

VERSION 3.1
JUNE 2024
702P09256

Xerox® B225/B230/
B235/B305/B310/
B315/B410/C230/
C235/C310/C315/
C410/C320/C325
Series Printers and
Multifunction Printers

Embedded Web Server

Administrator Guide

© 2024 Xerox Corporation. All rights reserved. Xerox® is trademark of Xerox Corporation in the United States and other countries.

Adobe and PostScript are either registered trademarks or trademarks of Adobe in the United States and/or other countries.

Apple and App Store are trademarks of Apple, Inc., registered in the U.S. and other countries and regions.

Microsoft and Windows are trademarks of the Microsoft group of companies.

Kerberos is a trademark of the Massachusetts Institute of Technology (MIT).

Wi-Fi CERTIFIED Wi-Fi Direct™ is a trademark of the Wi-Fi Alliance®.

PCL® is a registered trademark of the Hewlett-Packard Company.

All other trademarks are the property of their respective owners.

Contents

Overview	7
Supported Printer Models.....	8
Supported Web Browsers	9
Accessing the Embedded Web Server.....	10
Parts of the Embedded Web Server.....	11
Understanding Helper Text.....	12
Managing Printers.....	13
Checking the Status of Parts and Supplies from the Embedded Web Server.....	14
Generating Reports and Logs.....	15
Configuring Remote Operator Panel Settings.....	16
Configuring Supply Notifications	17
Xerox® Easy Assist App	18
Customizing the Home Screen	19
Editing the Home Screen.....	19
Adding an Application to the Home Screen	19
Arranging the Application on the Home Screen	19
Restoring the Home Screen	20
Importing and Exporting Home Screen Settings	20
Managing Contacts	21
Adding Contacts.....	21
Adding Groups	21
Editing Contacts or Groups.....	21
Deleting Contacts or Groups.....	22
Activating a Supplies Plan	23
Activating a PagePack® or Metered Supplies Plan	23
Activating a Subscription Service Plan.....	23
Printing	25
Configuring the Print Settings.....	26
Configuring the Layout Settings	26
Configuring the Setup Settings.....	26
Configuring the Quality Settings.....	27
Configuring the Job Accounting Settings.....	28
Configuring the XPS Settings	28
Configuring the PDF Settings.....	29
Configuring the PostScript Settings	29
Configuring the PCL Settings	29
Configuring the Image Settings	30
Scanning.....	31
Configuring the Scan Settings.....	32
Configuring the Copy Settings.....	32

Configuring the Email Settings	34
Configuring the FTP Settings	38
Configuring the Flash Drive Settings.....	40
Creating a Shortcut	44
Managing Scan Center Destinations	45
Configuring a Network Destination	45
Configuring an Email Destination	45
Configuring a Fax Destination.....	46
Configuring a Remote Printer Destination	46
Faxing.....	47
Configuring the Fax Settings.....	48
Setting the Fax Mode	48
Configuring Analog Fax Settings	49
General Fax Settings.....	49
Fax Send Settings	49
Fax Receive Settings.....	51
Fax Cover Page.....	52
Fax Log Settings	53
Speaker Settings.....	53
Configuring the Fax Server	54
General Fax Settings.....	54
Fax Server Email Settings	54
Fax Server Scan Settings	55
Networking.....	57
Configuring the HTTP/FTP Settings.....	58
Selecting the Active Network Adapter	59
Connecting to a Wireless Network	60
Securing Printers.....	61
Securing Network Connections.....	62
Configuring the TLS Settings.....	62
Configuring TCP/IP Port Access Settings.....	62
Configuring IP Security Settings	62
Configuring 802.1x Authentication	63
Setting the Restricted Server List.....	64
Managing Devices Remotely	65
Using HTTPS for Printer Management	65
Setting Up SNMP.....	65
Configuring Security Audit Log Settings	66
Managing Security Audit Logs.....	67
Updating Software	67
Managing Login Methods.....	69
Restricting Public Access on the Guest Account	69

Using Local Accounts	69
Using LDAP or LDAP+GSSAPI	71
Using Kerberos.....	73
Using Active Directory	75
Creating LDAP, LDAP+GSSAPI, Kerberos, or Active Directory Groups	77
Editing or Deleting LDAP, LDAP+GSSAPI, or Active Directory Groups.....	78
Understanding Access Controls	78
Managing Certificates.....	81
Configuring Printer Certificate Defaults	81
Creating a Printer Certificate.....	81
Installing Certificates Manually	82
Installing Certificates Automatically	82
Viewing, Downloading, and Deleting Certificates.....	82
Managing Other Access Functions.....	83
Universal Print.....	83
Scheduling Access to USB Devices	85
Setting Login Restrictions	85
Configuring Confidential Printing.....	86
Enabling Solutions LDAP Settings.....	86
Showing Secured Applications or Functions on the Home Screen.....	87
Enabling Print Permission	87
Enabling the Security Reset Jumper.....	88
Securing Data.....	89
Configuring Printer Settings.....	89
Erasing Printer Memory.....	91
Erasing Printer Hard Disk Memory.....	91
Configuring Printer Hard Disk Encryption.....	92
Restoring Factory Default Settings	92
Statement of Volatility	92
Troubleshooting.....	95
Application Error	96
Login Troubleshooting.....	97
Cannot Detect the Card Reader or the Smart Card.....	97
User Is Locked Out.....	97
User Is Logged Out Automatically	97
User Cannot Access Applications or Functions.....	97
KDC and MFP Clocks Are Out of Sync	98
Domain Controller Certificate Is Not Installed.....	98
KDC Is Not Responding Within the Required Time	98
Authentication Issues.....	99
Kerberos Authentication Failed.....	99
Cannot Generate or Read Certificate Information From the Smart Card.....	100
Cannot Validate the Domain Controller	100
Cannot Validate the Domain Controller Certificate.....	101
Cannot Find Realm in the Kerberos Configuration File	101
Domain Controller and Device Clocks are out of Sync.....	102
Cannot Validate the Domain Controller Certificate Chain.....	102

Contents

Cannot Connect to the OCSP Responder	102
Cannot Validate the Domain Controller Certificate Against the OCSP Responder	102
Cannot Access Individual Applications and Functions on the Printer	103
LDAP Troubleshooting	104
LDAP Lookups Fail	104
Scanning Problems	105
Cannot Scan to the Selected Destination	105
License Error	105
An Error Occurs When Opening a Secure PDF File	105
Faxing Problems	107
Cannot Receive Faxes from One Sender	107
Cannot Receive Faxes from All Senders	107
Cannot Send Faxes to One Destination	108
Cannot Send to All Fax Destinations	108
Networking Problems	110
Printer Is Not Communicating on the Network	110
Configuring Smart Card Authentication	111
Configuring the Login Screen Settings	112
Configuring the Manual Login Settings	113
Configuring the Smart Card Settings	114
Configuring Advanced Settings	116

Overview

This chapter contains:

Supported Printer Models	8
Supported Web Browsers.....	9
Accessing the Embedded Web Server.....	10
Parts of the Embedded Web Server	11
Understanding Helper Text	12



Note: Some settings are available only in some printer models.

Use this document to manage and configure printer, scan, fax, network, and security settings using the Embedded Web Server. To secure the printer, combine login methods and access controls to define users who are allowed to use the printer and the functions that they can use.

Before you begin, ensure that the printer settings are configured for email. For details, refer to the *User Guide* for your printer model.

Also, identify the following conditions:

- The login method to use:
 - **Local Accounts:** Use the authentication methods available on the printer. User credentials are stored in the printer memory.
 - **Lightweight Directory Access Protocol (LDAP)**
 - **Generic Security Services Application Program Interface (LDAP+GSSAPI)**
 - **Kerberos**
 - **Active Directory**
- Other solutions that you want to include:
 - **Smart Card Authentication:** A collection of applications used to secure access to printers and their functions. The applications allow you to log in to a printer manually or with a smart card, then send emails and release print jobs securely. In an application, you can configure more security settings, such as email signing and encryption. For more information, refer to [Configuring Smart Card Authentication](#).
 - **Card Authentication:** Secure access to a printer using a card reader. When users badge in, their credentials are authenticated by a master printer, LDAP, or identity service provider (ISP).
- The group to which the users belong. You can create groups after creating the login methods.
- The applications, functions, and printer management settings that users can access.



