Office Printers

XEROX

Phaser® 6300/6350 color laser printer
Phaser® 8500/8550 color printer

System Administrator Guide

www.xerox.com/office/support

Copyright © 2005 Xerox Corporation. All Rights Reserved. Unpublished rights reserved under the copyright laws of the United States. Contents of this publication may not be reproduced in any form without permission of Xerox Corporation.

Copyright protection claimed includes all forms of matters of copyrightable materials and information now allowed by statutory or judicial law or hereinafter granted, including without limitation, material generated from the software programs which are displayed on the screen such as styles, templates, icons, screen displays, looks, etc.

XEROX®, The Document Company®, the digital X®, CentreWare®, Phaser®, PhaserShare®, PhaserSMART®, and Walk-Up™ are trademarks of Xerox Corporation in the United States and/or other countries.

Adobe® and PostScript® are trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Apple®, AppleTalk®, Bonjour™, EtherTalk®, Macintosh®, and Mac OS® are trademarks of Apple Computer, Inc. in the United States and/or other countries.

PCL® is a trademark of Hewlett-Packard Corporation in the United States and/or other countries.

Windows®, Windows NT®, and Windows Server™ are trademarks of Microsoft Corporation in the United States and/or other countries.

Sun℠, Sun Microsystems™, and Solaris® are trademarks of Sun Microsystems, Incorporated in the United States and/or other countries.

UNIX® is a trademark in the United States and other countries, licensed exclusively through X/Open Company Limited.

Contents

4 Security Features

5 Printing Features

6 Glossary

A Configuration Card Parameters

1 Overview

This section includes:

You can obtain information regarding your printer and its capabilities from the following sources.

Resources

Information	Source
Setup Guide*	Packaged with printer
Quick Reference Guide*	Packaged with printer
User Guide (PDF)*	*Software and Documentation CD-ROM*
Advanced Features Guide (PDF)	www.xerox.com/office/support
Videos	www.xerox.com/office/support
Printer Management Tools	www.xerox.com/office/pmtools
Knowledge Base	www.xerox.com/office/support
PhaserSMART Technical Support. For more information, see PhaserSMART Technical Support on page 1-2.	www.phaserSMART.com
Technical Support	www.xerox.com/office/support
Information about menu selection or error messages on the control panel	Control panel **Help** (**?**) button
Information pages	Control panel menu

* Also available on the Support website.

PrintingScout Alerts

PrintingScout is an automated tool that is installed with the Xerox printer driver. It automatically checks the printer status when a print job is sent. If the printer is unable to print a job, PrintingScout automatically displays an alert on the user's computer screen to let them know that the printer needs attention. The user can click the alert to view instructions explaining how to fix the problem. PrintingScout provides real-time support to users, while eliminating many of the help calls requesting printer support. PrintScouting saves you time for more critical tasks.

PhaserSMART Technical Support

PhaserSMART Technical Support is an automated, internet-based support system that uses the user's default web browser to send diagnostic information from their printer to the Xerox website for analysis. PhaserSMART Technical Support examines the information, diagnoses the problem, and proposes a solution. If the problem is not resolved with the solution, PhaserSMART Technical Support assists the user in opening a Service Request with Xerox Customer Support.

PhaserSMART provides support to users, while eliminating many of the help calls requesting printer support. PhaserSMART Technical Support saves you time for more critical tasks.

Use one of the following options to access PhaserSMART Technical Support:

- PrintingScout
- Web
- CentreWare IS
- The printer driver
- Xerox Support Centre

Using PrintingScout

If PrintingScout displays an alert on your screen, do the following:

1. Click the alert to view instructions explaining how to fix the problem.
2. Follow the instructions on the screen.

Using the Web

To access PhaserSMART Technical Support from the web:

1. Open your browser and go to www.phaserSMART.com.
2. Enter your printer's IP address in the browser window.
3. Follow the instructions on the screen.

Using CentreWare IS

To access PhaserSMART Technical Support from CentreWare IS:

1. Launch your web browser.
2. Enter your printer's IP address in the browser's **Address** field (http://xxx.xxx.xxx.xxx).
3. Click **Support**.
4. Select the **PhaserSMART Diagnostic Tool** link.
5. Follow the instructions on the screen.

Using a Windows Printer Driver

To access PhaserSMART Technical Support from your printer driver:

1. Select **Start**, select **Settings,** and then select **Printers**.
2. Right-click the printer name, and then select **Properties**.
3. Select the **Troubleshooting** tab.
4. Select the **PhaserSMART Technical Support** link.
5. Follow the instructions on the screen.

Using the Xerox Support Centre

To access PhaserSMART Technical Support from the Xerox Support Centre:

1. Select one of the following options:
   - **Windows**: Double-click the **Xerox Support Centre** icon on your desktop.
   - **Macintosh**: Click the **Xerox Support Centre** icon in the dock.
2. Select your printer from the **Select Printer** drop-down list.
3. Select the **Troubleshooting** tab.
4. Select the **Advanced Troubleshooting Resources** link.
5. Click the **PhaserSMART** icon.

Xerox Support Centre

See also:

Xerox Support Centre on page 1-4

Xerox Support Centre

The **Xerox Support Centre** is a utility that is installed when running the driver installer. It is available for systems with Windows 2000 and later or Mac OS X, version 10.2 and higher.

The **Xerox Support Centre** appears on the desktop for Windows systems or is placed in the Mac OS X dock. It provides a central location for accessing the following information:

- User manuals and video tutorials
- Solutions to troubleshooting problems
- Printer and supplies status
- Supplies ordering and recycling
- Answers to frequently asked questions
- Default printer driver settings (Windows only)

Note: Xerox recommends that the Xerox driver installer be used to add a printer instead of the Microsoft Add Printer Wizard. If the Microsoft Add Printer Wizard is used, the Xerox Support Centre is not installed on the PC. Also, the Xerox driver installer installs the Xerox printer driver, enabling users to work more efficiently by accessing printer features and resources to solve simple problems. This eliminates many of the help calls requesting printer support, saving you time for more critical tasks.

To start the Xerox Support Centre utility:

1. Select one of the following options:
   - **Windows**: Double-click the **Xerox Support Centre** icon on your desktop.
   - **Macintosh**: Click the **Xerox Support Centre** icon in the dock.
2. Select your printer from the **Select Printer** drop-down list.

Xerox Support Centre

2 Network Installation Features

This chapter includes:

See also:

Advanced Features Guide at www.xerox.com/office/support

Using a Startup Network Configuration File

This section includes:

About the Configuration File

To configure printer settings or to perform other tasks, such as loading fonts, color tables, and job patches, you can create a startup network configuration file. Every time the printer is turned on or reset, the TFTP service on the TFTP server downloads the configuration file once an IP address is acquired and confirmed in the printer. The TFTP service processes the data in the configuration file as if it were a standard print job.

Configuration File Requirements

The configuration file must be:

- A valid PostScript or PCL file that contains the appropriate PostScript, PCL, or PJL commands. For a list of the Xerox-unique PCL and PJL commands, see Printer Commands on page B-1.
- 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, do one of the following:

- If the printer is connected to a TCP/IP network in a DHCP/BOOTP environment, use the DHCP/BOOTP environment.
  - Use DHCP option 66 to specify the TFTP server IP address or hostname.
  - Use DHCP option 67 to specify the pathname of the configuration file.

  For information on how to set these parameters, refer to your DHCP or BOOTP server documentation.
- If the printer is connected to a TCP/IP network in a non-DHCP environment, use CentreWare Internet Services (IS). On the **TCP/IP Settings** page, under **TFTP Settings**, do the following:
  - Enter the TFTP server IP address or hostname in the **TFTP Server Name** field.
  - Enter the pathname of the configuration file in the **Boot File Name** field.

  For more information, see the *CentreWare IS Online Help*.

Printer Driver Installation Features

This section includes:

Walk-Up Printing Driver

The Xerox Walk-Up Printing Driver enables printing from a PC to any Xerox Postscript-enabled printer. This is especially helpful for mobile professionals who travel to multiple locations and need to print to different printers. Instead of installing the printer drivers for each printer, you can download this driver from the web. Although it doesn't enable access to all printer-specific features, it does enable access to common printing features, such as 2-sided printing.

The driver contains basic features that are common to most of the Postscript-enabled printers, including:

- Portrait, landscape, and rotated landscape orientations
- Single-sided or two-sided printing
- Single or multiple pages per sheet (including booklet printing)
- Paper or transparency printing
- Page size selection

Note: For information about Xerox printer driver features that are available with specific operating systems, see Printer Driver Features in the *Advanced Features Guide* for your printer at www.xerox/office/support.

Walk-Up Installation

The Xerox Installer enables quick and easy installation of the printer driver. The installer is included on the *Software and Documentation CD-ROM,* supplied with the printer, and is available on the web. When you run the installer, the main screen lists the Xerox printers of that model discovered on the network or connected via USB. You can choose one of the discovered printers, enter the IP address of the desired printer, or use Walk-Up Technology. This technology is especially helpful when there is more than one Xerox printer on the discovered printers list and you don't know the printer's IP address. After selecting **Walk-Up Technology** and clicking the **Next** button on the main installer screen, you simply walk up to the desired printer and select **Walk-Up Features** and then **Select for Installation** on the control panel. The installer connects the computer to the printer, completes the driver installation, and then the printer prints a confirmation page.

Installation from the Printer's Hard Drive

If the printer has an internal hard drive, you can install the printer driver from the hard drive. This is especially useful if you do not have the *Software and Documentation CD-ROM*.

Note: If the printer doesn't have a hard drive but is connected to the internet, you can use this procedure to automatically connect to the web to install the driver.

To install the printer driver either from the hard drive or the web:

1. Launch your web browser.
2. Enter your printer's IP address in the browser's **Address** field (http://xxx.xxx.xxx.xxx).
3. Click **Support**.
4. Select **Software Installation** on the left sidebar.
5. Select the **Printer Drivers** link.
6. Do one of the following:
   - If you are a Windows user, click **Windows Driver Installer** to install the driver, and then click the **Install** button to install the printer.
   - If you are a Macintosh user, click **Macintosh Driver Installer** to download the driver.

Auto-Configuring Driver

For a printer connected to a network, the bi-directional communication between the driver and the printer during installation automatically tells the installer the printer's configuration (N, DN, DX, etc.) and, therefore, whether the printer has certain features, such as duplexing capability, additional trays, or a hard drive. As a result, the controls for settings, such as 2-sided printing, tray selection, and secure printing are displayed or hidden/grayed out, and the mimic shows the correct printer configuration. This driver feature prevents users from making incorrect selections during installation, eliminating many of the help calls requesting printer support.

