self-Signed Device Certificate**: This option modifies the default self-signed certificate that is created automatically on the printer. If you use HTTPS, each printer requires a unique certificate created for each browser that is used to access the printer.
5. Click **Next**.
6. Follow the onscreen instructions.
7. To add or create the certificate, click **Finish**.

Managing Certificates

1. In CentreWare Internet Services, click **Properties** > **Security**.
2. Click **Certificates**.
3. To view a certificate, click its Friendly Name.
4. To delete a certificate, select the check box next to the certificate name and click **Delete Selected**.

Setting the Certificate Key Length

1. In CentreWare Internet Services, click **Properties** > **Security**.
2. Click **Certificate Key Length**.
3. For Minimum Encryption Key Length, select an option.
4. Click **Save Changes**.

Configuring 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.

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.

To configure 802.1X:

1. In CentreWare Internet Services, click **Properties > Security**.
2. Click **802.1X**.
3. To begin configuration, click **Configuration Wizard**.
4. To use the existing certificate, click **Next**.
5. For Authentication Methods, select one or more options.
   - **MD5 Challenge**: You can use this option to require a user name and password.
   - **TLS**: You can use this option to require a root certificate, device certificate, and a user name and password.
   - **PEAP-MS-CHAPv2**: You can use this option to require a root certificate and a user name and password.
6. To configure each authentication method, click **Next**.
7. For Root Certificate, select an option.
8. For Device Certificate, select an option.
9. For Credentials, type the user name and password.
10. For 802.1X, select **Enabled**.
11. To activate the settings immediately, select **Reauthenticate on Finish**.
12. Click **Finish**.
13. For the new settings to take effect, restart your printer.

About HTTPS and SSL

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.

You can establish an HTTP Secure(HTTPS) connection to the printer by encrypting data sent over HTTP using SSL. Secure Sockets Layer (SSL) is a protocol that creates an encrypted connection between your printer and a server. Features that require HTTPS use it automatically. You can use SSL encryption for protocols such as SMTP as well.

Note: When SSL is enabled, all Web pages contain https:// in the URL.

Configuring HTTPS and SSL

SSL requires a digital certificate. For details, see About Certificates on page 54.

To configure SSL:

1. In CentreWare Internet Services, click **Properties > Security**.
2. Click **HTTPS**.
3. For Use SSL, select an option.
   – To disable SSL so that the printer does not require authentication, select **Never Select**.
   – To enable SSL so that the printer uses SSL to secure all Web pages, select **To Secure Pages and Passwords**.
4. To allow connections to the device using SSL v3 only, select **Require SSL V3**.
5. For Cipher Encryption Strength, when SSL is enabled, select an option. Default supports less than 128 bits.
6. Click **Save Changes**.
7. If you disabled SSL, for settings to take effect, restart the printer.

IPsec

This section includes:

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.

Notes:

- You cannot delete an IPsec host or protocol group that is used by an IPsec policy.
- You can restrict access to this feature. For details, see Administrative Security Settings on page 49.

Enabling IPsec

Before you begin:

- To ensure a secure connection between the printer and the server, create or add a certificate. For details, see About Certificates on page 54.
- Enable Secure HTTP (SSL). For details, see Configuring HTTPS and SSL on page 58.

To enable IPsec:

1. In CentreWare Internet Services, click **Properties > Security**.
2. Click **IPsec**.
3. Click **Security Policies**.
4. For IPsec, select **On**.
5. Click **Apply**.

Disabling IPsec

If an IPsec policy is configured incorrectly, it can cause the printer to become unavailable on the network. To re-establish printer connectivity, disable IPsec.

To disable IPsec in CentreWare Internet Services:
1. In CentreWare Internet Services, click **Properties** > **Security**.
2. Click **IPsec**.
3. Click **Security Policies**.
4. For IPsec, select **Off**.

To disable IPsec at the printer control panel:
1. At the printer control panel, use the arrows to navigate to **Printer Setup** > **Connection Setup** > **Network Setup** > **Network Services**.
2. Navigate to IPsec, then press **OK**.
3. For the new settings to take effect, restart your printer.