Note: Administrator rights are required to configure or troubleshoot the security settings.

Supported Printer Models

The supported printer models are:

- Xerox® B225/B235 Multifunction Printer
- Xerox® B230 Printer
- Xerox® B305/B315 Multifunction Printer
- Xerox® B310 Printer
- Xerox® B410 Printer
- Xerox® C230 Color Printer
- Xerox® C235 Color Multifunction Printer
- Xerox® C310 Color Printer
- Xerox® C315 Color Multifunction Printer
- Xerox® C410 Color Printer
- Xerox® C320 Color Printer
- Xerox® C325 Color Multifunction Printer

Supported Web Browsers


- Google Chrome™ version 32 or later
- Microsoft Edge
- Mozilla Firefox version 24 or later
- Apple Safari version 6 or later

Accessing the Embedded Web Server

1. Obtain the printer IP address. Do one of the following:
 - Locate the IP address on the printer home screen.
 - View the IP address in the Network Overview section or in the Ethernet or Wireless section of the Network/Ports menu.
2. Open a web browser, then type the printer IP address.

Parts of the Embedded Web Server



	SECTION	DESCRIPTION
1	Top	<ul style="list-style-type: none"> Shows the printer information and current status. Allows the user to change the language of the web page. <p> Note: Changing the language of the web page does not affect the language on the printer display.</p>
2	Left	<ul style="list-style-type: none"> Allows the user to search for items in the Embedded Web Server. Contains links to the printer settings and other major sections of the Embedded Web Server.
3	Center	<ul style="list-style-type: none"> Shows specific information on the selected section of the web page. Allows the user to change configurations and settings. Generates reports and logs. For more information, refer to Generating Reports and Logs.

Understanding Helper Text

Helper text is a short and concise description of a setting or page that indicates its usage or provides details on printer behavior when you apply a change. Helper text appears to the right of the setting field, below page or section headers, or at the bottom of the web page. Helper text also provides the user with a range of acceptable data entries.

Managing Printers

This chapter contains:

Checking the Status of Parts and Supplies from the Embedded Web Server	14
Generating Reports and Logs	15
Configuring Remote Operator Panel Settings.....	16
Configuring Supply Notifications.....	17
Xerox® Easy Assist App.....	18
Customizing the Home Screen.....	19
Managing Contacts.....	21
Activating a Supplies Plan.....	23

Checking the Status of Parts and Supplies from the Embedded Web Server



Note: Ensure that the computer and printer are connected to the same network.

1. To obtain the printer IP address, do one of the following:
 - Locate the IP address on the printer home screen.
 - View the IP address in the Network Overview section or in the Ethernet or Wireless section of the Network/Ports menu.
2. Open a web browser, then type the printer IP address.
3. You can view the status of the parts and supplies, click **Status > Supplies**.

Generating Reports and Logs

1. From the Embedded Web Server, click **Reports**.
2. Select a report or log.
 - **Menu Settings Page:** Shows the current printer preferences, settings, and configurations
 - **Device:**
 - **Device Information:** Shows information about the printer
 - **Device Statistics:** Shows printer usage and supply status
 - **Profiles List:** Shows a list of profiles that are stored on the printer
 - **Print:**
 - **Print Directory:** Shows the resources that are stored on the flash drive or printer hard disk.



Note: This report appears only when a flash drive or printer hard disk is installed.

- **Shortcuts:**
 - **All Shortcuts:** Shows a list of all the shortcuts that are stored on the printer
 - **Fax Shortcuts:** Shows a list of all fax shortcuts that are stored on the printer
 - **Copy Shortcuts:** Shows a list of all copy shortcuts that are stored on the printer
 - **Email Shortcuts:** Shows a list of all email shortcuts that are stored on the printer
 - **FTP Shortcuts:** Shows a list of all FTP shortcuts that are stored on the printer
 - **Network Folder Shortcuts:** Shows a list of all network folder shortcuts that are stored on the printer
- **Fax:**



Note: This setting is available only in some printer models.

- **Fax Job Log:** Lists the last 200 completed fax jobs.



Note: This report is available only when Enable Job Log is enabled.

- **Fax Call Log:** Lists the last 100 attempted, received, and blocked calls



Note: This report is available only when a flash drive or printer hard disk is installed.

- **Network:**
 - **Network Setup Page:** Shows the configured network and wireless settings on the printer



Note: This report is available only in network printers and printers connected to print servers.

- **Wi-Fi Direct Connected Clients:** Shows the list of devices that are connected to the printer using Wi-Fi Direct



Note: This report appears only when Enable Wi-Fi Direct is set to **On**.

Configuring Remote Operator Panel Settings

1. From the Embedded Web Server, click **Settings > Device > Remote Operator Panel**.
2. Configure the settings:
 - **External VNC Connection:** Connect an external Virtual Network Computing (VNC) client to the remote control panel.
 - **Authentication Type:** Set the authentication type when accessing the VNC client server.
 - **VNC Password:** Specify the password to connect to the VNC client server.



Note: This menu item appears only if Authentication Type is set to Standard Authentication.

3. To launch the remote operator panel, click **Launch**.
4. Click **Save**.

Configuring Supply Notifications

1. Open a web browser, then in the address field, type the printer IP address.

2. View the printer IP address on the printer home screen.

The IP address appears as four sets of numbers separated by periods, such as 123 . 123 . 123 . 123.

If you are using a proxy server, to load the web page correctly, disable the proxy server temporarily.

3. Click **Settings > Device > Notifications**.
4. From the Supplies menu, click **Custom Supply Notifications**.
5. For each supply item, select a notification.
6. Apply the changes.

Xerox® Easy Assist App

To access the printer from your smartphone, download and install the Xerox® Easy Assist (XEA) app to your mobile device. XEA app is available in the Apple App Store or Google Play Store.

By installing the Xerox Easy Assist app on your smartphone, you can:

- Setup your new printer easily for you and your team
- Manage its configuration
- View alerts indicating supply requirements and order them
- Get live troubleshooting support for your printer.

The Xerox Easy Assist app guides you through the simple process to connect to your printer using the IP address or a QR Code on the printer.

For more information about the Xerox Easy Assist app and its features, refer to the *User Guide* of your printer.




Note: Not all printer models support the Xerox Easy Assist app and its features.

Customizing the Home Screen

 Note: This setting is available only in some printer models.

This feature allows users to customize the applications in the printer display. Users can add, remove, or rearrange the applications from the home screen and other pages. Users can also customize the application labels.

 Note: For printers with a 4.3-inch screen, the home screen can accommodate eight applications. For printers with a 7-inch screen, the home screen can accommodate 15 applications.

EDITING THE HOME SCREEN

1. From the Embedded Web Server, click **Settings > Device > Home Screen Customizations**.
2. Select an application from the list, then perform the following:
 - a. Click **Edit**.
 - b. In the App Label field, type the name of the application.

 Note:

- The application label can have a maximum of 20 characters.
- Click **Restore** app to restore the application label.

3. Click **Save**.

 Note:

- Click **Remove** to remove the application from the list.
- The **Edit** option is disabled for BLANK SPACE and eSF applications.

ADDING AN APPLICATION TO THE HOME SCREEN

To add an application to the home screen, perform the following procedure:

1. Click **+** to add an application.
2. Select the applications that you want to add.
3. Click **Add**.

 Note:

- You can limit the applications to show on a particular page.
- If the number of applications on a particular page reaches the limit, the add icon for that page is disabled.

ARRANGING THE APPLICATION ON THE HOME SCREEN

To arrange an application on the home screen, perform the following procedure:

1. Select an application.

2. Drag and drop the application on the page where you want it to appear.
3. Click **Save**.



Note:

- Page 1 represents the first page of the home screen, while Other Pages represents the subsequent pages of the home screen. You can drag and drop applications to and from Page 1 to Other Pages.
- You can rearrange the order of applications for Page 1, but not for Other Pages.
- You cannot drag and drop any applications on a page which has reached the limit for the number of applications.
- If only one application remains, then you cannot drag an application out of that page.

RESTORING THE HOME SCREEN

To restore the home screen, perform the following procedure:

1. To restore the applications to their default label and location, click **Restore home screen**.
2. Click **Restore**.

IMPORTING AND EXPORTING HOME SCREEN SETTINGS

You can import or export home screen settings from one printer to another. If a native or eSF application is not supported, then it appears as a BLANK SPACE application in the home screen of that printer.