Discovery Protocols

This section includes:

Multicast DNS

To change the Multicast DNS (Bonjour) settings:

1. Launch your web browser.
2. Enter your printer's IP address in the browser's **Address** field (http://xxx.xxx.xxx.xxx).
3. Click **Properties**.
4. Click the **Protocols** folder on the left sidebar.
5. Select **TCP/IP**.
6. If prompted, enter your Admin or Key User name and password.
7. Under **DNS Settings**, in the **Multicast DNS Enable** field, select one of the following:
   - **On**: The printer can respond to Multicast DNS and be automatically discovered on an IP network by Apple Macintosh OS X technology.
   - **Off**: The printer cannot be automatically discovered.
8. If you selected **On**, follow the instructions on the page. For more information, including a description of the fields, click the **Help** button in CentreWare IS to view the online help.
9. Click the **Save Changes** button.
10. If prompted, enter your Admin or Key User name and password.

Service Location Protocol

To change the configuration of the Service Location Protocol (SLP) Service Agent in the printer:

1. Launch your web browser.
2. Enter your printer's IP address in the browser's **Address** field (http://xxx.xxx.xxx.xxx).
3. Click **Properties**.
4. Click the **Protocols** folder on the left sidebar.
5. Select **TCP/IP**.
6. If prompted, enter your Admin or Key User name and password.
7. Under **Service Location Protocol (SLP) Settings**, in the **SLP Enable** field, select **On** or **Off**.
8. If you selected **On**, follow the instructions on the page. For more information, including a description of the fields, click the **Help** button in CentreWare IS to view the online help.
9. Click the **Save Changes** button.
10. If prompted, enter your Admin or Key User name and password.

3 Network Administration Features

This chapter includes:

Printer Neighborhood

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

The default printer search mode is **Quick Phaser Search**, which quickly finds the Phaser printers on your local subnet. To search for all types of printers or to change other defaults, click the **Preferences** tab.

Note: Javascript is required in order to access and use pages in Printer Neighborhood. If Javascript is disabled, a warning message is displayed and the pages will not function properly.

To access Printer Neighborhood:

1. Launch your web browser.
2. Enter your printer's IP address in the browser's **Address** field (http://xxx.xxx.xxx.xxx).
3. Click the **Printer Neighborhood** button.

   A list of network printers is displayed.
4. To view topics contained in Printer Neighborhood, click **Neighborhood Index**.

Job Accounting

The printer stores information about print jobs. This information is stored in a log file, which lists job records. Each job record contains fields such as user name, job name, pages printed, job times, and toner or ink used. Not all fields are supported by all printers. For more information about the fields supported, go to the *CentreWare IS Online Help* or *CentreWare Web Online Help*.

The job accounting values reported also vary depending on the protocol and print command used when each job was printed. For example, using Windows via the default standard TCP/IP port with the Xerox recommended PostScript driver specific to your model provides the printer with the most information about the job being printed. When using other drivers with various protocols, the operating system may enter unexpected information in certain fields, such as a job name listed as LST: or LST:BANNER.

The log file is stored either in the printer's RAM memory or on the hard drive if one is installed in the printer. Xerox recommends that a hard drive be used for job accounting.

- With a hard drive, the printer can store information about 5000 print jobs. The data in the log file is saved when the printer is turned off or reset.
- Without a hard drive, the printer can store information about the most recent 50 to 500 print jobs depending on available RAM. The data in the log file is not saved when the printer is turned off or reset.

Note: Data in job accounting records may be a security risk because the names of users, as well as the titles, date, time, and length of printed jobs can be exposed. The content of print job pages is not stored in the job accounting system.

Job accounting is available through CentreWare IS and CentreWare Web.

To access job accounting information using CentreWare IS:

1. Launch your web browser.
2. Enter the printer's IP address in the browser's **Address** field (http://xxx.xxx.xxx.xxx).
3. Click **Jobs**.

The **Job Accounting Links** page provides links that enable you to browse, download, and clear job accounting records. For complete information on CentreWare IS job accounting, including clearing job information, downloading job information to a file, and job accounting file formats, click the **Help** button in CentreWare IS to view the online help.

To access CentreWare Web, go to www.xerox.com/office/pmtools.

Usage Profile Reports

The printer generates reports accessible through CentreWare IS that detail device usage. Usage profile reports track multiple items, including:

- Printer information, such as printer name, date installed, total pages printed, options installed, and network ID.
- Supplies usage data, such as toner or ink. By tracking supplies usage, you can order supplies before they reach their end of life.
- Media and tray information, such as how often prints are made on paper compared to transparencies, and how often each tray is used.
- Job characteristics, such as size and timing of jobs.

Setting Up Usage Profile Reporting

To set up usage profile reporting:

1. Launch your web browser.
2. Enter the printer's IP address in the browser's **Address** field (http://xxx.xxx.xxx.xxx).
3. Click **Jobs**.
4. Select **Usage Profile Reports** on the left sidebar.
5. Click the **Usage Profile Properties** link. Follow the instructions on the page to set up reports. For more information, including a description of the fields, click the **Help** button in CentreWare IS to view the online help.
6. Click the **Save Changes** button.

Sending Usage Profile Reports

To send a usage profile report:

1. Launch your web browser.
2. Enter the printer's IP address in your browser's **Address** field (http://xxx.xxx.xxx.xxx).
3. Click **Jobs**.
4. Select **Usage Profile Reports** on the left sidebar.
5. Enter the desired email address in the **Send to Specific Address** field.
6. Click the **Send Usage Profile Report** button.

Note: To send usage profile reports using email, MaiLinX must be properly set up. See MaiLinX Remote Printing on page 3-10.

Xerox Usage Analysis Tool

The Xerox Usage Analysis Tool enables you to collect and analyze enterprise-wide Xerox network printer usage data with customizable features:

- **Cost Analysis**: Track printing costs by groups of users or by groups of printers.
- **Print Job Analysis**: Analyze print jobs to review media type, color coverage, paper source, and other job specifics. Plan your next consumable order based on prior usage.
- **Printer Usage Analysis**: Track printer usage patterns to identify printers that are underworked or overused.
- **Reports**: Collect and present printer data in a number of formats with complete transaction and summary reports designed for Excel or other custom billing systems.

For complete information about using the Xerox Usage Analysis Tool provided by the application's online help system, go to www.xerox.com/office/uat.

System Requirements

- IP network
- Xerox printer with Ethernet interface (optional hard drive recommended)
- Xerox Usage Analysis Tool client:
  - A PC with an Intel Pentium III processor or higher, at least 128 MB of RAM, and at least 500 MB of hard drive space recommended.
  - Operating systems supported: Windows 2000 Professional or later and Windows XP or later.
- Xerox Usage Analysis Tool server:
  - A PC with an Intel Pentium III processor or higher, at least 256 MB of RAM, and at least 1 GB of hard drive space recommended.
  - Operating systems supported: Windows 2000 or later, Windows XP or later, and Windows 2003 server or later.
- Framework: .NET Framework 1.1 (included with the Xerox Usage Analysis Tool)

Protocol Control

This section includes:

See also:

Discovery Protocols on page 2-5

All network protocols, including network printing, printing services, printer discovery, and management protocols can be enabled or disabled on the printer. If a protocol is enabled, you can set configuration parameters.

Note: To secure protocols, disable any protocols you are not using. This prevents unauthorized access through applications that use these protocols. For example, if you want to use IPP for a secure printing channel, disable the other printing protocols, Port 9100 and LPR.

HTTP

By default, HTTP is enabled. For information on disabling HTTP, contact Xerox Technical Support at www.xerox/office/support.

See also:

About HTTP, HTTPS, and SSL/TLS on page 4-3

TCP/IP

To change TCP/IP settings:

1. Launch your web browser.
2. Enter your printer's IP address in the browser's **Address** field (http://xxx.xxx.xxx.xxx).
3. Click **Properties**.
4. Select the **Protocols** folder on the left sidebar.
5. Select **TCP/IP**.
6. If prompted, enter your Admin or Key User name and password.
7. In the **BOOTP/DHCP** box, select one of the following:
   - **On**: The printer issues BOOTP and DHCP requests on startup.
   - **Off**: The printer does not issue BOOTP or DHCP requests on startup.

8. If you selected **Off**, follow the instructions in the **TCP/IP Settings** section to manually enter the printer's TCP/IP information.
   - Enter the TFTP server IP address or hostname in the **TFTP Server Name** field.
   - Enter the pathname of the configuration file in the **Boot File Name** field.
9. Under **DDNS/WINS Settings**, in the **DDNS** box, select one of the following:
   - **On**: The printer registers its IP name and address so other devices on the network can refer to it by name.
   - **Off**: The printer does not register its IP name and address. If **DDNS** is **Off**, these values may be set by **BOOTP/DHCP** if enabled.
10. If you selected **On**, follow the instructions in **DDNS/WINS Settings** to manually enter settings to identify the printer. For more information, including a description of the fields, click the **Help** button in CentreWare IS to view the online help.
11. Click the **Save Changes** button.
12. If prompted, enter your Admin or Key User name and password.

Port 9100

To change Port 9100 settings:

1. Launch your web browser.
2. Enter your printer's IP address in the browser's **Address** field (http://xxx.xxx.xxx.xxx).
3. Click **Properties**.
4. Select the **Protocols** folder on the left sidebar.
5. Select **Port 9100**.
6. If prompted, enter your Admin or Key User name and password.
7. Select **On** or **Off** in the **Port 9100** box.
8. If you selected **On**, follow the instructions on the page to select Port 9100 settings. For more information, including a description of the fields, click the **Help** button in CentreWare IS to view the online help.
9. Click the **Save Changes** button.
10. If prompted, enter your Admin or Key User name and password.

LPR

To change LPR settings:

1. Launch your web browser.
2. Enter your printer's IP address in the browser's **Address** field (http://xxx.xxx.xxx.xxx).
3. Click **Properties**.
4. Select the **Protocols** folder on the left sidebar.
5. Select **LPR**.
6. If prompted, enter your Admin or Key User name and password.
7. Select **On** or **Off** in the **LPR** box.

8. If you selected **On**, follow the instructions on the page to select LPR settings. For more information, including a description of the fields, click the **Help** button in CentreWare IS to view the online help.
9. Click the **Save Changes** button.
10. If prompted, enter your Admin or Key User name and password.

IPP

To change IPP settings:

1. Launch your web browser.
2. Enter your printer's IP address in the browser's **Address** field (http://xxx.xxx.xxx.xxx).
3. Click **Properties**.
4. Select the **Protocols** folder on the left sidebar.
5. Select **IPP**.
6. If prompted, enter your Admin or Key User name and password.
7. Select **On** or **Off** in the **IPP (Internet Printing Protocol)** box.
8. If you selected **On**, follow the instructions on the page to select IPP settings. For more information, including a description of the fields, click the **Help** button in CentreWare IS to view the online help.

   Note: To configure IPP for secure/encrypted printing, specify a username, password, and digest authentication (for Windows only). Every client that tries to print to the printer over IPP must enter this information. The user name and password are sent in plain text to the printer. If you specify digest authentication, the password is secured before it is sent to the printer.

9. Click the **Save Changes** button.
10. If prompted, enter your Admin or Key User name and password.

SNMP

For information on configuring SNMP, see Configuring SNMP on page 4-14.