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.

Adding an IPsec Policy
1. In CentreWare Internet Services, click **Properties** > **Security** > **IPsec**.
2. Click **Security Policies**.
3. For Hosts, select an option, or click **Add Host Group**, configure as needed, then click **Save Changes**.
4. For Protocols, select an option, or click **Add Protocol Group**, configure as needed, then click **Save Changes**.
5. For Actions, select an option, or click **Add IPsec Action**, configure as needed, then click **Save Changes**.
6. Click **Add Policy**.
7. Click **Apply**.
8. Click **Continue**.

Modifying or Deleting an IPsec Policy
1. In CentreWare Internet Services, click **Properties** > **Security** > **IPsec**.
2. Click **Security Policies**.
3. To modify, click the name, modify as needed, then click **Save Changes** > **Apply**.
4. To delete a policy from the list, click **Select** > **Delete**.
5. To reset security association sessions, restart the printer.

Managing Host Groups

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

Creating an IP Host Group

1. In CentreWare Internet Services, click **Properties** > **Security** > **IPsec**.
2. Click **IP Host Groups**.
3. Click **Create Group**.
4. Type a Name and a Description for the group.
5. For Address List, enter network information.
6. Click **Save Changes**.
7. Click **Apply**.

Modifying or Deleting a Host Group

1. In CentreWare Internet Services, click **Properties** > **Security** > **IPsec**.
2. Click **IP Host Groups**.
3. To modify, click the name, modify as needed, then click **Save Changes** > **Apply**.
4. To delete a policy from the list, click **Select** > **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 an IP Protocol Group

1. In CentreWare Internet Services, click **Properties** > **Security** > **IPsec**.
2. Click **IP Protocol Groups**.
3. Click **Create Group**.
4. Type a Name and a Description for the group.
5. For Protocol, select at least one protocol to add to the group.
6. Click **Save Changes**.
7. Click **Apply**.

Modifying or Deleting an IP Protocol Group

1. In CentreWare Internet Services, click **Properties** > **Security** > **IPsec**.
2. Click **IP Protocol Groups**.
3. To modify, click the name, modify as needed, then click **Save Changes** > **Apply**.
4. To delete a policy from the list, click **Select** > **Delete**.

Managing Actions

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

Creating an IPsec Action

You can create IPsec actions with a manual keying method or an Internet Exchange Key (IKE). Use IKE to set up a Security Association (SA) in the IPsec protocol suite. Manual Keying is used when client systems either do not support IKE or are not configured for IKE.

To create an IPsec action:
1. In CentreWare Internet Services, click **Properties** > **Security**.
2. Click **IPsec**.
3. Click **IPsec Actions**.
4. Click **Create Action**.
5. Type a name and description.
6. For Keying Method, select an option.

Configuring Manual Keying Settings

For manual keying, you can select an IPsec transport or tunnel mode. 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).

1. For IPsec Mode, select **Transport Mode** or **Tunnel Mode**.
2. If you select Tunnel, type the Remote Tunnel Address.
3. For IPsec Proposal Protocol, select an option.
4. For Encryption and Hash Algorithms, select from options that correspond to the selected IPsec Proposal Protocol.
5. For the inbound and outbound SPI fields, type a 32-bit number greater than 256.
6. For the inbound and outbound keys, type key values that correspond to the selected protocol and algorithms.
   – AES-CBC is 32 hexadecimal characters long.
   – 3DEC is 48 hexadecimal characters long.
   – DEC is 16 hexadecimal characters long.
   – SHA1 is 40 hexadecimal characters long.
   – MD5 is 32 hexadecimal characters long.
7. Click **Next**.
8. Click **Finish**.
9. Click **Apply**.

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.