Exporting Home Screen Settings

To export the home screen settings, perform the following:

1. From the Embedded Web Server, click **Export Configuration > Custom**.
2. Select **Home Screen Icons**.
3. Click **Export**.



Note: The files are exported in .zip format.

Importing Home Screen Settings

To import the home screen settings, perform the following:

1. From the Embedded Web Server, click **Import Configuration**.
2. Select the folder, then click **Import**.
3. Click **OK**.



Note: If the files are not imported properly, then a warning message appears.

Managing Contacts

ADDING CONTACTS


 Note: This setting is available only in some printer models.

1. Open a web browser, then in the address field, type the printer IP address.
2. View the printer IP address on the printer home screen.

The IP address appears as four sets of numbers separated by periods, such as 123 . 123 . 123 . 123.

If you are using a proxy server, to load the web page correctly, disable the proxy server temporarily.

3. Click **Address Book**.
4. In the Contacts section, add a contact.

 Note: You can assign the contact to one or more groups.

5. If necessary, specify a login method to allow application access.
6. To apply the changes, click **Save**.

ADDING GROUPS


 Note: This setting is available only in some printer models.

1. Open a web browser, then in the address field, type the printer IP address.
2. View the printer IP address on the printer home screen.

The IP address appears as four sets of numbers separated by periods, such as 123 . 123 . 123 . 123.

If you are using a proxy server, to load the web page correctly, disable the proxy server temporarily.

3. Click **Address Book**.
4. In the Contact Groups section, type a group name.

 Note: You can assign one or more contacts to the group.

5. To apply the changes, click **Save**.

EDITING CONTACTS OR GROUPS

 Note: This setting is available only in some printer models.

1. Open a web browser, then in the address field, type the printer IP address.
2. View the printer IP address on the printer home screen.

The IP address appears as four sets of numbers separated by periods, such as 123 . 123 . 123 . 123.

If you are using a proxy server, to load the web page correctly, disable the proxy server temporarily.

3. Click **Address Book**.

4. Do one of the following:
 - In the Contacts section, click a contact name, then edit the information.
 - In the Contact Groups section, click a group name, then edit the information.
5. To apply the changes, click **Save**.

DELETING CONTACTS OR GROUPS



Note: This setting is available only in some printer models.

1. Open a web browser, then in the address field, type the printer IP address.
2. View the printer IP address on the printer home screen.

The IP address appears as four sets of numbers separated by periods, such as 123 . 123 . 123 . 123.

If you are using a proxy server, to load the web page correctly, disable the proxy server temporarily.

3. Click **Address Book**.
4. Do one of the following:
 - In the Contacts section, select a contact that you want to delete.
 - In the Contact Groups section, select a group name that you want to delete.

Activating a Supplies Plan

Your Xerox representative offers supplies and service plans.

- PagePack™ and Metered plans are based on a cost per page and include all service and supplies for your printer in one contract. When a starter cartridge is replaced with a PagePack® or Metered cartridge, the printer sets the plan automatically.
- A Subscription Service plan enables the printer to monitor supplies and when low, replacement supplies are ordered automatically.



Note: Subscription Service plans are not offered in all geographic locations.

For more information about Xerox® supplies and service plans, contact your Xerox representative.

ACTIVATING A PAGEPACK® OR METERED SUPPLIES PLAN

When you are enrolled in a supplies program, you need to activate the supplies plan at regular intervals. To enable your printer for your purchased plan, contact your Xerox representative to get a Supplies Activation Code.

To enter your Supplies Activation Code, do the following:

1. In the Embedded Web Server, log in as the administrator.
2. For Settings, click **Supplies Plan**.
3. For Supplies Plan, click **Plan Activation**.
4. In the Activation Code field, type the Supplies Activation Code.
5. Click **Activate Plan**.

ACTIVATING A SUBSCRIPTION SERVICE PLAN

For a Subscription Service plan, do the following:

1. In the Embedded Web Server, log in as the administrator.
2. For Settings, click **Supplies Plan**.
3. For Supplies Plan, click **Subscription Service**.
4. For the Subscription Service, click **Check Subscription**, then follow the directions provided by your Xerox representative.

Printing

This chapter contains:

Configuring the Print Settings.....	26
-------------------------------------	----

Configuring the Print Settings

CONFIGURING THE LAYOUT SETTINGS



Note: Some settings are available only in some printer models.

1. From the Embedded Web Server, click **Settings > Print > Layout**.
2. Configure the settings:
 - **Sides:** Specify whether to print on one side or two sides of the paper.
 - **Flip Style:** Determine which side of the paper (long edge or short edge) is bound when performing 2-sided printing.
 - **Blank Pages:** Print blank pages that are included in a print job.
 - **Collate:** Keep the pages of a print job stacked in sequence, particularly when printing multiple copies of the job.
 - **Separator Sheets:** Insert blank separator sheets when printing.
 - **Separator Sheet Source:** Specify the paper source for the separator sheet.
 - **Pages per Side:** Print multiple page images on one side of a sheet of paper.
 - **Pages per Side Ordering:** Specify the positioning of multiple page images when using Pages per Side.
 - **Pages per Side Orientation:** Specify the orientation of a multiple-page document when using Pages per Side.
 - **Pages per Side Border:** Print a border around each page image when using Pages per Side.
 - **Copies:** Specify the number of copies for each print job.
3. Click **Save**.



Note: The range of number of copies is from 1 to 9999.

- **Print Area:** Set the printable area on a sheet of paper.

CONFIGURING THE SETUP SETTINGS



Note: Some settings are available only in some printer models.

1. From the Embedded Web Server, click **Settings > Print > Setup**.

2. Configure the settings:

- **Printer Language:** Set the printer language.
- **Job Waiting:** Preserve print jobs requiring supplies so that jobs not requiring the missing supplies can print.



Note: This menu item appears only when a printer hard disk is installed.

- **Job Hold Timeout:** Set the time in seconds that the printer waits for user intervention before it holds jobs that require unavailable resources and continues to print other jobs in the print queue. The range is 0–255.



Note: This menu item appears only when a printer hard disk is installed.

- **Printer Usage:** Determine how the color print cartridges operate during printing.
- **Resource Save:** Determine what the printer does with downloaded resources, such as fonts and macros, when it receives a job that requires more than the available memory.
- **Print All Order:** Specify the order in which held and confidential jobs are printed when Print All is selected.
- **PJL File Access Control:** Allow the users to set the printer job language file access control.
- **Automatic Deletion of Suspended Print Jobs:** Automatically cancels or deletes the queued print jobs that are interrupted by errors, such as paper jams and missing supplies.
- **Time until Suspended Print Jobs are Automatically Deleted:** Specify the wait time for the printer to cancel queued print jobs that are interrupted by errors. The range is 1–60 minutes.



Note: This setting appears only when Automatic Deletion of Suspended Print Jobs is enabled.

3. Click **Save**.**CONFIGURING THE QUALITY SETTINGS**

Note: Some settings are available only in some printer models.

1. From the Embedded Web Server, click **Settings > Print > Quality**.

2. Configure the settings:

- **Print Mode:** Set how the printer generates color content.
- **Print Resolution:** Set the resolution for the printed output.



Note: 4800 CQ provides high-quality output at maximum speed.

- **Toner Darkness:** Determine the lightness or darkness of text images.
- **Halftone:** Enhance the printed output to have smoother lines with sharper edges.
- **Color Saver:** Reduce the amount of toner used to print graphics and images.
- **RGB Brightness:** Adjust the brightness for color output. The range is -6 to 6 (including 0).
- **RGB Contrast:** Adjust the contrast for color output. The range is 0–5.
- **RGB Saturation:** Adjust the saturation for color output.

3. Configure Advanced Imaging:
 - **Color Table:** Identifies the color tables currently in use on the device. This can be changed by installing a color table bundle.
 - **Color Balance:** Adjust the amount of toner that is used for each color.
 - **Reset Defaults:** Reset all color settings to their default values.
 - **Color Correction:** Modify the color settings used to print documents.
 - **Color Samples:** Print sample pages for each of the RGB and CMYK color conversion tables used in the printer.
 - **Color Adjust:** Calibrate the printer to adjust color variations in the printed output.
 - **Spot Color Replacement:** Assign specific CMYK values to 20 named spot colors.
 - **RGB Replacement:** Match the colors of the output with that of the original document.
4. Click **Save**.