FTP

To change FTP settings:

1. Launch your web browser.
2. Enter your printer's IP address in the browser's **Address** field (http://xxx.xxx.xxx.xxx).
3. Click **Properties**.
4. Select the **Protocols** folder on the left sidebar.
5. Select **FTP**.
6. If prompted, enter your Admin or Key User name and password.
7. Select **On** or **Off** in the **FTP** box.

8. If you selected **On**, follow the instructions on the page to select FTP settings. For more information, including a description of the fields, click the **Help** button in CentreWare IS to view the online help.
9. Click the **Save Changes** button.
10. If prompted, enter your Admin or Key User name and password.

Email Server

You can configure email server settings in CentreWare IS by either:

- Automatically identifying the SMTP email server (recommended).
- Manually specifying the SMTP email server.

You can also specify a return email address for undelivered email, such as MaiLinX alerts and usage profile reports, to your email address.

To configure email server settings:

1. Launch your web browser.
2. Enter the printer's IP address in the browser's **Address** field (http://xxx.xxx.xxx.xxx).
3. Click **Properties**.
4. Select the **Protocols** folder on the left sidebar.
5. Select **Email Server**.
6. If prompted, enter your Admin or Key User name and password.
7. Do one of the following:
   - To automatically identify the SMTP email server, click the **Use DNS to Identify SMTP Server (Automatic)** option, and then enter the **Primary Name Server IP Address** and the **Secondary Name Server IP Address** using the 4-byte IP address of the email server.
   - To manually specify the SMTP email server, click the **Specify SMTP Server Manually** option, and then enter the information for the email server. Set the 4-byte IP address of the SMTP Email Server to send alert notifications. If there is no DNS server, then only the IP Address is allowed.
8. (Optional) To specify an email address for returning undelivered email, enter your email address in the **Return Email Address** field.
9. Click the **Save Changes** button.
10. If prompted, enter your Admin or Key User name and password.

See also:

MaiLinX Alerts on page 3-11
Usage Profile Reports on page 3-4

MaiLinX Remote Printing

About MaiLinX Remote Printing

MaiLinX Remote Printing provides the following key features:

- The ability to send print jobs to a group of printers.
- Print services across firewalls and proxies.
- Status reporting using email messages.

MaiLinX Remote Printing consists of two parts:

- Client software installed on each user's workstation or PC enables users to send print jobs from Windows applications to Xerox printers over the Internet. The client software enables users to set up their Internet-connected printers and create groups and subgroups of printers for easy distribution of print jobs.
- A CentreWare IS Printing Service on a Xerox printer processes the print jobs from the clients.

System Requirements

- The client software requires an SMTP-capable email server/forwarder through which the client software on the user's computer can send email.
- Each printer requires an account on a POP3-capable email server from which it can retrieve email.

Setting Up MaiLinX Remote Printing

To set up your printer for remote printing:

1. Launch your web browser.
2. Enter the printer's IP address in the browser's **Address** field (http://xxx.xxx.xxx.xxx).
3. Click **Properties**.
4. Select the **Protocols** folder on the left sidebar.
5. Select **Remote Printing**.
6. If prompted, enter your Admin or Key User name and password.
7. Set the **MaiLinX Remote Printing** box to **On**. Follow the instructions on the **MaiLinX Remote Printing** page to set up your printer for remote printing. For more information including a description of the fields, click the **Help** button in CentreWare IS to view the online help.

MaiLinX Alerts

About MaiLinX Alerts

MaiLinX alerts enable the printer to automatically send email to you and/or specified users when the following conditions occur:

- The printer requires attention or when service is needed.
- The printer displays an error, warning, or alert.
- A reply to a MaiLinX Remote Printing message is desired.

For more information, click the **Help** button in CentreWare IS to view the online help.

Setting Up MaiLinX Alerts

To enable MaiLinX alerts:

1. Launch your web browser.
2. Enter the printer's IP address in the browser's **Address** field (http://xxx.xxx.xxx.xxx).
3. Click **Properties**.
4. Select the **General** folder on the left sidebar.
5. Select **Mail Alerts**.
6. If prompted, enter your Admin or Key User name and password.
7. Select **On** in the **MaiLinX (and Usage Profile Properties)** box.
8. Follow the instructions on the page to specify up to three users to receive messages: Admin, Key User, and Service. You can also select advanced settings for:
   - Specifying email server settings.
   - Reading or changing default messages.
   - Reading or changing conditions and trigger settings.
9. Click the **Save Changes** button.
10. If prompted, enter your Admin or Key User name and password.

EtherTalk

To change EtherTalk settings:

1. Launch your web browser.
2. Enter the printer's IP address in the browser's **Address** field (http://xxx.xxx.xxx.xxx).
3. Click **Properties**.
4. Select the **Protocols** folder on the left sidebar.
5. Select **EtherTalk**.
6. If prompted, enter your Admin or Key User name and password.
7. Select **On** or **Off** in the **EtherTalk** box.
8. If you selected **On**, follow the instructions on the page to select Ethertalk options. For more information, including a description of the fields, click the **Help** button in CentreWare IS to view the online help.
9. Click the **Save Changes** button.
10. If prompted, enter your Admin or Key User name and password.

Cloning

Cloning enables you to configure one printer and then copy that configuration to another printer on the same network. You can access cloning using CentreWare IS or CentreWare Web. Using CentreWare IS, you can select the settings you want to clone from one printer to another printer. Using CentreWare Web, you can select the settings you want to clone from one printer to one or more printers.

To clone settings from one printer to another printer using CentreWare IS:

1. Launch your web browser.
2. Enter your printer's IP address in the browser's **Address** field (http://xxx.xxx.xxx.xxx).
3. Click **Properties**.
4. Select **Clone Printer** on the left sidebar.
5. If prompted, enter your Admin or Key User name and password.
6. On the **Clone Printer** page, select the settings you want to clone from the source printer or click **Check All** to select all the settings. The settings are:
   - Usage Profile Properties
   - FTP
   - EtherTalk
   - Information Forwarding
   - E-Supplies
   - Printer Defaults
   - LPR
   - Security
   - Date and Time
   - Warmup
   - Control Panel Lockout
   - TCP/IP
   - Email Server
   - MaiLinX Alerts
   - USB
   - PostScript
   - Remote Printing
   - IPP (Internet Printing Protocol)
   - Port 9100
   - SNMP
   - PCL
   - SSL Configuration
7. Enter the IP address or DNS Name of the destination printer in the **IP Address** or **DNS Name** field.
8. (Optional) To assign a printer name to the destination printer, enter this name in the **Printer Name (SNMP System Name)** field.
9. If the destination printer is located in a different domain/zone, modify the information in the **EtherTalk Zone** and/or **IP Domain Name** fields.

10. Click the **Clone Selected Settings** button.

    A list of the selected settings to clone is displayed.

11. Click the **Clone** button to clone the destination printer with the selected settings from the source printer.
12. If prompted, enter the Admin or Key User name and password.

To access CentreWare Web, go to www.xerox.com/office/pmtools.

4 Security Features

This chapter includes:

See also:

Jam Recovery on page 5-5

Basic Concepts

This section includes:

About Admin and Key User Accounts

Admin and Key User accounts in CentreWare IS enable you to limit access to specific printer functions by specifying passwords for user classes. CentreWare IS requires a name and password before access to the controlled printer functions are allowed.

The user classes are:

- **Admin**: The person with the ultimate management responsibility and authority for controlling all functions of the printer.
- **Key User**: A person who has some administrative responsibilities and who manages some or all of the printer functions.
- **Any User**: Includes the majority of people who will be sending print jobs to the printer.

Once the passwords are set, select the printer functions that each user class has the right to access. The three categories of printer functions are:

- Administrative Functions
- Web Server Printing
- Printer Neighborhood Functions

See also:

Configuring Administrator and Key User Settings on page 4-8

About HTTP, HTTPS, and SSL/TLS

HTTP (Hyper Text Transfer Protocol) is the protocol used to communicate across the internet between the printer web server and the web browser (clients). Because the data is transmitted in plain text and passwords are only slightly encrypted, it is not secure; the data can be read or intercepted by other people.

HTTPS (Secure Hyper Text Transfer Protocol) is a secure version of HTTP. HTTPS provides authentication and encrypted communication to preserve the confidentiality of your data. Instead of using plain text, HTTPS uses either the SSL (Secure Socket Layer) protocol or the TLS (Transport Layer Security) protocol to encrypt data, thus ensuring reasonable protection from eavesdroppers and man-in-the-middle attacks.

Before using HTTPS, you must set up a certificate and select when to use SSL to encrypt data. You can set the printer to use SSL either to secure web pages that use passwords or to secure all web pages.

See also:

About Certificates on page 4-3
Setting Up a Certificate on page 4-6
Configuring SSL on page 4-7

About Certificates

A certificate is an electronic message containing information about the printer and a digital signature. A certificate is stored in the printer and is used to validate the identity of the printer to clients and network servers and to allow encrypted communication.

Before configuring passwords, set up a certificate and then configure SSL to encrypt data including passwords for maximum security. You can set up a self-signed certificate or download a root-signed certificate, depending on your requirements.

See also:

Self-Signed Certificates on page 4-3
Root-Signed Certificates on page 4-4

Self-Signed Certificates

Setting up a self-signed certificate is a quick and easy to establish a certificate on the printer. The printer automatically generates a default self-signed certificate when the printer is turned on for the first time. To modify the certificate so it is specific to your printer, use CentreWare IS to enter information about the location of the printer.

While self-signed certificates are safe for most applications and allow data encryption, they do not ensure valid authentication. Self-signed certificates are not necessarily secure because the certificate owner is only confirming his own identify instead of verification by a trusted third party. Although self-signed certificates encrypt the data that is exchanged, they do not prevent man-in-the-middle attacks.

If you want to use HTTPS, each printer must have a unique certificate that is accepted by each browser used to access the printer. This allows the printer web server to use HTTPS and encrypt data between the web browser and the printer. In addition, because each printer's certificate is unique, you must load a different certificate into the browser for each printer the browser will access.

Root-Signed Certificates

Root-signed certificates are from a trusted Certificate Authority (CA). Using a certificate signed by a CA enables you to load one certificate into each browser, allowing access to all printers. Certificates from a trusted third party are considered more secure than self-signed certificates. Unlike self-signed certificates, root-signed certificates are not susceptible to man-in-the-middle attacks.

See also:

Setting Up a Certificate on page 4-6
Configuring SSL on page 4-7

About Access Control Lists

Access control lists enable you to limit access to devices, as well as device configuration and management features. By default, access control lists are unrestricted, which means all computers and host systems are allowed access.