To configure IKE:

1. For IKE Phase 1, for Authentication, select an option.
   - For X.509 Certificate, select an option.
   - For Pre-shared Key, type a key phrase. This field cannot be blank and cannot contain special characters.
2. Click **Next**.
3. For Authentication Transforms 1, 2, or 3, select at least one algorithm combination used during IKE protocol negotiation.
4. To specify the key expiration time, for Key Lifetime, type a value in seconds or KB. The minimum Key Lifetime value is 12 seconds or 2560 KB.

   When a key reaches this lifetime, the Security Association (SA) is renegotiated and the key is regenerated or refreshed.
5. Click **Next**.
6. For IPsec Mode, select **Transport Mode** or **Tunnel Mode**.
7. If you select Tunnel, type the Remote Tunnel Address.
8. To configure at least one protocol, for IPsec Proposal Protocol 1, 2, and 3, select an option.
9. For Encryption and Hash Algorithms, select from options that correspond to the selected IPsec Proposal Protocol.
10. For DH Group, select an option.
11. To specify the key expiration time, for Key Lifetime, type a value in seconds or KB. The minimum Key Lifetime value is 12 seconds or 2560 KB.
12. Click **Next**.
13. Click **Finish**.
14. Click **Apply**.

Modifying or Deleting an IPsec Action

1. In CentreWare Internet Services, click **Properties** > **Security** > **IPsec**.
2. Click **IPsec Actions**.
3. To modify, click the name, modify as needed, then click **Save Changes** > **Apply**.
4. To delete an action, for that action, select the check box, then click **Delete Action**.

Setting Access Control Levels

You can set access control levels to specify group and user permissions for job types, paper trays, and applications. Application Permissions control jobs that do not originate from the print driver.

Notes:

- To use this feature, you must have the optional solid-state drive installed.
- You cannot restrict permissions for all job types at the same time.
- Access control settings apply only to jobs sent after permissions were set.

Setting Access Control Levels

1. In CentreWare Internet Services, click **Properties** > **Security**.
2. Click **Access Control**.
3. To configure a group, select an option.
4. To add users to the selected group, for Users, click **New**.
5. Type the login name.
   This field cannot be blank and cannot contain special characters.
6. To specify the period of time when printing or color printing is allowed, for Begin and End, select the time.
7. To enable or disable printing for specific job types, for Job Type Permissions, configure as needed.
8. To enable or disable printing from specific trays, for Tray Permissions, configure as needed.
9. For Application Permissions, perform the following steps.
   a. To add an application name, click **New**.
   b. Select an application name or type a name.
   c. For print permissions for the selected application, configure as needed.
10. Click **Save Changes**.

Administrator Tools

5

This chapter includes:

Accessing Usage Profile Reports

Usage Profile reports provide information on many aspects of printer usage, such as ink or toner used, number of pages printed, and paper types used.

Before you begin:

To send Usage Profile reports, configure MaiLinx. For details, see Configuring MaiLinX on page 44.

To access Usage Profile reports:

1. In CentreWare Internet Services, click **Jobs**.
2. Click **Usage Profile Reports**.
3. Select an option.
   - View, print, or email the Usage Profile Report.
   - To send to multiple recipients on a regular interval, set up the recipients on the User Profile Properties page, then select **Send Regular Interval Reports**.

Configuring Emulations

In CentreWare Internet Services, you can configure emulations for your printer.

To configure emulations:

1. In CentreWare Internet Services, click **Properties**.
2. Click **Emulations**.
3. To configure the Page Description Language sensing mode for each printer port, click **Sensing**.
4. Configure as needed.
5. Click **Save Changes**.

    Note: For details, see the Help in CentreWare Internet Services.

Configuring Web Server Features

You can use Web Server pages to configure server information, add printer support links, and customize Internet page information.

To configure Web server features:

1. In CentreWare Internet Services, click **Properties**.
2. Click **Web Server**.
3. Select an option.
4. Configure as needed.

   Note: For details, see the Help in CentreWare Internet Services.

Managing Personal Folders

You can manage the personal folders that the printer uses to store special job types. Personal Saved Jobs require a password.