CONFIGURING THE JOB ACCOUNTING SETTINGS



Note: Some settings are available only in some printer models.

1. From the Embedded Web Server, click **Settings > Print > Job Accounting**.
2. Configure the settings:
 - **Job Accounting:** Set the printer to create a log of the print jobs that it receives.
 - **Accounting Log Frequency:** Specify how often the printer creates a log file.
 - **Log Action at End of Frequency:** Specify how the printer responds when the frequency threshold expires.
 - **Log Action at Near Full:** The value defined in Log Near Full Level determines when this action is triggered.
 - **Log Action at Full:** Specify how the printer responds when disk usage reaches the maximum limit (100 MB).
 - **URL to Post Log:** Specify where the printer posts job accounting logs.
 - **Email Address to Send Logs:** Specify the email address to which the printer sends job accounting logs.



Note: Addresses are comma-delimited and up to 256 characters.

- **Log File Prefix:** Specify the prefix for the log file name.
3. Click **Save**.

CONFIGURING THE XPS SETTINGS



Note: Some settings are available only in some printer models.

1. From the Embedded Web Server, click **Settings > Print > XPS**.

2. Configure the settings:
 - **Print Error Pages:** Set the printer to print the error pages.
 - **Minimum Line Width:** Set the initial minimum stroke width.
3. Click **Save**.

CONFIGURING THE PDF SETTINGS



Note: Some settings are available only in some printer models.

1. From the Embedded Web Server, click **Settings > Print > PDF**.
2. Configure the settings:
 - **Scale To Fit:** Scale the page content to fit the selected paper size.
 - **Annotations:** Specify whether to print annotations in the PDF.
 - **Print PDF Error:** Enable the printing of PDF error.
3. Click **Save**.

CONFIGURING THE POSTSCRIPT SETTINGS



Note: Some settings are available only in some printer models.

1. From the Embedded Web Server, click **Settings > Print > PostScript**.
2. Configure the settings:
 - **Print PS Error:** Print a page that describes the PostScript error.
 - **Minimum Line Width:** Set the minimum stroke width.
 - **Lock PS Startup Mode:** Disable the SysStart file.
 - **Image Smoothing:** Enhance the contrast and sharpness of low-resolution images.
 - **Wait Timeout:** Enable the printer to wait for more data before canceling a print job. The range is 15–65,535.
3. Click **Save**.

CONFIGURING THE PCL SETTINGS



Note: Some settings are available only in some printer models.

1. From the Embedded Web Server, click **Settings > Print > PCL**.

2. Configure the settings:
 - **Font Source:** Select the source that contains the default font selection.
 - **Font Name:** Select a font from the specified font source.
 - **Symbol Set:** Specify the symbol set for each font name.
 - **Pitch:** Specify the pitch for fixed or monospaced fonts.
 - **Orientation:** Specify the orientation of text and graphics on the page.
 - **Lines per Page:** Specify the number of lines of text for each page printed through the PCL datastream. The range is 1–255.
 - **PCL5 Minimum Line Width:** Set the initial minimum stroke width.
 - **PCLXL Minimum Line Width:** Set the initial minimum stroke width.
 - **A4 Width:** Set the width of the logical page on A4-size paper.
 - **Auto CR after LF:** Set the printer to perform a carriage return after a line feed control command.
 - **Auto LF after CR:** Set the printer to perform a line feed after a carriage return control command.
 - **Tray Renumber:** Configure the printer to work with a different print driver or custom application that uses a different set of source assignments to request a given paper source.
 - **View Factory Defaults:** Show the factory default value assigned for each paper source.
 - **Restore Defaults:** Restore the tray renumber values to their factory defaults.
 - **Print Timeout:** Set the printer to end a print job after it has been idle for the specified amount of time in seconds. The range is 1–255.
3. Click **Save**.

CONFIGURING THE IMAGE SETTINGS



Note: Some settings are available only in some printer models.

1. From the Embedded Web Server, click **Settings > Print > Image**.
2. Configure the settings:
 - **Auto Fit:** Select the best available paper size and orientation setting for an image.
 - **Invert:** Invert bitonal monochrome images.
 - **Scaling:** Adjust the image to fit the printable area.
 - **Orientation:** Specify the orientation of text and graphics on the page.
3. Click **Save**.

Scanning

This chapter contains:

Configuring the Scan Settings	32
Creating a Shortcut	44
Managing Scan Center Destinations.....	45

Configuring the Scan Settings


CONFIGURING THE COPY SETTINGS



Note: Some settings are available only in some printer models.

1. From the Embedded Web Server, click **Settings > Copy**.
2. Configure the Copy Defaults.
 - **Content Type:** Improve the output result based on the content of the original document.
 - **Content Source:** Improve the output result based on the source of the original document.
 - **Sides:** Specify the scanning behavior based on the original document.
 - **Separator Sheets:** Specify whether to insert blank separator sheets when printing.
 - **Separator Sheet Source:** Specify the paper source for the separator sheet.
 - **Color:** Specify whether to print copies in color.
 - **Pages per Side:** Specify the number of page images to print on one side of a sheet of paper.
 - **Print Page Borders:** Specify whether to print a border around each image when printing multiple pages on a single page.
 - **Collate:** Specify whether to print multiple copies in sequence.
 - **"Copy from" Size:** Set the paper size of the original document.
 - **"Copy to" Source:** Specify the paper source for the copy job.
 - **Temperature:** Specify whether to generate a cooler or warmer output.
 - **Darkness:** Adjust the darkness of the scanned image.
 - **Number of Copies:** Specify the number of copies to print by default.
 - **Header/Footer:** Specify the header and footer of the document.
 - **Left Header:** Specify whether to insert text on the left header of the document.
 - **Middle Header:** Specify whether to insert text on the middle header of the document.
 - **Right Header:** Specify whether to insert text on the right header of the document.
 - **Left Footer:** Specify whether to insert text on the left footer of the document.
 - **Middle Footer:** Specify whether to insert text on the middle footer of the document.
 - **Right Footer:** Specify whether to insert text on the right footer of the document.
 - **Overlay:** Specify the overlay text printed on each page of the copy job.
 - **Custom Overlay:** Type a custom overlay text.


3. Configure the Advanced Imaging settings.
 - **Color Balance:** Adjust the amount of toner being used in each color.
 - **Color Dropout:** Specify which color to drop during scanning, and adjusts the dropout setting for that color.
 - **Auto Color Detect:** Set the amount of color that the printer detects from the original document.
 - **Contrast:** Specify the contrast of the output.
 - **Background Removal:** Adjust the amount of background visible on a scanned image.
 - **Background Detection:** Specify the background detection parameters:
 - To remove the background color from the original document, set Background Detection to **Content-based**.
 - To remove the image noise, set **Background Detection** to **Fixed**.
 - **Level:** Specify the background removal level.
 - **Auto Center:** Align the content at the center of the page.
 - **Mirror Image:** Create a mirror image of the original document.
 - **Negative Image:** Create a negative image of the original document.
 - **Shadow Detail:** Adjust the amount of shadow detail visible on a scanned image.
 - **Scan Edge to Edge:** Allow edge-to-edge scanning of the original document.
 - **Sharpness:** Adjust the sharpness of a scanned image.
4. Configure the Admin Controls settings.
 - **Allow Color Copies:** Specify whether to allow printing of copies in color.
 - **Allow Priority Copies:** Specify whether to allow interruption of a print job to copy a page or document.
 - **Allow Save as Shortcut:** Specify whether to allow custom copy settings to be saved as shortcuts.
 - **Adjust ADF Skew:** Specify the front-side and back-side skew angles.

 Note: Adjust ADF Skew is disabled if Express Mode is On and if electronic deskew is not supported on the device. Examples of Express Mode are Express Scanning and Express Printing.
5. Click **Save**.


Customize Settings List

This feature allows you to customize the settings on the screen.


1. Do one of the following:
 - To hide settings from the screen, drag and drop the settings from Settings List to More Settings List.
 - To show settings on the screen, drag and drop the settings from More Settings List section to Settings List.
2. Click **Save**.

 Note: To undo the changes, click **Reset**.

CONFIGURING THE EMAIL SETTINGS

 Note: Some settings are available only in some models.