The printer has four access control lists that may be configured using CWIS:

- **Print Host Access List**: The computers from which users can print. For information on setting up the Print Host Access List, see Configuring the Print Host Access List on page 4-9.
- **Administrator Access List**: The computers from which you can change printer settings. For information on setting up the Administrator Access List, see Configuring Administrator and Key User Settings on page 4-8.
- **Key User Access List**: The computers from which key users can change printer settings. For information on setting up the Key User Access List, see Configuring Administrator and Key User Settings on page 4-8.
- **SNMP Access List**: The host machines that are authorized to access the printer using SNMP. For information on setting up the SNMP Access List, see Configuring the SNMP Access Control List on page 4-18.

Securing the Printer in a High Security Environment

If you are concerned about the security of your printer in a high security environment, such as a college or printing kiosk, you can configure settings in CentreWare IS to “lockdown” or fully secure the printer. If you are not concerned about the security of your printer, you may only need to set up a certificate and then configure SSL to encrypt data including passwords.

To fully secure a printer:

1. Set up a certificate. (See Setting Up a Certificate on page 4-6.)
2. Select when to use SSL. (See Configuring SSL on page 4-7.)

   Note: The following steps may be completed in any order.

3. Select the Administrator and Key User Settings. (See Configuring Administrator and Key User Settings on page 4-8.)

   Note: To prevent users from changing settings, clear the **Modify Configuration Web Pages** check box. To prevent users from viewing settings, clear the **View Configuration Web Pages** check box.

4. Set up the Print Host Access List. (See Configuring the Print Host Access List on page 4-9.)
5. Select the Hard Drive Overwrite option. (See Securing the Hard Drive on page 4-10.)
6. Select the Jam Recovery option. (See Jam Recovery on page 5-5.)
7. Lock the control panel menus. (See Locking the Control Panel Menus on page 4-13.)
8. Configure SNMP. (See Configuring SNMP on page 4-14.)
9. Disable unused protocols. (See Protocol Control on page 3-6.)

   Note: To secure protocols, disable any protocols you are not using. This prevents unauthorized access through applications that use these protocols. For example, if you want to use IPP for a secure printing channel, disable the other printing protocols, Port 9100 and LPR. Disabling some protocols also disables some printer functions, such as printer discovery and PrintingScout.

Setting Up a Certificate

To modify a self-signed certificate so it is specific to your printer or to install a downloaded root-signed certificate on the printer:

1. Launch your web browser.
2. Enter your printer's IP address in the browser's **Address** field (http://xxx.xxx.xxx.xxx).
3. Click **Properties**.
4. Select the **Security** folder on the left sidebar.
5. Select **SSL**.
6. If prompted, enter your Admin or Key User name and password.

   The **Current State** field displays the current state of the printer. Possible values include:

   - **A digital certificate is not established on this machine**. This state displays if an error occurred when the certificate was created.
   - **A self-signed certificate is established on this machine.**
   - **A digital certificate has been installed on this machine.**
7. Click the **Create Certificate** button.
8. Do one of the following:
   - To modify a self-signed digital certificate, select **Self-Signed Certificate**.
   - To install a signed digital certificate that includes a private key from a trusted Certificate Authority (CA), select **Install downloaded Certificate**.
9. Click the **Next** button.
10. Do one of the following:
    - If you selected **Self-Signed Certificate**, enter the appropriate information in the fields, and then click the **Finish** button to save the settings. For more information, including a description of the fields, click the **Help** button in CentreWare IS to view the online help.
    - If you selected **Install Downloaded Certificate**, click the **Browse** button to select the certificate from the PC's hard drive, and then click the **Finish** button to validate and install the certificate. Once the certificate is installed, the main SSL page displays.

See also:

About Certificates on page 4-3

Configuring SSL

Once a certificate is set up, you can select when to use SSL to secure the connection between the printer and the server.

Note: You can restrict user access to SSL pages in CentreWare IS. For more information, see Configuring Administrator and Key User Settings on page 4-8.

To configure SSL:

1. Launch your web browser.
2. Enter your printer's IP address in the browser's **Address** field (http://xxx.xxx.xxx.xxx).
3. Click **Properties**.
4. Select the **Security** folder on the left sidebar.
5. Select **SSL**.
6. If prompted, enter your Admin or Key User name and password.
7. In the **Use SSL** box, select one of the following options:
   - **Never** (the default): SSL authentication is not required.
   - **To Secure Passwords**: Secures web pages that use passwords.
   - **To Secure Pages and Passwords**: Secures all web pages.
8. Click the **Save Changes** button.
9. If prompted, enter your Admin or Key User name and password.

See also:

Setting Up a Certificate on page 4-6

Configuring Administrator and Key User Settings

To prevent unauthorized changes to printer settings:

1. Launch your web browser.
2. Enter your printer's IP address in the browser's **Address** field (http://xxx.xxx.xxx.xxx).
3. Click **Properties**.
4. Select the **Security** folder on the left sidebar.
5. Select **Administrative Security Settings**.
6. If prompted, enter your Admin or Key User name and password.
7. In the **Administrator Settings** box, do one or both of the following:
   - In the **Host Access List** field, enter the IP addresses or host names of the computers allowed to change printer settings. Separate entries with a blank or a comma, specify ranges with a hypen (-), and use an asterisk (*) to represent a group of numbers (e.g., 13.62.156.*). The default setting is **Unrestricted**, which allows all users to change printer settings.
   - In the **User Name** and **Password** fields, enter your user name and password (up to 10 alphanumeric characters). In **Verify Password**, re-enter the password. The user name and password should be kept secure.
8. Repeat Step 7 in the **Key User** box. When entering the user name and password, enter the user name and password for key users.

   Note: If you want to use the Key User account, you must configure an Administrator account. If the Administrator account is empty, then Any User has the same permissions as the Administrator user.

9. In the **Feature Authorization Settings** box, select the check boxes next to the settings you want to enable for each type of user. Clear the check boxes next to the settings you want to prevent users from changing. The administrator has full rights and access to all functions. Any User may not have greater access to a function than the Key User.

   Note: If you want to prevent users in the **Key User** or **Any User** classes from using CentreWare IS to change printer settings, clear the **Modify Configuration Web Pages** check box. If you want to prevent users in the **Key User** or **Any User** classes from viewing CentreWare IS pages that control printer settings, clear the **View Configuration Web Pages** check box.

10. Click the **Save Changes** button.
11. If prompted, enter your Admin or Key User name and password.

See also:

About Admin and Key User Accounts on page 4-2

Configuring the Print Host Access List

To prevent unauthorized printing to your printer:

1. Launch your web browser.
2. Enter your printer's IP address in the browser's **Address** field (http://xxx.xxx.xxx.xxx).
3. Click **Properties**.
4. Select the **Security** folder on the left sidebar.
5. Select **Printing Security Settings**.
6. If prompted, enter your Admin or Key User name and password.
7. Enter the IP addresses or host names of the computers allowed printing access in the **Host Access List** field. Separate entries with a blank or a comma, specify ranges with a hypen (-), and use an asterisk (*) to represent a group of numbers (e.g., 13.62.156.*). The default setting is **Unrestricted**, which allows all users to access the printer to print their jobs.
8. Click the **Save Changes** button.
9. If prompted, enter your Admin or Key User name and password.

See also:

About Access Control Lists on page 4-4

Securing the Hard Drive

This section includes:

Selecting the Hard Drive Overwrite Security Option

When a file is deleted from the printer's hard drive, only the file name is deleted; the data in the file remains on the hard drive, regardless of the operating system. An unauthorized person could, possibly, retrieve the data in the file that was deleted.

Printers with a hard drive have a Hard Drive Overwrite Security option. This option overwrites the data stored on the hard drive of a file marked for deletion using DOD5200.28-M, a U.S. Department of Defense three-pass overwriting process: first with a pattern of 0's, next with a pattern of 1's, and finally with a random pattern of bits. This is done before the file's directory entry is removed and the storage space on the hard drive is marked as available for reuse. The random pattern of bits stays on the hard drive until it is overwritten by another file.

By default, the Hard Drive Overwrite Security option is disabled. To select the Hard Drive Overwrite Security option, use one of the following methods:

- The printer's control panel
- CentreWare IS

Using the Control Panel

To select the Hard Drive Overwrite Security option:

1. On the control panel, select **Printer Setup**, and then press the **OK** button.
2. Select **File Security**, and then press the **OK** button.

   Note: If **File Security** is locked on the control panel, use CentreWare IS to select the Hard Drive Overwrite Security option.

3. Select **Overwrite Removals**, and then press the **OK** button.
4. Select **On** or **Off**, and then press the **OK** button.

Using CentreWare IS

To select the Hard Drive Overwrite Security option:

1. Launch your web browser.
2. Enter the printer's IP address in the browser's **Address** field (http://xxx.xxx.xxx.xxx).
3. Click **Properties**.
4. Select the **Security** folder on the left sidebar.
5. Select **Printing Security Settings**.

6. If prompted, enter your Admin or Key User name and password.
7. Under **Hard Drive Overwrite Security Options**, select one of the following options:
   - **Never overwrite files/jobs**: Disables the printer's overwrite feature.
   - **Always overwrite when deleting files/jobs**: Sets the printer to always overwrite the files on the hard drive when they are deleted.
8. Click the **Save Changes** button.
9. If prompted, enter your Admin or Key User name and password.

Selecting the Automatic Removal of Secure, Personal, and Proof Jobs Option

The printer enables you to store secure, personal, and proof jobs on the hard drive and then print them later. You can choose how long these jobs remain on the hard drive. This feature is useful when someone:

- Forgets about an unprinted secure, personal, or proof job that was stored on the hard drive.
- Sends a secure job to the printer, but does not walk to the printer to print the job.
- Stores a proof job, prints it once, and then forgets to delete it.

To set the automatic removal of secure, personal, and proof print files from the hard drive, use one of the following methods:

- The printer's control panel
- CentreWare IS

Using the Control Panel

To select the automatic removal of secure, personal, and proof print files from the hard drive:

1. On the control panel, select **Printer Setup**, and then press the **OK** button.
2. Select **File Security**, and then press the **OK** button.

   Note: If **File Security** is locked on the control panel, use CentreWare IS to select the Hard Drive Overwrite Security option.

3. To remove all secure, personal, and proof print job files:
   a. Select **Overwrite Removals**, and then press the **OK** button.
   b. Select **On** or **Off**, and then press the **OK** button.

   Note: **Remove Job Files** does not remove saved or protected print job files.

4. To remove all secure, personal, and proof print files every day at a set time:
   a. Select **Daily Removal**, and then press the **OK** button.
   b. Select **On** or **Off**, and then press the **OK** button.
   c. Select **Remove At HH:MM**, and then press the **OK** button.
   d. Enter the hour, and then press the **OK** button.
   e. Enter the minute, and then press the **OK** button.
5. To remove all secure, personal, and proof print files after the files are a certain age or older:
   a. Select **Age-based Removal**, and then press the **OK** button.
   b. Select **On** or **Off**, and then press the **OK** button.
   c. If you selected **On**, select **Remove At Age**, and then press the **OK** button.
   d. Enter **1** to **999** hours, and then press the **OK** button.

Note: To reset all items in the File Security menu to their default values, select **Reset File Security**.