To create a personal folder:
1. In CentreWare Internet Services, click **Properties**.
2. Click **Personal Folders > Create Folder**.
3. Enter a valid login name and password.

To delete a personal folder:
1. In CentreWare Internet Services, click **Properties**.
2. Click **Personal Folders > Manage Folders**.
3. To delete a folder, select the folder, then click **Delete Folder**.

To delete all the jobs in a folder:
1. In CentreWare Internet Services, click **Properties**.
2. Click **Personal Folders > Manage Folders**.
3. Select a Personal Jobs Folder.
4. To delete all jobs in a folder, select the folder and click **Delete Jobs**.

To change the password for a personal folder:
1. In CentreWare Internet Services, click **Properties**.
2. Click **Personal Folders > Manage Folders**.
3. Select a Personal Jobs Folder.
4. Click **Change Password**.
5. Type the old password.
6. Type the new password, then type the password again to verify.
7. Click **Save**.

Cloning Printer Settings

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: To ensure that EtherTalk Zone or IP Domain Name settings are cloned, select EtherTalk or TCP/IP settings for the source printer.

Before you begin:
- If you are using a clone file to copy your printer settings to another printer, ensure that both printers are the same model and have the same version of software installed.
- Ensure that the source printer and the destination printer have an IP address, network mask, and default gateway.

To clone the printer settings:
1. In CentreWare Internet Services, click **Properties**.
2. Click **Clone Printer**.
3. To specify the parameters that you want to clone from the source printer, select check boxes, or click **Check All**.
4. To specify the Destination Printer, type the IP address or DNS name.
5. For Optional Settings, type the name of the destination printer.
6. For EtherTalk Zone or IP Domain Name, if the destination printer is in a different location, type the modifications as needed.
7. Click **Clone Selected Settings**.
8. Click **Clone**.

Updating Firmware

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

⚠ **CAUTION:**

- Do not interrupt the firmware installation process. Interruptions or loss of power can corrupt the firmware and render the system temporarily unusable.
- Do not submit a print job to the device while upgrading firmware. If you interrupt a firmware upgrade, it can cause corruption to the printer firmware that can require a service call.

Notes:

- Firmware updates can change some printer factory settings. Xerox recommends that you print the Configuration Page as a reference to restore printer settings as needed after the firmware update completes.
- If you set the PostScript and PJL Configuration password, the printer prompts you to log in. For details, see Administrative Security Settings on page 49.

Before You Begin

Before you update the printer firmware, verify that the latest firmware version is older than the one you want to install.

Verifying the Latest Version of Firmware

To print the Configuration Page:

1. At the printer control panel, to navigate to the Information Menu, use the arrows, then press **OK**.
2. Navigate to Information Pages, then press **OK**.
   The Configuration Page is highlighted by default.
3. To print the Configuration Page, press **OK**.
4. On the Configuration Page, under General Information, locate the current firmware version.

To locate firmware:

1. To locate firmware for your printer, go to the Xerox support website, then click **Drivers & Downloads**.
   - Xerox®ColorQube 8580 Color Printer: www.xerox.com/office/CQ8580support
   - Xerox®ColorQube 8880 Color Printer: www.xerox.com/office/CQ8880support
2. Ensure that the latest version of firmware on the website is newer than the version that appears on the printer Configuration Page.

Downloading and Saving the Firmware Update

1. To locate firmware for your printer, go to the Xerox support website, then click **Drivers & Downloads**.
   - Xerox®ColorQube 8580 Color Printer: www.xerox.com/office/CQ8580support
   - Xerox®ColorQube 8880 Color Printer: www.xerox.com/office/CQ8880support
2. To download and save the software on your computer, click the link for the latest firmware, then follow the prompts.
3. Before you install the firmware, restart the printer.
   a. At the printer control panel, use the arrows to navigate to Shut Down, then press **OK**.
   b. Navigate to Restart Printer, then press **OK**.
   c. To restart the printer, at the Restart the printer NOW? prompt, press **OK**.