1. From the Embedded Web Server, click **Settings > Email**.
2. Configure Email Setup:
 - **Primary SMTP Gateway:** Type the IP address or host name of the primary SMTP server for sending email.
 - **Primary SMTP Gateway Port:** Type the port number of the primary SMTP server.
 - **Secondary SMTP Gateway:** Type the server IP address or host name of your secondary or backup SMTP server.
 - **Secondary SMTP Gateway Port:** Type the server port number of your secondary or backup SMTP server.
 - **SMTP Timeout:** Set the time before the printer times out when the SMTP server does not respond.
 - **Reply Address:** Specify the reply address to appear in the email.
 - **Always Use SMTP Default Reply Address:** Always use the default reply address in the SMTP server.
 - **Use SSL/TLS:** Specify whether to send email using an encrypted link.
 - **Require Trusted Certificate:** Require a trusted certificate when accessing the SMTP server.
 - **SMTP Server Authentication:** Set the authentication type for the SMTP server.
 - **Device-Initiated Email:** Specify whether credentials are required for device-initiated email.
 - **User-Initiated Email:** Specify whether credentials are required for user-initiated email.
 - **Use Active Directory Device Credentials:** Specify whether to use user credentials and group designations to connect to the SMTP server.
 - **Device Userid:** Specify the user ID to connect to the SMTP server.
 - **Device Password:** Specify the password to connect to the SMTP server.
 - **Kerberos 5 REALM:** Specify the realm for the Kerberos 5 authentication protocol.
 - **NTLM Domain:** Specify the domain name for the NTLM security protocol.

 Note: When SMTP Server is not configured, the settings in the **Setup Email Lists and Alerts** section are disabled.

- **Disable "SMTP server not set up" error:** Disable the SMTP server not set up error message.
- **Test Connection:** Configure the settings for test connection.
 - **Recipient Email Address:** Type the email address of the recipient.
 - **Send Test Email to Recipient:** Send a test email to the recipient email address.

 Note: Test email supports device-initiated emails only

- **Test:** Select to send the test email.

 Note: This option is enabled after you enter a valid address in the Recipient Email Address field.

3. Configure Email Defaults:

- **Subject:** Specify the email subject.
- **Message:** Specify the email message.
- **File Name:** Specify the file name for the scanned image.
- **Format:** Specify the file format for the scanned image.
- **PDF Settings:** Set the PDF format of the scanned image.
 - **PDF Version:** Specify the PDF version of the scanned image.
 - **Archival Version:** Specify the Archival Version of the scanned image.
 - **A-2u:** It simplifies the text searching and copying of Unicode text for digitally created PDF documents and PDF documents that were scanned with subsequent optical character recognition (OCR).



Note: The archival version, A-2u is only available for PDF version 1.7.

- **Secure:** Specify whether to enable security for the scanned image.
- **Archival (PDF/A):** Specify whether to enable archival for the scanned image.



Note: Archival Version and Archival (PDF/A) are supported only when PDF Version is set to 1.4 and 1.7.

- **Split Job by Pages:** Enter a number to split pages. The split pages are sent as separate emails. To disable, enter 0. The range is 1–999.
- **Content Type:** Specify the content type of the original document.
- **Content Source:** Specify the source of the original document.
- **Color:** Specify the color when scanning an image.
- **Resolution:** Set the resolution of the scanned image.
- **Darkness:** Adjust the darkness of the scanned image.
- **Orientation:** Specify the orientation of text and graphics on the page.
- **Original Size:** Set the paper size of the original document.
- **Sides:** Specify the page orientation of text and graphics when scanning a two-sided document.

4. Configure Advanced Imaging:

- **Color Balance:** Adjust the amount of toner being used in each color.
- **Color Dropout:** Specify which color to drop during scanning, and adjust the dropout setting for that color.
- **Auto Color Detect:** Set the amount of color that the printer detects from the original document.
 - **Color Sensitivity:** Specify the color sensitivity when scanning the original document.
 - **Area Sensitivity:** Specify the area sensitivity when scanning the original document.
 - **Email Bit Depth:** Specify the bit depth to use for images detected as mono when the Color setting is set to Auto.

- **Minimum Scan Resolution:** Set the minimum resolution for images detected as mono when the Color setting is set to Auto.
- **JPEG Quality:** Set the quality of a JPEG-format scanned image.
- **Contrast:** Specify the contrast for the output.
- **Background Removal:** Adjust the amount of background visible on a scanned image.
 - **Background Detection:** Specify the background detection.
 - **Level:** Specify the background removal level.
- **Mirror Image:** Create a mirror image of the original document.
- **Negative Image:** Create a negative image of the original document.
- **Shadow Detail:** Adjust the amount of shadow detail visible on a scanned image.
- **Scan Edge to Edge:** Allow edge-to-edge scanning of the original document.
- **Sharpness:** Adjust the sharpness of a scanned image.
- **Temperature:** Specify whether to generate a cooler or warmer output.
- **Blank Pages:** Specify whether to include blank pages.
 - **Blank Page Removal:** Specify whether to remove blank pages.
 - **Blank Page Sensitivity:** Specify the sensitivity for detecting blank pages.

5. Configure Admin Controls:

- **Max Email Size:** Set the allowable file size for each email.
- **Size Error Message:** Specify the error message that the printer sends when an email exceeds its allowable file size.
- **Limit Destinations:** Allow email to be sent only to the specified list of domain names.
- **Send Me a Copy:** Send a copy of the email to yourself.
- **Allow Self Emails Only:** Allow email to be sent to the email address for the logged-in user only.
- **Use cc:/bcc:** Enable carbon copy and blind carbon copy in email.
- **Use Multi-Page TIFF:** Choose between single- and multiple-page TIFF files.
- **TIFF Compression:** Set a compression option for TIFF files.
- **Text Default:** Set the quality of text on a scanned image.
- **Adjust ADF Skew:** Adjust the front-side and back-side skew angles.



Note: Adjust ADF Skew is disabled if Express Mode is On and if electronic deskew is not supported on the device. Examples of Express Mode are Express Scanning and Express Printing.

- **Text/Photo Default:** Set the quality of text or photo on a scanned image.
- **Photo Default:** Set the quality of a photo on a scanned image.
- **Transmission Log:** Print a log for successful email transmission.
- **Log Paper Source:** Specify the paper source for printing logs.
- **Allow Save as Shortcut:** Specify whether to allow email addresses to be saved as shortcuts.
- **Email Images Sent As:** Specify how to send the images in email.
- **Reset Email Information After Sending:** Restore the default email information after sending an email.

6. Configure Web Link Setup:




Note: Use the Web Link Setup to transfer scanned documents and images to an FTP server and send link to the documents and images to email recipients.

- **Server:** Set the FTP server address.
- **Login:** Set the user name of the FTP server.
- **Password:** Set the password to use for the user name on the FTP server.
- **Path:** Set path on the FTP server to transfer scanned documents and images.
- **File Name:** Set the file name to use for the web link.
- **Web Link:** Set the web link.

7. Click **Save**.**Customize Settings List**

This feature allows you to customize the settings on the screen.


1. Do one of the following:
 - To hide settings from the screen, drag and drop the settings from Settings List to More Settings List.
 - To show settings on the screen, drag and drop the settings from More Settings List section to Settings List.
2. Click **Save**.

 Note: To undo the changes, click **Reset**.


CONFIGURING THE FTP SETTINGS

 Note: Some settings are available only in some printer models.

1. From the Embedded Web Server, click **Settings > FTP**.
2. Configure FTP Defaults:
 - **Format:** Specify the file format for the scanned image.
 - **PDF Settings:** Set the PDF format of the scanned image.
 - **PDF Version:** Specify the PDF version of the scanned image.
 - **Archival Version:** Specify the Archival Version of the scanned image.
 - **A-2u:** It simplifies the text searching and copying of Unicode text for digitally created PDF documents and PDF documents that were scanned with subsequent optical character recognition (OCR).

 Note: The archival version, A-2u is only available for PDF version 1.7.

- **Secure:** Specify whether to enable security for the scanned image.
- **Archival (PDF/A):** Specify whether to enable archival for the scanned image.

 Note: Archival Version and Archival (PDF/A) are supported only when PDF Version is set to 1.4 and 1.7.