Using CentreWare IS

To select the automatic removal of secure, personal, and proof print files from the hard drive:

1. Launch your web browser.
2. Enter the printer's IP address in the browser's **Address** field (http://xxx.xxx.xxx.xxx).
3. Click **Properties**.
4. Select the **Security** folder on the left sidebar.
5. Select **Printing Security Settings**.
6. If prompted, enter your Admin or Key User name and password.
7. Under **Remove Unprinted Personal**, **Secure and Proof Jobs**, select one or more of the following options:
   - **Upon Save Changes**: All personal, secure, and proof jobs are removed when you click the **Save Changes** button.
   - **At this time each day (24hr)**: All unprinted personal, secure, and proof jobs are removed at this time each day.
   - **When jobs are**: All unprinted, personal, secure, and proof jobs are removed when they are this age or older.

   Note: Files deleted using one of these options are overwritten if the Hard Drive Overwrite Security option has been enabled. For more information, see Selecting the Hard Drive Overwrite Security Option on page 4-10.

8. Click the **Save Changes** button.
9. If prompted, enter your Admin or Key User name and password.

Locking the Control Panel Menus

To prevent others from changing settings in the printer setup menus, you can lock some or all of the control panel menus. This is useful when printers are located in public places, such as schools, libraries, and office/print centers.

Use CentreWare IS to lock or unlock the control panel menus:

1. Launch your web browser.
2. Enter your printer's IP address in the browser's **Address** field (http://xxx.xxx.xxx.xxx).
3. Click **Properties**.
4. Select the **Security** folder on the left sidebar.
5. Select **Control Panel Lockout**.
6. If prompted, enter your Admin or Key User name and password.
7. Select the check box of each control panel menu item you want to lock.

   Note: If you lose the Admin password and **Reset NVRAM** is locked on the control panel, a Fee-For-Service call is required to reset the password and to enable changes to printer settings. When the password is reset, you must reconfigure the printer settings because all the stored data is deleted.

8. Click the **Save Changes** button.
9. If prompted, enter your Admin or Key User name and password.

Configuring SNMP

This section includes:

If you are using SNMP, you must configure it using CentreWare IS. If you are not using SNMP, disable it to prevent unauthorized access through applications that use SNMP. For information on disabling SNMP, see Disabling SNMP on page 4-19.

Note: The **Current State** field on the **SNMP Configuration page** identifies the SNMP enable/disable status. Possible values include **SNMP v3 Enabled**, **SNMP v1/v2c Enabled**, and **All SNMP Protocols Disabled**.

Configuring SNMP for Maximum Security

Use CentreWare IS to configure SNMP for maximum security:

1. Launch your web browser.
2. Enter the printer's IP address in the browser's **Address** field (http://xxx.xxx.xxx.xxx).
3. Click **Properties**.
4. Select SSL:
   a. Select the **Security** folder on the left sidebar, and then select **SSL**.
   b. If prompted, enter your Admin or Key User name and password.
   c. On the **SSL** page, for **Use SSL**, select **To Secure Pages and Passwords**.
5. Restrict access to the CentreWare IS SNMP and SSL pages:
   a. Select **Administrative Security Settings** on the left sidebar.
   b. If prompted, enter your Admin or Key User name and password.
   c. On the **Administrative Security Settings** page, clear the **View Configuration Web Pages** and **Modify Configuration Web Pages** check boxes for users who should not have access to these pages.
6. Configure SNMP v3 by setting up the SNMP Administrative and Key User accounts:
   a. Select the **Protocols** folder on the left sidebar, and then select **SNMP**.
   b. If prompted, enter your Admin or Key User name and password.
   c. On the **SNMP Configuration** page, click the **Configure SNMP v3** button and set up the SNMP Administrative account. For more information, see Configuring SNMP v3 on page 4-16.

Configuring SNMP v1/v2c

Configuring SNMP v1/v2c Community Names

To configure SNMP v1v2c community names:

1. Launch your web browser.
2. Enter the printer's IP address in the browser's **Address** field (http://xxx.xxx.xxx.xxx).
3. Click **Properties**.
4. Select the **Protocols** folder on the left sidebar.
5. Select **SNMP**.
6. If prompted, enter your Admin or Key User name and password.
7. On the **SNMP Configuration** page, click the **Configure SNMP v1/v2c** button.
8. To set community names for GET/SET SNMP queries and traps, enter information (up to 32 alphanumeric characters) in one or more of the following fields:

   Note: These names are not displayed on this page, but are shown as a row of asterisks (*).

   - **GET Community Name**: Allows a host to perform SNMP GETS on the printer using this community name.
   - **SET Community Name**: Allows a host to perform SNMP SETS on the printer using this community name.
   - **Trap Community Name**: Allows a host to receive traps from the printer using this community name.

   Note: Hosts must have these community names configured in their applications to access the printer using **SNMP v1/v2c**.

9. Click the **Apply** button to save the changes.
10. If prompted, enter your Admin or Key User name and password.

Adding or Editing Traps for SNMP v1/v2c

To add or edit traps for SNMP v1v2c:

1. On the **SNMP Configuration: Configure SNMP v1v2c** page, click the **Configure Traps** button.

   The **SNMP Configuration: Configure Traps** page lists the current Trap Destination Addresses for the SNMP protocol.

   - The **Address** column lists the Trap Destination IP address or DNS Name.
   - The **Version/Type** column lists the SNMP Trap version or Inform Request for sending to the specified trap address. SNMP Trap versions include SNMP v1 Traps, SNMP v2c Traps, and SNMP v2c Inform Requests.
   - The **Traps** column lists the types of traps to send to the Trap Destination Address. Traps to be received include Printer Traps, Job Monitoring Traps, Cold Start, and Authentication Traps.

2. Do one of the following:
   - To add traps for SNMP v1v2c, click the **Add Destination** button, and then go to Step 3.
   - To edit the settings for a Trap Destination Address, click the corresponding **Edit** button, and then go to Step 3.
   - To delete a Trap Destination Address, click the corresponding **Delete** button.
3. To add or edit a Trap Destination IP Address, click the **IP Address** radio button, and then enter the IP Address in the fields.
4. To add or edit a Trap Destination DNS Name, click the **DNS Name** radio button, and then enter the DNS Name in the field.
5. For a non-standard UDP port, enter the UDP Port Number in the field.
6. Select the SNMP trap version to send to the specified address. SNMP versions include SNMP v1 Traps (default), SNMP v2c Traps, and SNMP v2c Inform Requests. SNMP v1 Traps is the default.
7. Enter the community name of the destination device in the **Community Name** field.
8. For **Traps to be received**, select the check boxes of the different types of traps to send to the specified address. Traps to be received include Printer Traps (default), Job Monitoring Traps, Cold Start Traps, and Authentication Traps. At least one trap type must be selected.
9. Click the **Apply** button to save the changes.
10. If prompted, enter your Admin or Key User name and password.

Configuring SNMP v3

When configuring SNMP v3, you can set up:

- Admin and Key User accounts with Privacy and Authentication Keys associated with each account.
- SNMP user read and write access.
- An access control list that limits SNMP printer access to the specific hosts. See Configuring the SNMP Access Control List on page 4-18.

To configure and enable SNMP v3:

1. Launch your web browser.
2. Enter the printer's IP address in the browser's **Address** field (http://xxx.xxx.xxx.xxx).
3. Click **Properties**.
4. Select the **Protocols** folder on the left sidebar.
5. Select **SNMP**.
6. If prompted, enter your Admin or Key User name and password.
7. On the **SNMP Configuration** page, click the **Configure SNMP v3** button.

   The current settings for the SNMP v3 Administrative User, Key User, and Any User/Driver accounts display.

The Administrative User Account section displays the following information:

- **User Name**: Displays the Administrative User account name defined on the **Configure SNMP v3: Administrative User Account** page.
- **Authentication Key**: Displays a row of asterisks (*) if the **Hide Typing** check box is selected on the **Configure SNMP v3: Administrative User Account** page. Displays the Authentication Key if the **Hide Typing** check box is cleared.
- **Privacy Key**: Displays a row of asterisks (*) if the **Hide Typing** check box is selected on the **Configure SNMP v3: Administrative User Account** page. Displays the Privacy Key if the **Hide Typing** check box is cleared.
- **SNMP Read**: Displays a check symbol if SNMP Read access is enabled for the Administrative User Account.
- **SNMP Write**: Displays a check symbol if SNMP Write access is enabled for the Administrative User Account.

The Key User Account section displays the following information:

- **User Name**: Displays the Key User Account name defined on the **Configure SNMP v3: Key User Account** page.
- **Authentication Key**: Displays a row of asterisks (*) if the **Hide Typing** check box is selected on the **Configure SNMP v3: Administrative User Account** page. Displays the Authentication Key if the **Hide Typing** check box is cleared.
- **Privacy Key**: Displays a row of asterisks (*) if the **Hide Typing** check box is selected on the **Configure SNMP v3: Administrative User Account** page. Displays the Privacy Key if the **Hide Typing** check box is cleared.
- **SNMP Read**: Displays a check symbol if SNMP Read access is enabled.
- **SNMP Write**: Displays a check symbol if SNMP Write access is enabled.

Note: SNMP Read and SNMP Write access for the Any User account must be equal to or less than the read and write access privileges set for the Key User account. Once the Key User account is created, if the Any User account is set to have read and/or write access, but the Key User account access is not set, the Key User account is set with the same access privileges as the Any User account by default. Similarly, if the Key User account does not have SNMP Write access, the Any User account cannot be set with write access.

The Any User/Driver Account section displays the following information:

- **User Name**: Displays **anyuser** by default and cannot be changed.
- **SNMP Read**: Displays a check symbol if SNMP Read access is enabled. SNMP Read access can be enabled for the Any User account after the Key User account is created.
- **SNMP Write**: Displays a check symbol if SNMP Write access is enabled. SNMP Write access can be enabled for the Any User account after the Key User account is created.
- **Driver Account Enabled**: Displays a check symbol if the **Driver Account** is enabled (default).

Note: If the **Driver Account** is disabled, it breaks communication between the printer and any applications using SNMP v3, such as Xerox printer drivers and PrintingScout. For a complete list of applications disabled, see Disabling SNMP on page 4-19.

8. Click the **Configure Account(s)** button. A series of pages display that enable you to configure SNMP v3 and the **Administrative User**, **Key User**, and **Any User/Driver** settings. The first page displays Administrative User account information after the account has been created.
9. Do one of the following:
   - To create the Administrative User account and to enable SNMP v3, enter a user name or accept the default name **admin**, and then click the **Create** button.
   - To configure the Key User and other account settings, click the **Next** button.
   - To delete the Administrative User account and disable SNMP v3, click the **Delete** button. This also deletes all other accounts, including the Key User and Any User settings.