Updating the Firmware

1. In CentreWare Internet Services, click the **Print** tab.
2. Click **File Download**.
3. To select the new firmware file, click **Browse** or **Choose File**.
4. Click **Open**.
5. To send the file to the printer, click the blue button.

PhaserSMART Technical Support

PhaserSMART is an automated, Internet-based system that uses your Web browser to send diagnostic information from your printer to the Xerox® website. PhaserSMART examines the information, diagnoses the problem, and proposes a solution.

1. Open your Web browser and go to www.phaserSMART.com.
2. Enter the IP address of your printer in the form fields.
3. Follow the onscreen instructions.

Printer Neighborhood

Printer Neighborhood is a tool that enables you to search for printers on your network, check their status, and manage them remotely. You can also install, manage, troubleshoot, and view printer usage information from a variety of pages. Access to the embedded web server for each printer enables you to perform other management tasks.

Note: To access and use Printer Neighborhood, enable JavaScript. If you disable JavaScript, a warning message appears, and pages do not function properly.

For details on Printer Neighborhood features, from any Printer Neighborhood page, click the Help button.

Accessing Printer Neighborhood

1. In CentreWare Internet Services, click **Printer Neighborhood**.
2. When prompted, click **Continue**.
3. To expand your search or change your preferred IP Address/Subnet Settings, click **Preferences**.

Xerox® Usage Analysis Tool

The Xerox® Usage Analysis Tool (UAT) collects and analyzes enterprise-wide Xerox network printer usage data. You can use the Usage Analysis Tool for cost tracking and analysis, and for printer usage analysis.

Notes:

- To ensure accurate reports, synchronize the date and time on the printer with the computer where the Usage Analysis Tool is installed.
- For information about using the Xerox® Usage Analysis Tool, see the Help provided with the application.

Xerox® Usage Analysis Tool System Requirements

Requirement	Minimum Specification
Xerox Printer	• Ethernet network connection • Xeroxrecommends the optional solid-state drive.
Windows Client Computer	• Intel Pentium III processor • 128 MB RAM • 500-MB hard drive • Windows XP SP1 or later
Windows Server Computer	• Intel Pentium III processor • 256 MB RAM • 1-GB hard drive • Windows XP SP1 or later
.NET Framework	Framework 1.1 is included with the Xerox® Usage Analysis Tool.
The Job Accounting Feature	The Job accounting feature is enabled on your printer.

Installing the Xerox® Usage Analysis Tool

1. In CentreWare Internet Services, click **Support**.
2. Click **Software Installation > Printer Management Software**.
3. Click **Utilities & Applications > Usage Analysis Tool for Xerox Printers**.
4. Follow the onscreen instructions.

Disabling or Enabling CentreWare Internet Services

You can disable or enable CentreWare Internet Services at the printer control panel.

1. At the printer control panel, use the arrows to navigate to **Printer Setup** > **Connection Setup** > **Network Setup** > **Network Services**.
2. Navigate to CentreWare IS.
3. To change the setting to On or Off, press **OK**.
4. To exit the menu, press **Back/Return**.

Configuration Card A

This appendix includes:

The printer configuration card stores network settings and configuration data. If your printer needs to be replaced, to retain configuration settings, the service technician will transfer the configuration card to the new printer. When you restart the new printer, it inherits the settings on the configuration card from the old printer. A configuration card eliminates the need to manually reconfigure printer settings.

Configuration Card Parameters

General Information Parameters

- Printer Name
- Startup Page Enabled
- Printer ID
- Sys/Start Job
- Job Timeout
- Load Paper Timeout
- Menu Timeout
- Fast Resume
- Intelligent Ready
- Paper Source
- Tray 1 Size and Type
- Tray 2 Type
- Tray 3 Type
- Tray 4 Type
- Tray 5 Type
- Tray 1 Mode
- Tray 1 Prompt
- Tray 2 - N Prompt
- Tray 2 - N Mode
- Letter/A4 Substitution
- 2-Sided Printing
- Metric Defaults

  Note: If the trays are installed in the printer, the Tray 3, Tray 4, and Tray 5 parameters are stored on the printer configuration card.