- **Content Type:** Specify the content type of the original document.
- **Content Source:** Specify the source of the original document.
- **Color:** Specify the color when scanning an image.
- **Resolution:** Set the resolution of the scanned image.
- **Darkness:** Adjust the darkness of the scanned image.
- **Orientation:** Specify the orientation of text and graphics on the page.
- **Original Size:** Set the paper size of the original document.
- **Sides:** Specify the page orientation of text and graphics when scanning a two-sided document.
- **File Name:** Specify the file name for the scanned image.

3. Configure Advanced Imaging:
 - **Color Balance:** Adjust the amount of toner being used in each color.
 - **Color Dropout:** Specify which color to drop during scanning, and adjust the dropout setting for that color.
 - **Auto Color Detect:** Set the amount of color that the printer detects from the original document.
 - **Color Sensitivity:** Specify the color sensitivity when scanning the original document.
 - **Area Sensitivity:** Specify the area sensitivity when scanning the original document.
 - **Scan Bit Depth:** Specify the bit depth to use for images detected as mono when the Color setting is set to **Auto**.
 - **Minimum Scan Resolution:** Set the minimum resolution for images detected as mono when the Color setting is set to **Auto**.
 - **JPEG Quality:** Set the quality of a JPEG-format scanned image.
 - **Contrast:** Specify the contrast of the output.
 - **Background Removal:** Adjust the amount of background visible on a scanned image.
 - **Background Detection:** Specify the background detection.
 - **Level:** Specify the background removal level.
 - **Mirror Image:** Create a mirror image of the original document.
 - **Negative Image:** Create a negative image of the original document.
 - **Shadow Detail:** Adjust the amount of shadow detail visible on a scanned image.
 - **Scan Edge to Edge:** Allow edge-to-edge scanning of the original document.
 - **Sharpness:** Adjust the sharpness of a scanned image.
 - **Temperature:** Specify whether to generate a cooler or warmer output.
 - **Blank Pages:** Specify whether to include blank pages.
 - **Blank Page Removal:** Specify whether to remove blank pages.
 - **Blank Page Sensitivity:** Specify the sensitivity for detecting blank pages.

4. Configure Admin Controls:

- **Text Default:** Set the quality of text on a scanned image.
- **Text/Photo Default:** Set the quality of text or photo on a scanned image.
- **Photo Default:** Set the quality of a photo on a scanned image.
- **Use Multi-Page TIFF:** Choose between single- and multiple-page TIFF files.
- **TIFF Compression:** Set a compression option for TIFF files.
- **Transmission Log:** Print a log for successful FTP scan transmission.
- **Log Paper Source:** Specify the paper source for printing FTP logs.
- **Adjust ADF Skew:** Adjust the front-side and back-side skew angles.



Note: Adjust ADF Skew is disabled if Express Mode is On and if electronic deskew is not supported on the device. Examples of Express Mode are Express Scanning and Express Printing.

- **Allow Save as Shortcut:** Specify whether to allow custom FTP settings to be saved as shortcuts.
- **Use Passive FTP:** When enabled, the FTP server specifies the data port that the printer will connect to.

5. Click **Save**.

Customize Settings List

This feature allows you to customize the settings on the screen.

1. Do one of the following:

- To hide settings from the screen, drag and drop the settings from Settings List to More Settings List.
- To show settings on the screen, drag and drop the settings from More Settings List section to Settings List.

2. Click **Save**.



Note: To undo the changes, click **Reset**.

CONFIGURING THE FLASH DRIVE SETTINGS



Note: Some settings are available only in some printer models.

1. From the Embedded Web Server, click **Settings > USB Drive**.

2. Configure the Flash Drive Scan settings:

- **Format:** Specify the file format for the scanned image.
- **PDF Settings:** Set the PDF format of the scanned image.
 - **PDF Version:** Specify the PDF version of the scanned image.
 - **Archival Version:** Specify the Archival Version of the scanned image.
 - **A-2u:** It simplifies the text searching and copying of Unicode text for digitally created PDF documents and PDF documents that were scanned with subsequent optical character recognition (OCR).



Note: The archival version, A-2u is only available for PDF version 1.7.

- **Secure:** Specify whether to enable security for the scanned image.
- **Archival (PDF/A):** Specify whether to enable archival for the scanned image.



Note: Archival Version and Archival (PDF/A) are supported only when PDF Version is set to 1.4 and 1.7.

- **Content Type:** Specify the content type of the original document.
- **Content Source:** Specify the source of the original document.
- **Color:** Specify the color when scanning an image.
- **Resolution:** Set the resolution of the scanned image.
- **Darkness:** Adjust the darkness of the scanned image.
- **Orientation:** Specify the orientation of text and graphics on the page.
- **Original Size:** Set the paper size of the original document.
- **Sides:** Specify the page orientation of text and graphics when scanning a two-sided document.
- **File Name:** Specify the file name for the scanned image.

3. Configure Advanced Imaging:

- **Color Balance:** Adjust the amount of toner being used in each color.
- **Color Dropout:** Specify which color to drop during scanning, and adjust the dropout setting for that color.
- **Auto Color Detect:** Set the amount of color that the printer detects from the original document.
 - **Color Sensitivity:** Specify the color sensitivity when scanning the original document.
 - **Area Sensitivity:** Specify the area sensitivity when scanning the original document.
 - **FTP Bit Depth:** Specify the bit depth to use for images detected as mono when the Color setting is set to Auto.

- **Minimum Scan Resolution:** Set the minimum resolution for images detected as mono when the Color setting is set to Auto.
- **JPEG Quality:** Set the quality of a JPEG-format scanned image.
- **Contrast:** Specify the contrast of the output.
- **Background Removal:** Adjust the amount of background visible on a scanned image.
 - **Background Detection:** Specify the background detection.
 - **Level:** Specify the background removal level.
- **Mirror Image:** Create a mirror image of the original document.
- **Negative Image:** Create a negative image of the original document.
- **Shadow Detail:** Adjust the amount of shadow detail visible on a scanned image.
- **Scan Edge to Edge:** Allow edge-to-edge scanning of the original document.
- **Sharpness:** Adjust the sharpness of a scanned image.
- **Temperature:** Specify whether to generate a cooler or warmer output.
- **Blank Pages:** Specify whether to include blank pages.
 - **Blank Page Removal:** Specify whether to remove blank pages.
 - **Blank Page Sensitivity:** Specify the sensitivity of detecting blank pages.

4. Configure Admin Controls:

- **Text Default:** Set the quality of text on a scanned image.
- **Text/Photo Default:** Set the quality of text or photo on a scanned image.
- **Photo Default:** Set the quality of a photo on a scanned image.
- **Use Multi-Page TIFF:** Choose between single- and multiple-page TIFF files.
- **TIFF Compression:** Set a compression option for TIFF files.
- **Adjust ADF Skew:** Adjust the front-side and back-side skew angles.



Note: Adjust ADF Skew is disabled if Express Mode is On and if electronic deskew is not supported on the device. Examples of Express Mode are Express Scanning and Express Printing.

Customize Scan Settings List

This feature allows you to customize the settings on the screen.

1. Do one of the following:

- To hide settings from the screen, drag and drop the settings from Settings List to More Settings List.
- To show settings on the screen, drag and drop the settings from More Settings List section to Settings List.

2. Click **Save**.



Note: To undo the changes, click **Reset**.

5. Configure Flash Drive Print:

- **Number of Copies:** Set the number of copies.
- **Paper Source:** Set the paper source for the print job.
- **Color:** Specify whether to print the output in color.
- **Collate:** Specify whether to print multiple copies in sequence.
- **Sides:** Specify whether to print on one side or two sides of the paper.
- **Flip Style:** Determine whether the long edge or the short edge of the paper is bound when performing two-sided printing.
- **Pages per Side:** Print multiple page images on one side of a sheet of paper.
- **Pages per Side Ordering:** Specify the positioning of multiple page images when using Pages per Side.
- **Pages per Side Orientation:** Specify the orientation of a multiple-page document when using Pages per Side.
- **Pages per Side Border:** Specify whether to print a border around each image when using Pages per Side.
- **Separator Sheets:** Specify whether to insert blank separator sheets when printing.
- **Separator Sheet Source:** Specify the paper source for the separator sheet.
- **Blank Pages:** Specify whether to print blank pages in a print job.

6. Click **Save**.

Note: To undo the changes, click **Reset**.

Customize Print Settings List

This feature allows you to customize the settings on the screen.