Configuring the SNMP Access Control List

To set up a list of hosts that are authorized to access the printer using SNMP:

1. Launch your web browser.
2. Enter your printer's IP address in the browser's **Address** field (http://xxx.xxx.xxx.xxx).
3. Click **Properties**.
4. Select the **Protocol** folder on the left sidebar.
5. Select **SNMP**.
6. If prompted, enter your Admin or Key User name and password.
7. Enter up to ten host IP addresses in the **SNMP Access Control List** field. Separate entries with a blank or a comma, specify ranges with a hypen (-), and use an asterisk (*) to represent a group of numbers (e.g., 13.62.156.*).
8. Click the **Save Changes** button.
9. If prompted, enter your Admin or Key User name and password.

See also:

About Access Control Lists on page 4-4

Disabling SNMP

If you are not using SNMP, disable it to prevent unauthorized access through applications that use these protocols. If you disable SNMP, the following driver features are also disabled:

- PrintingScout alerts
- Walk-Up Printing Installer
- Smart Trays
- PhaserSMART
- Auto supplies ordering
- Consumable levels
- Warning and error status
- Synchronization with installed options, such as hard drive, memory, and extra trays

To disable SNMP:

1. Launch your web browser.
2. Enter your printer's IP address in the browser's **Address** field (http://xxx.xxx.xxx.xxx).
3. Click **Properties**.
4. Select the **Protocols** folder on the left sidebar.
5. Select **SNMP**.
6. If prompted, enter your Admin or Key User name and password.
7. Click the **Disable SNMP Now** button.
8. Click the **Save Changes** button.
9. If prompted, enter your Admin or Key User name and password.

5 Printing Features

This chapter includes:

Secure, Personal, Proof, and Saved Print Jobs

These features are available if your printer has an internal hard drive. These jobs are stored on the hard drive and remain in the printer even when it is turned off.

Select one of the following special job types:

- **Secure Print**: Prints the job only after you enter the four-digit numeric password on the control panel. This is useful for printing confidential documents. It eliminates the risk of confidential documents lying unattended in the printer's output tray, where they are vulnerable to theft and unauthorized viewing.
- **Personal Print**: Prints the job when you select your user name on the printer's control panel or in CentreWare IS. This eliminates the risk of personal documents lying unattended in the printer's output tray, where they are vulnerable to theft and unauthorized viewing.
- **Proof Print**: Prints only one copy of the job so that you can proof the copy. If you want to print the remaining copies, select the job name on the printer's control panel.
- **Saved Print**: Stores the job on the hard drive so you can print it on demand from the control panel. The job is not deleted after printing. This is useful for any document you frequently print, such as tax forms, personnel forms, or requisition forms.

Note: Protected Jobs are another special job type. These are jobs that have been copied or moved from the Public Jobs group in CentreWare IS. For more information, click the **Help** button in CentreWare IS to view the online help.

Specifying Secure, Personal, Proof, and Saved Print Jobs

Use a supported driver to specify a job as a secure print, personal print, proof print, or saved print job:

Operating System	Steps
Windows 98 SE, Windows Me, Windows 2000, Windows XP, Windows Server 2003, Windows NT 4.x PostScript driver	1. Select the **Output Options** tab. 2. Select the job type under **Walk-Up Features**. ■ For a secure print job, enter a four-digit password to assign to this job. ■ For a proof print or saved print job, enter the name you want to give this job.
Mac OS 9 driver	In the **Print** dialog box, select the job type from the **Job Type** drop-down list. ■ For a secure print job, enter a four-digit password to assign to this job. ■ For a proof print or saved print job, enter the name you want to give this job in the **Job Name** field.
Mac OS X (version 10.2 and higher) driver	In the **Print** dialog box, select the job type from the **Job Types** drop-down list. ■ For a secure print job, enter a four digit number, ranging from **0000** through **9999**, in the **Job Password** field. ■ For a proof print or saved print job, enter a document name (up to 20 alpha characters) in the **Document Name** field.

Note: Personal print jobs are not supported in Windows 98 SE and Windows Me.

Printing or Deleting Secure Print Jobs

To print or delete a secure print job, specify the four-digit password on the control panel:

1. Select **Walk-Up Printing**, and then press the **OK** button.
2. Select **Secure Print Jobs**, and then press the **OK** button.
3. Scroll to your User Name, and then press the **OK** button.
4. Scroll to the correct number for the first digit of the numeric password, and then press the **OK** button to accept that digit.
5. Repeat Step 4 for the second, third, and fourth digits.

   Note: If you enter less than four digits in the driver's **Password** field, enter zeros before your password so that there are four digits displayed on the control panel. For example, if you entered **222** in the driver, enter **0222** on the control panel. Use the **Back** button to return to a previous digit.

6. If you submitted more than one secure print job with that password, select the desired job or select **All of Them**, and then press the **OK** button.
7. Select **Print and Delete** or **Delete**, and then press the **OK** button to print or delete the job.

You can also use CentreWare IS to delete secure print jobs:

1. Launch your web browser.
2. Enter your printer's IP address in the browser's **Address** field (http://xxx.xxx.xxx.xxx).
3. Click **Jobs**.
4. Select **Delete Secure Jobs** on the left sidebar.
5. If prompted, enter your Admin or Key User name and password.
6. Do one of the following:
   - To delete all jobs, select **Delete All Secure Jobs**.
   - To delete jobs associated with a specific user name and password, select **Delete Secure Jobs with the Following**, and then enter the **User Name** and **Numeric Password** associated with the jobs.
7. Click the **Delete Job(s)** button.
8. If prompted, enter your Admin or Key User name and password.

Printing or Deleting Personal Print Jobs

To print or delete a personal print job, select your user name on the control panel:

1. Select **Walk-Up Printing**, and then press the **OK** button.
2. Select **Personal Print Jobs**, and then press the **OK** button.
3. Select your User Name, and then press the **OK** button.
4. Select **Print and Delete** or **Delete**, and then press the **OK** button to print or delete all of your personal print jobs.

Printing or Deleting Proof and Saved Print Jobs

To print a saved print job, print the remaining copies of a proof print job, or delete a saved or proof print job, select the job name on the control panel:

1. Select **Walk-Up Printing**, and then press the **OK** button.
2. Select **Proof Print Jobs** or **Saved Print Jobs**, and then press the **OK** button.
3. Select your job name, and then press the **OK** button. (If you use the Windows NT printer driver, select **NT4User** as the job name.)
4. Select **Print and Delete** (for proof prints), **Print and Save** (for saved prints), or **Delete**, and then press the **OK** button.
5. If you are printing, scroll to the desired number of copies, and then press the **OK** button to print the job.

Smart Trays

The Smart Trays feature in the Windows drivers enables you to view the size and type of media in each tray of the printer before sending the job. In Windows environments, when you access the printer properties, the driver queries the printer for the current paper and tray configuration and displays that information on the **Paper/Quality** tab.

Jam Recovery

The jam recovery settings enable you to select how the printer handles jobs that are in the process of printing when a media jam occurs. Jam recovery settings are especially important to consider when printing checks. Normally when a media jam occurs, you can pull out the jammed media and the printer reprints that page and then the rest of the job. While printing checks, someone could cause a media jam as the media is exiting the printer so that a check is reprinted. To prevent the printer from printing two copies of the same check, you can set the printer to begin printing the job from the point where the media jammed, excluding the jammed media, through the end of the job.

To configure the jam recovery setting, use one of the following methods:

- The printer's control panel
- CentreWare IS

Using the Control Panel

To configure the jam recovery setting:

1. On the control panel, select **Paper Tray Setup**, and then press the **OK** button.
2. Select **Paper Handling Setup**, and then press the **OK** button.

   Note: If **Paper Handling Setup** is locked on the control panel, use CentreWare IS to select the jam recovery setting.

3. Select **Reprint Jammed Pages**, and then press the **OK** button.
4. Select **On** or **Off**, and then press the **OK** button.

Using CentreWare IS

To configure the jam recovery setting:

1. Launch your web browser.
2. Enter the printer's IP address in the browser's **Address** field (http://xxx.xxx.xxx.xxx).
3. Click **Properties**.
4. Select the **Security** folder on the left sidebar.
5. Select **Printing Security Settings**.
6. If prompted, enter your Admin or Key User name and password.
7. Under **Jam Recovery Options**, select one of the following options:
   - **Reprint the jammed page and continue printing the rest of the job**: After the jam is cleared, the printer begins printing the job from the point where the media jammed, including the jammed page, through the end of the job.
   - **Do not reprint the jammed page, but do continue printing the rest of the job**: After the jam is cleared, the printer begins printing the job from the point where the media jammed, excluding the jammed page, through the end of the job.
8. Click the **Save Changes** button.
9. If prompted, enter your Admin or Key User name and password.

Paper Tips Page

For information on the supported media types and corresponding trays, print the Paper Tips page:

1. On the control panel, select **Information**, and then press the **OK** button.
2. Select **Information Pages**, and then press the **OK** button.
3. Select **Paper Tips Page**, and then press the **OK** button.

6 Glossary

Terms and Abbreviations

Terms and Abbreviations	Definitions
access control list	A CentreWare IS feature that enables you to limit access to devices, as well as device configuration and management features.
Admin account	A CentreWare IS feature that enables you to limit access to specific printer functions by specifying a name and password. The Admin account has the most permissions. The administrator must know the Admin name and password to access the printer functions in CentreWare IS.
authentication	A CentreWare IS feature that requires users to login with a network user ID and password for security and tracking purposes.
bi-directional	A type of connection in which communications are sent and received simultaneously.
BOOTP	BOOTP (Boot Parameter Protocol) is a protocol that allows a network user to be automatically configured (receive an IP address) and have an operating system boot or initiated without user involvement.
CentreWare Internet Services (IS)	CenterWare IS is a printer administration and support tool. With CenterWare IS software, you can access printer status and manage your printer over a TCP/IP network using a web browser.
CentreWare Web	A web-based, device-management solution for Windows 2000 environments where you use a browser for administration.
certificate	An electronic message containing information about the printer and a digital signature, which is stored in the printer. A certificate is used to validate the identity of the printer to clients and network servers and to allow encrypted communication.
DHCP	DHCP (Dynamic Host Configuration Protocol) is a protocol in which UNIX, Windows, NT, and Window 2000 servers can dynamically allocate TCP/IP addresses.
DNS	DNS (Domain Name System) is used in the Internet for translating names of network nodes into addresses.