PostScript Parameters

- Printer Quality
- Color Correction
- Error Info

PCL Parameters

- Font Number
- Pitch
- Point Size
- Symbol Set
- Orientation
- Form Length
- Line Termination
- Color Mode
- Wide A4 (210 x 297 mm)
- Enhanced Mode

USB 2.0 Parameters

- Enabled
- Language
- Wait Timeout

Hard Drive Parameters

- Daily Removal
- Daily Removal Time
- Removal Age
- Age-Based Removal

    Note: If the printer contains the optional solid-state drive, the hard drive parameters are stored on the configuration card.

Network Information Parameters

- Wait Timeout
- System Admin Contact
- Printer Location

Ethernet Network Parameters

- Network Speed/Type
- Network Address

Certificates

- Device Certificate
- Friendly Name
- Root Certificate

802.1X Parameters

Enabled

EtherTalk Parameters

- Enabled
- Language
- Filtering
- Name
- Printer Type
- Zone
- Network Node

TCP/IP Parameters

IPv4 Parameters

- Enabled
- Auto IP
- BOOTP/DHCP
- DHCP Server Address
- DHCP Lease Expiration
- DHCP Lease Renewal
- IP Address
- Network Mask
- Router/Gateway

IPv6 Parameters

- Enabled
- Interface ID
- Automatic Address Assignment
- DHCPv6
- Manual Address Assignment
- Address Precedence

DNS Parameters

- Primary Server
- Secondary Server
- mDNS (Bonjour) Enable

SLP Parameters

- Enabled
- Directory Agent Discovery Enable
- Directory Agent
- Scope 1
- Scope 2
- Scope 3
- SLP Multicast Enable
- SLP Multicast TTL
- SLP MTU

SSDP Parameters

- Enabled
- SSDP TTL

NBNS (WINS) Parameters

- Node Type
- WINS Servers

Access Control Parameter

Host Access List

LPR Parameters

- Enabled
- Filtering
- Enable Banners

AppSocket (Port 9100) Parameters

- Enabled
- Language
- Filtering

IPP Parameters

- Enabled
- Language
- Filtering
- Network Path

SNMP Parameters

- Enabled
- SNMP v1/v2c
- SNMP v3
- Host Access List

CentreWare Internet Services (HTTP) Parameters

- Enabled
- Custom Link
- Refresh Delay
- Administrator Password
- Key User Password
- Use SSL

FTP Parameters

- Enabled
- Language
- Filtering
- Login Password

Status Notification Parameters

- Enabled
- System Admin Email Address
- Service Email Address
- Key User Email Address

MaiLinX Remote Printing Parameters

- Language
- Filtering
- POP3 Server
- POP3 User Name
- POP3 Password
- POP3 Polling Interval
- Printing Password
- Authorized Users

Printer Commands

B

This appendix includes:

You can use Printer Control Language (PCL) and Printer Job Language (PJL) commands to control print job settings and printer defaults. Xerox printers support the standard set of PCL and PJL commands along with an expanded set of commands. This appendix contains the most commonly used PCL and PJL commands.

PCL Commands

Paper Size

The following table defines the PCL commands for supported paper sizes. For information on supported paper sizes and trays, from the printer control panel, you can print the Paper Tips page.