1. Do one of the following:

- To hide settings from the screen, drag and drop the settings from Settings List to More Settings List.
- To show settings on the screen, drag and drop the settings from More Settings List section to Settings List.

2. Click **Save**.

Note: To undo the changes, click **Reset**.

Creating a Shortcut



Note: Administrator rights are required to create a shortcut.

1. Open a web browser, then in the address field, type the printer IP address.
2. View the printer IP address on the printer home screen.

The IP address appears as four sets of numbers separated by periods, such as 123 . 123 . 123 . 123.

If you are using a proxy server, to load the web page correctly, disable the proxy server temporarily.

3. Click **Shortcuts > Add Shortcut**.
4. Select a shortcut type, and then configure the settings.
5. Click **Save**.


Managing Scan Center Destinations

Administrator rights are required to configure the application.


CONFIGURING A NETWORK DESTINATION

 Note: This application is supported only in some printer models.

1. From the Embedded Web Server, to navigate to the configuration page for the application, click **Apps > Scan Center > Configure**.
2. Click **Network Folder > Create Network Folder**.
3. Select the connection type, and then do one of the following:
 - For SMB, type or browse to the network folder.
 - For FTP or SFTP, type the FTP address and the port number.

 Note: For SFTP, set the port number to 22.

4. Configure the settings.
5. Click **Save**.


 Note: Refer to the following information:

- To use the home directory attribute in the Folder Address field, type % before and after the attribute. For example, %customAttribute%. You can also use other LDAP attributes such as %cn%, %sAMAccountName%, and %userPrincipalName%.
- To edit a destination, select a destination from the list.
- To delete a destination, for the destination, click the trash can icon.
- You can also prevent users from creating or editing destinations at the printer control panel.

CONFIGURING AN EMAIL DESTINATION

 Note: This application is supported only in some printer models.

1. From the Embedded Web Server, to navigate to the configuration page for the application, click **Apps > Scan Center > Configure**.
2. Click **Email > Create Email**.
3. Configure the settings.
4. Click **Save**.

 Note: Refer to the following information:

- To edit a destination, select a destination from the list.
- To delete a destination, for the destination, click the trash can icon.
- You can also prevent users from creating or editing destinations at the printer control panel.

CONFIGURING A FAX DESTINATION



Note: This application is supported only in some printer models.

1. From the Embedded Web Server, to navigate to the configuration page for the application, click **Apps > Scan Center > Configure**.
2. Click **Fax > Create Fax**.
3. Configure the settings.
4. Click **Save**.



Note: Refer to the following information:

- To edit a destination, select a destination from the list.
- To delete a destination, for the destination, click the trash can icon.
- You can also prevent users from creating or editing destinations at the printer control panel.

CONFIGURING A REMOTE PRINTER DESTINATION

You can scan documents on a supported printer and then send the scanned documents to another printer on the network.



Note: This application is supported only in some printer models.

1. From the Embedded Web Server, to navigate to the configuration page for the application, click **Apps > Scan Center > Configure**.
2. Click **Remote Printer > Create Remote Printer**.
3. Configure the settings.
4. Click **Save**.



Note: Refer to the following information:

- To edit a destination, select a destination from the list.
- To delete a destination, for the destination, click the trash can icon.
- You can also prevent users from creating or editing destinations at the printer control panel.

Faxing

This chapter contains:

Configuring the Fax Settings	48
Configuring Analog Fax Settings	49
Configuring the Fax Server	54

Configuring the Fax Settings

SETTING THE FAX MODE

1. From the Embedded Web Server, click **Settings > Fax > Fax Defaults**.
2. From the **Fax Mode** field, select a fax mode:
 - **Fax**: Send fax jobs through a telephone line.
 - **Fax Server**: Send fax jobs through a fax server.



Note: This setting is available only in some printer models.

- **Disabled**: Disable Fax Mode.
3. Click **Save**.

Configuring Analog Fax Settings

GENERAL FAX SETTINGS



Note: Some settings are available only in some printer models.

1. From the Embedded Web Server, click **Settings > Fax > Fax Setup > General Fax Settings**.
2. Configure the settings.
 - **Fax Name:** Identify your fax machine.
 - **Fax Number:** Identify your fax number.
 - **Fax ID:** Specify whether to notify recipients of your fax name or fax number.
 - **Memory Use:** Set the amount of internal printer memory allocated for faxing.
 - **Cancel Faxes:** Cancel outgoing faxes before they are transmitted, or cancel incoming faxes before they finish printing.
 - **Fax Number Masking:** Specify the format for masking an outgoing fax number.
 - **Digits to Mask:** Specify the number of digits to mask in an outgoing fax number.
 - **Enable Line Connected Detection:** Determine whether a telephone line is connected to the printer.
 - **Enable Line In Wrong Jack Detection:** Determine whether a telephone line is connected to a wrong jack.
 - **Enable Extension In Use Support:** Determine the extension printer line to be used in Use Support.



Note: This feature is available only if the fax card is installed and supports two jacks.

- **Optimize Fax Compatibility:** Configure the printer fax functionality for optimal compatibility with other fax machines.
 - **Fax Transport:** Set the transport to use for faxing.
3. Click **Save**.

FAX SEND SETTINGS



Note: Some settings are available only in some printer models.

1. From the Embedded Web Server, click **Settings > Fax > Fax Setup > Fax Send Settings**.

2. Configure the settings.
 - **Resolution:** Set the resolution of the scanned image.
 - **Original Size:** Specify the size of the original document.
 - **Orientation:** Specify the orientation of the original document.
 - **Sides:** Specify the page orientation of text and graphics when scanning a two-sided document.
 - **Content Type:** Specify the content type of the original document.
 - **Content Source:** Specify the source of the original document.
 - **Darkness:** Adjust the darkness of the scanned image.
 - **Behind a PABX:** Set the printer to dial a fax number without waiting to recognize the dial tone.
 - **Dial Mode:** Specify the dial mode for incoming or outgoing faxes.
3. Configure Advanced Imaging:
 - **Color Balance:** Adjust the amount of toner being used in each color.
 - **Color Dropout:** Specify which color to drop during scanning, and adjust the dropout setting for that color.
 - **Contrast:** Specify the contrast of the output.
 - **Background Removal:** Adjust the amount of background visible on a scanned image.
 - **Background Detection:** Specify the background detection.
 - **Level:** Specify the background removal level.
 - **Mirror Image:** Create a mirror image of the original document.
 - **Negative Image:** Create a negative image of the original document.
 - **Shadow Detail:** Adjust the amount of shadow detail visible on a scanned image.
 - **Scan Edge to Edge:** Allow edge-to-edge scanning of the original document.
 - **Sharpness:** Adjust the sharpness of a scanned image.
 - **Temperature:** Specify whether to generate a cooler or warmer output.

4. Configure Admin Controls:
 - **Automatic Redial:** Adjust the number of redial attempts based on the activity levels of recipient fax machines.
 - **Redial Frequency:** Increase the time between redial attempts to increase the chance of sending a fax successfully.
 - **Enable ECM:** Activate Error Correction Mode (ECM) for fax jobs.
 - **Enable Fax Scans:** Fax documents that are scanned at the printer.
 - **Allow Save as Shortcut:** Save fax numbers as shortcuts in the printer.
 - **Max Speed:** Set the maximum speed for sending a fax.
 - **Enable Color Fax Scans:** Enable color scans for faxes.
 - **Auto Convert Color Faxes to Mono Faxes:** Convert all outgoing color faxes to black and white.
 - **Confirm Fax Number:** Ask the user to confirm the fax number.
 - **Dial Prefix:** Set a dialing prefix.
 - **Dialing Prefix Rules:** Establish a dialing prefix rule.
5. Click **Save**.

FAX RECEIVE SETTINGS



Note: Some settings are available only in some printer models.

1. From the Embedded Web Server, click **Settings > Fax > Fax Setup > Fax Receive Settings**.
2. Configure the settings.
 - **Fax Job Waiting:** Remove fax jobs that request specific unavailable resources from the print queue.
 - **Rings to Answer:** Set the number of rings for an incoming fax.
 - **Auto Reduction:** Scale the incoming fax to fit on the page.
 - **Paper Source:** Set the paper source for printing an incoming fax.
 - **Sides:** Print on both sides of the paper.
 - **Separator Sheets:** Specify whether to insert blank separator sheets when printing.
 - **Separator Sheet Source:** Specify the paper source for the separator sheet.
 - **Output Bin:** Specify the output bin for received faxes.
 - **Fax Footer:** Print the transmission information at the bottom of each page from a received fax.
 - **Fax Footer Time Stamp:** Print the time stamp at the bottom of each page from a received fax.
3. Configure Holding Faxes.