Terms and Abbreviations	Definitions
driver	Software that is loaded on the client workstation that prepares data to be sent to the printer.
EtherTalk	A type of network connection (provided by EtherTalk software installed in a Macintosh computer) that enables use of AppleTalk network services on an Ethernet network.
FTP	FTP (File Transfer Protocol) is a basic TCP/IP connectivity utility used to transfer data between computers.
host	A computer or other device on a TCP/IP network.
HTTP	HTTP (Hyper Text Transfer Protocol) is a non-secure protocol used to communicate across the internet between the printer web server and the web browser (clients).
HTTPS	HTTPS (Secure Hyper Text Transfer Protocol) is a secure protocol used to provide authentication and encrypted communication to preserve the confidentiality of your data.
Internet	The global collection of networks that are connected together and share a common range of IP addresses.
IP	The network protocol used for sending network packets over a TCP/IP network.
IP address	A unique 32-bit address for a host on a TCP/IP network or Internet working.
IPP	IPP (Internet Printing Protocol) is an application-level protocol that is used for distributed printing on the Internet and intranets, designed and implemented by Xerox research to validate the IPP specification and as an aid in developing IPP servers.
job accounting	The purpose of job accounting is to collect and report information about all jobs that print. The information collected identifies the submitter of the job and the resources used to print the job.
Key User account	A CentreWare IS feature that enables you to limit access to specific printer functions by specifying a name and password. You can set up a Key User account that is password protected. The Key User has the ability to change some printer settings. CentreWare IS requires the name and password before access to the printer function is allowed.
LPR	LPR (Line Printer Remote) is an application-level printing protocol that uses TCP/IP to establish connections between printers and workstations on a network.
MaiLinX alerts	A feature in CentreWare IS that allows the printer to automatically send email to you and others under certain conditions.
MaiLinX remote printing	A feature in CentreWare IS that enables you to print to Xerox printers over the Internet, directly from Windows applications. The print jobs are sent as email.
mDNS	mDNS (multicast DNS) is a multicast-based discovery protocol that enables you to find your printer on an Apple network or another device that uses multicast-based discovery.

Terms and Abbreviations	Definitions
MIB	MIB (Management Information Base) provides specific information about the state of hardware components and software processes. MIB is used as part of network management tools and functions.
network	A collection of connected devices, such as computers and printers. A network is a tool for communication that allows users to store and retrieve information, share printers, and exchange information.
network address	The network portion of an IP address. For a class A network, the network address is the first byte of the IP address. For a class B network, the network address is the first two bytes of the IP address.
network connection	The software and protocol that connect network devices, such as PCs and printers.
PCL	PCL (Printer Control Language) is the PDL language created by Hewlett-Packard. It became an industry standard and is now available in almost all printer platforms for the office (e.g., PCL 5).
PJL	PJL (Printer Job Language) and PCL commands are used in application programs to control job settings and printer defaults.
PhaserSMART Technical Support	PhaserSMART Technical Support is an automated, internet-based support system that uses the user's default web browser to send diagnostic information from their printer to the Xerox website for analysis.
Port 9100	A printing protocol known as AppSocket, RAW, or Windows TCPmon.
PostScript	A page description language created by Adobe and used in most Xerox Phaser printers.
printer driver	Enables your computer and printer to communicate; provides access to the features of your printer.
printer discovery	Software mechanism for finding printers typically on a network.
Printer Neighborhood	A tool in CentreWare IS that enables you to search for printers on your network, check their status, and manage them remotely.
PrintingScout alerts	PrintingScout is a tool that is installed with the Xerox printer driver. It automatically checks the printer status when a print job is sent. If the printer is unable to print a job, PrintingScout automatically displays an alert on the user's computer screen to let them know that the printer needs attention. The user can click the alert to view instructions explaining how to fix the problem.
printing kiosk	A digital imaging/print platform that is used to connect a laptop computer to a network for printing to a printer, and then paying for the output. A printing kiosk is sometimes located in an airport or library.
protocol	The rules that control the transmitting and receiving of data.
SLP	SLP (Service Location Protocol) is a protocol that provides a flexible and scalable framework for providing hosts with access to information about the existence, location, and configuration of networked services. SLP is useful in enterprise networks.
Smart Trays	A driver feature that displays the current paper type and size available in each printer tray.

Terms and Abbreviations	Definitions
SMTP	SMTP (Simple Mail Transfer Protocol) is a protocol for sending e-mail messages between servers.
SNMP	SNMP (Simple Network Management Protocol) is a protocol used to help manage complex networks. SNMP-compliant devices store data about themselves in MIBs (Management Information Bases) and return this data to the SNMP requestors.
SSL	SSL (Secure Socket Layer) is a protocol that has become the universal standard on the Web for authenticating sites and for encrypting communications between users and Web servers. Because SSL is built into all major browsers and Web servers, simply installing a digital certificate or Server ID enable SSL capabilities.
TCP/IP	TCP/IP (Transmission Control Protocol/Internet Protocol) is a set of communication protocols that is supported by a variety of computer platforms. TCP controls data transfer, and IP controls data routing.
TFTP	TFTP (Trivial File Transfer Protocol) is a version of the TC/IP FTP protocol that uses UDP and has no directory or pass capability.
TLS	TLS (Transport Layer Security) is a protocol for establishing a secure connection between the client and the server. TLS is capable of authenticating both the client and the server and creating an encrypted connection between the two. HTTP uses TLS to establish secure connections.
UDP	UDP (User Datagram Protocol) is a minimal message-oriented transport layer protocol found on domain name servers (DNS).
Walk-Up Printing Driver	The Xerox Walk-Up Printing Driver enables printing from a PC to any Xerox Postscript-enabled printer. For more information, see Walk-Up Printing Driver on page 2-3.
Walk-Up Technology	The Xerox Print Driver Installer (Windows) is a software utility that provides for quick and easy installation of the printer driver. One choice for installation is Walk-Up Technology. For more information, see Walk-Up Installation on page 2-3.
Xerox Usage Analysis Tool	The Xerox Usage Analysis Tool enables you to collect and analyze enterprise-wide Xerox network printer usage data with customizable features.

A Configuration Card Parameters

The printer has a configuration card that stores network parameters and configuration (N, DN, DX, etc.) data. The configuration card is hot swappable, enabling you to share or replace it, providing an alternative to on-site service.

Network settings are saved on the configuration card. If the configuration card is removed from an old printer and inserted into a new printer, the saved settings on the configuration card are copied to the new printer when it is powered on. The new printer assumes the identity of the old printer, eliminating the need to reconfigure network settings.

This appendix includes:

General Information Parameters

- Printer Name
- Startup Page Enabled
- Printer ID
- Sys/Start Job
- Job Timeout
- Load Paper Timeout
- Manual Feed Timeout
- Power Saver Timeout
- Intelligent Ready
- Paper Source
- Tray 1
- Tray 2
- Tray 3
- Tray 4
- Tray 5 (Phaser 6300/6350 only)

Note: The Tray 3, Tray 4, and Tray 5 parameters are only stored on the printer configuration card if the tray is installed in the printer.

- Tray 1 (MPT) Behavior (Phaser 6300/6350 printer only)
- Tray 1 (MPT) Prompt (Phaser 6300/6350 printer only)
- Tray 2 - N Prompt (Phaser 6300/6350 printer only)
- Letter/A4 Substitution
- 2-Sided Printing
- Power Saver
- Metric Defaults
- Metered Toner (Phaser 6300/6350 printer only)

PostScript Parameters

- Printer Quality
- TekColor Correction
- Error Info
- Image Smoothing

PCL Parameters

- Font Number
- Pitch
- Point Size
- Symbol Set
- Orientation
- Form Length
- Line Termination

USB 2.0 Parameters

- Language
- Wait Timeout

Hard Drive Parameters

The hard drive parameters are only stored on the configuration card if the printer has an internal hard drive.

- Overwrite Deleted Files
- Daily Removal
- Age-based Removal

Network Information Parameters

- Wait Timeout
- Sys Admin Contact
- Printer Location

PhaserShare Series B Interface for Ethernet Network Parameters

- Network Speed/Type
- Network Address

EtherTalk Parameters

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

TCP/IP Parameters

- Host Name
- Host Name Requested
- IP Address
- Network Mask
- Router/Gateway
- DHCP/BOOTP
- IP Address Source
- DHCP Server
- DHCP Lease Expiration
- DHCP Lease Renewal
- DDNS
- SMTP Server
- SMTP Reverse Path

DNS Parameters

- Primary Server
- Secondary Server
- Multicast DNS (Bonjour) Enable

SLP Parameters

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

SSDP Parameter

- SSDP TTL

NBNS (WINS) Parameters

- Node Type
- WINS Servers

Access Control Parameter

- Host Access List

LPR Parameters

- Filtering
- Enable Banners

AppSocket (Port 9100) Parameters

- Language
- Filtering

IPP (Internet Printing Protocol) Parameters

- Language
- Filtering
- Network Path

SNMP Parameters

- SNMP v1/v2c
- SNMP v3
- Host Access List
- Admin Account
- Key User Account
- Any User Account
- Drivers Account

HTTP (CentreWare IS) Parameters

- Custom Link
- Refresh Delay
- Administrator Password
- Key User Password
- Use SSL
- Machine Digital Certificate

FTP Parameters

- Language
- Filtering
- Login Password

Status Notification Parameter

- Disabled

MaiLinX Remote Printing Parameters

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

B Printer Commands

Printer Control Language (PCL) and Printer Job Language (PJL) commands can be used to control print job settings and printer defaults. In addition to the standard PCL and PJL commands, the Phaser printers support Xerox-unique PCL and PJL commands. This appendix lists the most commonly used standard and Xerox-unique PCL and PJL commands.

This appendix includes:

See also:

HP PCL 5 Printer Language Reference Manual for standard PCL commands.

Phaser 6300/6350 PCL Commands

This section includes:

Media Size

The following table lists the PCL commands for the media sizes supported by the Phaser 6300/6350 printer. For information on the corresponding trays supported, print the Paper Tips page. See Paper Tips Page on page 5-6.

Note: If you are using custom sizes in PCL commands, you need to load the paper into the tray, set the type and size on the control panel, select the printing options in the printer driver, and then send the job to the printer from the software application's **Print** dialog box.

Media Size	PCL 5 Command*
A4 (210 x 297 mm)	<Esc>&l26A
A5 (148 x 210 mm)	<Esc>&l25A
A6 (105 x 148 mm)	<Esc>&l24A
ISO-B5 (176 x 250 mm)	<Esc>&l65A
B5-JIS (182 x 257 mm)	<Esc>&l45A
Statement (5.5 x 8.5 in.)	<Esc>&l15A
Executive (7.25 x 10.5 in.)	<Esc>&l1A
Letter (8.5 x 11in.)	<Esc>&l2A
US Folio (8.5 x 13 in.)	<Esc>&l10A
Legal (8.5 x 14 in.)	<Esc>&l3A
A7 Envelope (5.25 x 7.25 in.)	<Esc>&l84A
B5 Envelope (175 x 250 mm)	<Esc>&l100A
#10 Commercial Envelope (4.12 x 9.5 in.)	<Esc>&l81A
Monarch Envelope (3.87 x 7.5 in.)	<Esc>&l80A
C5 Envelope (162 x 229 mm)	<Esc>&l91A
C6 Envelope (114 x 162 mm)	<Esc>&l92A
DL Envelope (110 x 220 mm)	<Esc>&l90A
Custom	<Esc>&l101A

* The character that follows the "&" in the command is the lowercase letter "L".

Media Type

The following table lists the PCL commands for the media types supported by the Phaser 6300/6350 printer.