Paper Size	PCL 5 Command
A3 (297 x 420 mm, 11.7 x 16.5 in.)	<Esc>&l27A
A4 (210 x 297 mm, 8.3 x 11.7 in.)	<Esc>&l26A
A5 (148 x 210 mm, 5.8 x 8.3 in.)	<Esc>&l25A
A6 (105 x 148 mm, 4.1 x 5.8 in.)	<Esc>&l24A
JIS B4 (257 x364 mm, 10.1 x 14.3 in.)	<Esc>&l46A
B5 (176 x 250 mm, 6.9 x 9.8 in.)	<Esc>&l100A
ISO B5 (176 x 250 mm, 6.9 x 9.8 in.)	<Esc>&l100A
JIS B5 (182 x 257 mm, 7.2 x 10.1 in.)	<Esc>&l45A
SRA3 (320 x 450 mm, 12.6 x 17.7 in.)	<Esc>&l112A
Statement (140 x 216 mm, 5.5 x 8.5 in.)	<Esc>&l143A
Tabloid (279 x 432 mm, 11 x 17 in.)	<Esc>&l16A
305 x 457 mm, 12 x 18 in.	<Esc>&l148A
Executive (184 x 267 mm, 7.25 x 10.5 in.)	<Esc>&l1A
Letter (216 x 279 mm, 8.5 x 11 in.)	<Esc>&l12A
216 x 330 mm, 8.5 x 13 in.	<Esc>&l18A
Legal (216 x 356 mm, 8.5 x 14 in.)	<Esc>&l13A
A7 envelope (133 x 184 mm, 5.25 x 7.25 in.)	<Esc>&l174A
No. 10 envelope (241 x 105 mm, 4.1 x 9.5 in.)	<Esc>&l81A
Monarch envelope (98 x 190 mm, 3.9 x 7.5 in.)	<Esc>&l80A
C4 envelope (324 x 229 mm, 12.8 x 9 in.)	<Esc>&l171A
C5 envelope (162 x 229 mm, 6.4 x 9 in.)	<Esc>&l91A
C6 envelope (114 x 162 mm, 4.5 x 6.38 in.)	<Esc>&l170A
DL envelope (110 x 220 mm, 4.33 x 8.66 in.)	<Esc>&l90A
Custom	<Esc>&l101A
Note: The lowercase letter L follows the ampersand (&) symbol in the command.	

Paper Type

This table lists the most common PCL commands for supported paper types. For information on supported paper types and trays, from the printer control panel, print the Paper Tips page.

Paper Type	PCL 5 Command
Plain	<Esc>&n6WdPaper
Cardstock	<Esc>&n10WCardStock
Transparency	<Esc>&n13WdTransparency
Lightweight Cardstock	<Esc>&n14WdThinCardStock
Envelopes	<Esc>&n9WdEnvelope
Labels	<Esc>&n6WdLabel
Letterhead	<Esc>&n11WdLetterhead
Glossy	<Esc>&n12WdCoatedPaper
Colored Paper	<Esc>&n13WdColoredPaper
Pre-Printed	<Esc>&n11WdPreprinted
Pre-punched	<Esc>&n11WdPrepunched
Custom	<Esc>&n12WdCustomType 1 through <Esc>&n12WdCustomType 5

Input Trays

The following table lists the most common PCL commands for the input trays supported by your printer. If the optional input tray is not installed, the alternate tray is used.

Note: If there is more than one command available for the function, you can select any command listed.

Input Tray Options	PCL 5 Command	Alternate Tray
Tray 1	There is no corresponding command for this option.	Not all printer models support this feature.
Tray 1 in multi-sheet mode	<Esc>&l4H <Esc>&l6H	Not all printer models support this feature.
Tray 1 in manual feed mode	<Esc>&l2H <Esc>&l3H	Not all printer models support this feature.
Tray 2	<Esc>&l1H	Not all printer models support this feature.
Tray 3	<Esc>&l5H <Esc>l23H	Tray 2

Input Tray Options	PCL 5 Command	Alternate Tray
Tray 4	<Esc>&l8H <Esc>&l20H <Esc>&l24H	Tray 1
Tray 5	<Esc>&l21H	Tray 1
AutoSelect	<Esc>&l7H	Not all printer models support this feature.
Current tray	<Esc>&l0H	Not all printer models support this feature.
Note: The lowercase letter L follows the ampersand (&) symbol in the command.		

PJL Commands

The following table lists the most commonly used HP PJL and other PJL commands.