Media Type	PCL 5 Command
Plain Paper	<Esc>&n6WdPaper
Heavy Plain Paper	<Esc>&n11WdHeavyPaper
Transparency	<Esc>&n13WdTransparency
Thin Card Stock	<Esc>&n14WdThinCardStock
Thick Card Stock	<Esc>&n15WdThickCardStock
Envelope	<Esc>&n9WdEnvelope
Labels	<Esc>&n6WdLabel
Letterhead	<Esc>&n11WdLetterhead
Glossy Paper	<Esc>&n12WdCoatedPaper
Colored Paper	<Esc>&n13WdColoredPaper
Preprinted	<Esc>&n11WdPreprinted
Prepunched	<Esc>&n11WdPrepunched
Special	<Esc>&n8WdSpecial

Input Trays

The following table lists the PCL commands for the input trays supported by the Phaser 6300/6350 printer. The table also lists the alternate tray used if the optional input tray is not installed.

Note: When more than one command is listed, you can use either command.

Input Tray	PCL 5 Command*	Alternate Tray
Tray 1 (MPT) in multi-sheet mode	<Esc>&l4H <Esc>&6H	n/a
Tray 1 (MPT) in manual feed mode	<Esc>&l2H <Esc>&l3H	
Tray 2	<Esc>&l1H	n/a
Tray 3	<Esc>&l5H	Tray 2
Tray 4	<Esc>&l8H <Esc>&l20H	Tray 1
Tray 5	<Esc>&l21H	Tray 1
Autoselect	<Esc>&l7H	n/a
Current tray/page eject	<Esc>&l0H	n/a

* The character that follows the “&” in the command is the lowercase letter “L”.

Phaser 8500/8550 PCL Commands

This section includes:

Media Size

The following table lists the PCL commands for the media sizes supported by the Phaser 8500/8550 printer. For information on the corresponding trays supported, print the Paper Tips page. See Paper Tips Page on page 5-6.

Media Size	PCL 5 Command*
A4 (210 x 297 mm)	<Esc>&l26A
A5 (148 x 210 mm)	<Esc>&l25A
A6 (105 x 148 mm)	<Esc>&l24A
B5-ISO (176 x 250 mm)	<Esc>&l65A
B5-JIS (182 x 257 mm)	<Esc>&l45A
Statement (5.5 x 8.5 in.)	<Esc>&l15A
Executive (7.25 x 10.5 in.)	<Esc>&l1A
Letter (8.5 x 11 in.)	<Esc>&l2A
US Folio (8.5 x 13 in.)	<Esc>&l10A
Legal (8.5 x 14 in.)	<Esc>&l3A
A7 Envelope (5.25 x 7.25 in.)	<Esc>&l84A
#10 Commercial Envelope (4.12 x 9.5 in.)	<Esc>&l81A
DL Envelope (110 x 220 mm)	<Esc>&l90A
C5 Envelope (162 x 229 mm)	<Esc>&l91A
#5-1/2 Envelope (4.375 x 5.75 in.)	<Esc>&l208A
#6-3/4 Envelope (3.625 x 6.5 in.)	<Esc>&l83A
Monarch Envelope (3.8 x 7.5 in.)	<Esc>&l80A
Brochure Envelope (6 x 9 in.)	<Esc>&l207A

Media Size	PCL 5 Command*
Choukei 3 Gou (120 x 235 mm)	<Esc>&l87A
Choukei 4 Gou (90 x 205 mm)	<Esc>&l86A
Index Card (3.0 x 5.0 in.)	<Esc>&l78A
Custom	<Esc>&l101A

* The character that follows the “&” in the command is the lowercase letter “L”.

Media Type

The following table lists the PCL commands for the media types supported by the Phaser 8500/8550 printer.

Media Type	PCL 5 Command
Plain Paper	<Esc>&n6WdPaper
Transparency	<Esc>&n13WdTransparency
Card Stock	<Esc>&n10WdCardStock
Envelope	<Esc>&n9WdEnvelope
Labels	<Esc>&n6WdLabel
Letterhead	<Esc>&n11WdLetterhead
Colored Paper	<Esc>&n13WdColoredPaper
Preprinted	<Esc>&n11WdPreprinted
Prepunched	<Esc>&n11WdPrepunched
Special	<Esc>&n8WdSpecial

Input Trays

The following table lists the PCL commands for the input trays supported by the Phaser 8500/8550 printer. The table also lists the alternate tray used if the optional input tray is not installed.

Note: When more than one command is listed, you can use either command.

Input Tray	PCL 5 Command*	Alternate Tray
Tray 1 in multi-sheet mode	<Esc>&l2H <Esc>&l3H <Esc>&l4H <Esc>&l6H	n/a
Tray 2	<Esc>&l1H	n/a
Tray 3	<Esc>&l5H	Tray 2
Tray 4	<Esc>&l8H <Esc>&l20H	Tray 1
Autoselect	<Esc>&l7H	n/a
Current tray/page eject	<Esc>&l0H	

* The character that follows the “&” in the command is the lowercase letter “L”.

Phaser PJL Commands

The following table lists the most commonly used HP PJL and Xerox-unique PJL commands.

See also:

HP Printer Job Language Technical Reference for the standard set of PJL commands.

PJL Command	Values	Description
@PJL FSDELETE NAME="*pathname*"	*	Deletes a file from the internal 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 internal hard drive.
@PJL FSINIT VOLUME=*value*	*	Initializes the internal hard drive.
@PJL FSMKDIR NAME="*pathname*"	*	Creates the specified directory on the internal hard drive.
@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	n/a	Turns off all status responses.
@PJL FSAPPEND	n/a	Appends data to an existing file, or if the file doesn't exist, creates the file and loads it with the given data.
@PJL XCLIENTJOBID=*value*	Exactly 48 bytes (first byte is 8 and the 8 last bytes represent a time in the format *hhmmsshs*.	Sets the client job id used with PrintingScout.
@PJL XJAFILENAME="*filename*"	Roman-8 characters 1-255	Sets the file name for Job Accounting.
@PJL XJAHOSTNAME="*hostname*"	Roman-8 characters 1-255	Sets the host name for Job Accounting.
@PJL XJAJOBNAME="*jobname*"	Roman-8 characters 1-255	Sets the job name for Job Accounting.

PJL Command	Values	Description
@PJL XJAUSERNAME="*username*"	Roman-8 characters 1-255	Sets the user name for Job Accounting.
@PJL XJOBPASSWORD=*value*	4-digit string (1-9)	Assigns the job password used by Secure Print.
@PJL XPERSONALJOB	n/a	Starts a Personal Print job.
@PJL XPROOFJOB	n/a	Starts a Proof Print job.
@PJL XSAVEDJOB	n/a	Starts a Saved Print job.
@PJL XSECUREJOB	n/a	Starts a Secure Print job.
@PJL XIGNOREFF	ON, OFF	Ignores FormFeed commands when printing PCL blank pages.
@PJL XLINETERMINATION=*value*	ON, OFF	Terminates a line.
@PJL XMBFSIZE=*value*	ANY or any supported media size, such as LETTER, STATEMENT, and EXECUTIVE.	Sets the media size for Tray 1.
@PJL XMEDIASOURCE=v*alue*	ANY, TRAY*n*	Sets the media source.
@PJL XMEDIATYPE=*value*	ANY or any supported media type, such as PAPER and LABEL.	Sets the media type.
@PJL XPCLTRAYSWITCH=*value*	ON, OFF	Switches trays when a tray goes empty. If AutoSelect is chosen as the paper source (tray) in PCL, then tray switching is always active, regardless of the value. When the current tray goes empty, the printer attempts to switch to another tray containing 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 goes empty. When this command is OFF, no switching occurs and the user is prompted to load paper.

PJL Command	Values	Description
@PJL XPCLPAPERSRC*x* = *y*	*x* is 0, 1, 2, 3, 4, 5, 6, 7, 8, 20, 21, 22, 23, which is the number in the <Esc>&l#H tray selection commands. *y* is -1 for AutoSelect, 0 for the current tray (eject page), 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.

C Acknowledgements

Original SSLeay License

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscape's SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.

This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- All advertising materials mentioning features or use of this software must display the following acknowledgement:
- "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)."
- The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related.
- If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

  "This product includes software written by Tim Hudson (tjh@cryptsoft.com)."

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed, i.e., this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

Net-SNMP License

Part 1: CMU/UCD copyright notice: (BSD like) -----

Copyright © 1989, 1991, 1992 by Carnegie Mellon University

Derivative Work - 1996, 1998-2000

Copyright © 1996, 1998-2000 The Regents of the University of California. All rights reserved.

Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU and The Regents of the University of California not be used in advertising or publicity pertaining to distribution of the software without specific written permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Part 2: Networks Associates Technology, Inc. copyright notice (BSD) -----

Copyright © 2001-2003, Networks Associates Technology, Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the Networks Associates Technology, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 3: Cambridge Broadband Ltd. copyright notice (BSD) -----

Copyright © 2001-2003, Cambridge Broadband Ltd. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- The name of Cambridge Broadband Ltd. may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER “AS IS”" AND ANYEXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY

THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 4: Sun Microsystems, Inc. copyright notice (BSD) -----

Copyright © 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

Use is subject to license terms below.

This distribution may include materials developed by third parties. Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the Sun Microsystems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 5: Sparta, Inc. copyright notice (BSD) -----

Copyright © 2003-2004, Sparta, Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the Networks Associates Technology, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Other Copyright Notices

Copyright © 2002-2003 Apple Computer, Inc. All rights reserved.

This file contains Original Code and/or Modifications of Original Code as defined in and that are subject to the Apple Public Source License Version 2.0 (the 'License'). You may not use this file except in compliance with the License. Please obtain a copy of the License at http://www.opensource.apple.com/apsl/ and read it before using this file.

The Original Code and all software distributed under the License are distributed on an 'AS IS' basis, WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, AND APPLE HEREBY DISCLAIMS ALL SUCH WARRANTIES, INCLUDING WITHOUT LIMITATION, ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, QUIET ENJOYMENT OR NON-INFRINGEMENT.

Please see the License for the specific language governing rights and limitations under the License.

Copyright © 1983, 1989 Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms are permitted provided that: (1) source distributions retain this entire copyright notice and comment, and (2) distributions including binaries display the following acknowledgement: “This product includes software developed by the University of California, Berkeley and its contributors” in the documentation or other materials provided with the distribution and in all advertising materials mentioning features or use of this software. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Copyright © 2000 Caldera Systems, Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of Caldera Systems nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE CALDERA SYSTEMS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright © 1991, 1999 Free Software Foundation, Inc.

Blowfish is covered by the GNU General Lesser Public License © 1991, 1999 Free Software Foundation, Inc. that can be found at www.gnu.org/copyleft/lesser. The licensed library is available for download at www.schneier.com/code/bfsh-koc.zip or at cost to distribute by request to Xerox Corporation.

JPEG Library

This software is based in part on the work of the Independent JPEG Group.

Index

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

X