PJL Command	Values	Description
@PJL FSAPPEND	There is no corresponding value.	Appends data to an existing file, or if the file does not exist, creates the file, and loads the given data.
@PJL FSDELETE NAME="*pathname*"	*	Deletes a file from the installed hard drive.
@PJL FSDIRLIST NAME="*pathname*"	*	Lists PJL system files and directories.
@PJL FSDOWNLOAD FORMAT:BINARY SIZE=*size* NAME="*pathname*"	*	Downloads a file to the installed hard drive.
@PJL FSINIT VOLUME=*value*	*	Initializes the installed hard drive.
@PJL FSMKDIR NAME="*pathname*"	*	Creates the specified directory on the installed hard drive.
@PJL FSQUERY NAME="*pathname*"	*	Responds with information about the file or directory.
@PJL FSUPLOAD NAME="*pathname*"	*	Uploads file from the printer to the host.
@PJL USTATUS	*	Allows the printer to send unsolicited status messages for device status changes, end-of-job status, and pages printed. Status can be sent at specified time intervals.
@PJL USTATUSOFF	There is no corresponding value.	Turns off all status responses.
@PJL XCLIENT JOBID=*value*	There are exactly 48 bytes. The first byte is "8" and the last 8 bytes represent a time in the format hhmmsshs. The remainder of the bytes corresponds to the job ID.	Sets the client job ID used with Job Tracker.
@PJL XJAFILENAME="*filename*"	Roman-8 characters 1 through 255	Sets the file name for Job Accounting.
@PJL XJAHOSTNAME="*hostname*"	Roman-8 characters 1 through 255	Sets the host name for Job Accounting
@PJL XJAJOBNAME="*jobname*"	Roman-8 characters 1 through 255	Sets the job name for Job Accounting.
@PJL XJAUSERNAME="*username*"	Roman-8 characters 1 through 255	Sets the user name for Job Accounting.
@PJL XJOBPASSWORD=*value*	4-digits	Assigns the job password used by Secure Print.

PJL Command	Values	Description
@PJL XPERSONALJOB	There is no corresponding value.	Starts a Personal Print job.
@PJL XPROOFJOB	There is no corresponding value.	Starts a Proof Print job.
@PJL XSAVEDJOB	There is no corresponding value.	Starts a Saved Print job.
@PJL XSECUREJOB	There is no corresponding value.	Starts a Secure Print job.
@PJL XIGNOREFF=*value*	ON, OFF	Ignores FormFeed commands when printing PCL blank pages.
@PJL XLINETERMINATION=*value*	ON, OFF	Terminates a line.
@PJL XMBFSIZE=*value*	Values can include ANY, LETTER, STATEMENT, EXECUTIVE, or other supported paper type names. The terms are case-sensitive.	Sets the paper size for Tray 1.
@PJL XMEDIASOURCE=*value*	Values can include ANY or TRAYn, where n is the number of the tray.	Sets the media source.
@PJL XMEDIATYPE=*value*	Values can include ANY, PAPER, LABEL, or other supported media type names. The terms are case-sensitive.	Sets the paper type.
@PJL XPCLTRAYSWITCH=*value*	ON, OFF	This command switches trays when a tray becomes empty. If AutoSelect is chosen as the tray in PCL, then tray switching is always active, regardless of the value. When the current tray becomes empty, the printer attempts to switch to another tray with the same size and type of paper. This command only takes effect when a specific tray, such as Tray 2, is selected in the job. When this command is ON, tray switching still occurs when the tray becomes empty. When this command is OFF, no switching occurs and the user is prompted to load paper.

PJL Command	Values	Description
@PJL XPCLPAPERSRCx = y	The value x is 0, 1, 2, 3, 4, 5, 6, 7, 8, 20, 21, 22, 23. The value x represents the number in the <Esc>&l#H tray selection commands. The value y is -1 for AutoSelect and 0 for the current tray (eject page). The value y is 1 for Tray 1, 2 for Tray 2, etc., and 99 for the factory defaults.	Overrides the tray selected in the <Esc>&l#H PCL tray selection commands.
*See the *HP Printer Job Language Technical Reference* for the values.		