Held Fax Mode: Hold received faxes from printing until they are released.

4. Configure Admin Controls:

- **Enable Fax Receive:** Set the printer to receive faxes.
- **Enable Color Fax Receive:** Set the printer to receive faxes in color.
- **Enable Caller ID:** Show the number that is sending the incoming fax.
- **Block No Name Fax:** Block incoming faxes sent from devices with no station ID or fax ID specified.
- **Banned Fax List:** Specify the phone numbers that you want to block.
- **Answer On:** Set a distinctive ring pattern for incoming faxes.
- **Manual Answer Code:** Set the answer code for incoming manual faxes.



Note: Manual Answer Code is tied to Manual Fax support.

- **Auto Answer:** Set the printer to receive faxes automatically.
- **Fax Forwarding:** Specify how to forward received faxes.
- **Forward to:** Specify a forwarding destination for received faxes.
- **Confirmation Email:** Send a confirmation email when fax forwarding is successful.
- **Max Speed:** Set the maximum speed for transmitting faxes.

5. Click **Save**.

FAX COVER PAGE



Note: Some settings are available only in some printer models.

1. From the Embedded Web Server, click **Settings > Fax > Fax Setup > Fax Cover Page**.
2. Configure the settings.
 - **Fax Cover Page:** Configure the settings for the fax cover page.
 - **Include To field:** Specify whether to enable the To field.
 - **Include From field:** Specify whether to enable the From field.
 - **From:** Set the From field.
 - **Include Message Field:** Specify whether to enable the Message field.
 - **Message:** Set the Message field.
 - **Include Logo:** Specify whether to enable the logo.
 - **Import Fax Logo:** Set the logo.
 - **Include Footer [x]:** Specify whether to enable the Footer [x] field.
 - **Footer [x]:** Set the Footer [x] field.
3. Click **Save**.

FAX LOG SETTINGS



Note: Some settings are available only in some printer models.

1. From the Embedded Web Server, click **Settings > Fax > Fax Setup > Fax Log Settings**.
2. Configure the settings.
 - **Transmission Log:** Print log for successful fax transmission or transmission error.
 - **Transmission Log Frequency:** Specify how often the transmission log is created.
 - **Transmission Log Action:** Print or email a log for successful fax transmission or transmission error.



Note: To exclude PDF attachment in the Transmission Log, disable the **Include faxed document** option.

- **Receive Error Log:** Print a log for fax-receive failures.
 - **Auto Print Logs:** Print all fax activity.
 - **Log Paper Source:** Specify the paper source for printing logs.
 - **Logs Display:** Identify the sender by remote fax name or fax number.
 - **Enable Job Log:** View a summary of all fax jobs.
 - **Enable Call Log:** View a summary of fax dialing history.
 - **Log Output Bin:** Specify the output bin for printed logs.
3. Click **Save**.

SPEAKER SETTINGS



Note: Some settings are available only in some printer models.

1. From the Embedded Web Server, click **Settings > Fax > Fax Setup > Speaker Settings**.
2. Configure the settings.
 - **Speaker Mode:** Set the fax speaker mode.
 - **Speaker Volume:** Adjust the fax speaker volume.
 - **Ringer Volume:** Enable the ringer volume.
3. Click **Save**.

Configuring the Fax Server

GENERAL FAX SETTINGS

1. From the Embedded Web Server, click **Settings > Fax > Fax Server Setup > General Fax Settings**.
2. Configure the settings.
 - **To Format:** Specify a fax recipient.
 - **Reply Address:** Specify a reply address for sending faxes.
 - **Subject:** Specify the fax subject.
 - **Message:** Specify the fax message.
 - **Enable analog receive:** Set the printer to receive analog faxes.
3. Click **Save**.

FAX SERVER EMAIL SETTINGS



Note: Some settings are available only in some printer models.

1. From the Embedded Web Server, click **Settings > Fax > Fax Server Setup > Fax Server Email Settings**.

2. Configure the settings.
 - **Primary SMTP Gateway:** Type the IP address or host name of the primary SMTP server for sending email.
 - **Primary SMTP Gateway Port:** Type the port number of the primary SMTP server.
 - **Secondary SMTP Gateway:** Type the server IP address or host name of your secondary or backup SMTP server.
 - **Secondary SMTP Gateway Port:** Type the server port number of your secondary or backup SMTP server.
 - **SMTP Timeout:** Set the time before the printer times out when the SMTP server does not respond.
 - **Reply Address:** Specify a reply address for sending faxes.
 - **Always Use SMTP Default Reply Address:** Specify the SMTP reply address for sending faxes.
 - **Use SSL/TLS:** Specify whether to send a fax using an encrypted link.
 - **Require Trusted Certificate:** Require a trusted certificate when accessing the SMTP server.
 - **SMTP Server Authentication:** Set the authentication type for the SMTP server.
 - **Device-Initiated Email:** Specify whether credentials are required for device-initiated email.
 - **User-Initiated Email:** Specify whether credentials are required for user-initiated email.
 - **Use Active Directory Device Credentials:** Specify whether to use user credentials and group designations to connect to the SMTP server.
 - **Device Userid:** Specify the user ID to connect to the SMTP server.
 - **Device Password:** Specify the password to connect to the SMTP server.
 - **Kerberos 5 REALM:** Specify the realm for the Kerberos 5 authentication protocol.
 - **NTLM Domain:** Specify the domain name for the NTLM security protocol.
 - **Disable "SMTP server not set up" error:** Disable the SMTP server not set up error message.
 - **Test Connection:** Configure the settings for test connection.
 - **Recipient Email Address:** Type the email address of the recipient.
 - **Send Test Email to Recipient:** Send a test email to the recipient email address.

 Note: Test email supports device-initiated emails only

- **Test:** Select to send the test email.

 Note: This option is enabled after you enter a valid address in the Recipient Email Address field.

3. Click **Save**.

FAX SERVER SCAN SETTINGS

1. From the Embedded Web Server, click **Settings > Fax > Fax Server Setup > Fax Server Scan Settings**.

2. Configure the settings.
 - **Image Format:** Specify the file format for the scanned image.
 - **Content Type:** Specify the content type of the original document.
 - **Content Source:** Specify the source of the original document.
 - **Sides:** Specify the page orientation of text and graphics when scanning a two-sided document.
 - **Fax Resolution:** Set the fax resolution.
 - **Darkness:** Set the darkness of the output.
 - **Orientation:** Specify the orientation of text and graphics on the page.
 - **Original Size:** Set the paper size of the original document.
 - **Use Multi-Page TIFF:** Choose between single- and multiple-page TIFF files.
3. Click **Save**.

Networking

This chapter contains:

Configuring the HTTP/FTP Settings	58
Selecting the Active Network Adapter	59
Connecting to a Wireless Network.....	60

Configuring the HTTP/FTP Settings



Note: These settings are available only in network printers or printers attached to print servers.

1. From the Embedded Web Server, click **Settings > Network/Ports > HTTP/FTP Settings**.
2. Configure the settings.

Proxy

- **HTTP Proxy IP Address:** Configure the HTTP server settings.
- **HTTP Default IP Port:** The factory default port for HTTP is 80.
- **FTP Proxy IP Address:** Configure the FTP server settings.
- **FTP Default IP Port:** The factory default port for FTP is 21.
- **Authentication:** Specify the authentication credentials.
- **User Name:** Specify the unique user name.
- **Password:** Specify the unique password.
- **Local Domains:** Specify domain names for HTTP and FTP servers.

Other Settings

- **Enable HTTP Server:** Allow access to the Embedded Web Server for printer monitoring and management.
 - **Enable HTTPS:** Configure the HyperText Transfer Protocol Secure (HTTPS) settings.
 - **Force HTTPS Connections:** Force the printer to use the HTTPS connections.
 - **Enable FTP/TFTP:** Send files using FTP.
 - **HTTPS Device Certificate**
 - **Timeout for HTTP/FTP Requests:** Specify the time before the server connection stops.
 - **Retries for HTTP/FTP Requests:** Set the number of retries to connect to the HTTP/FTP server.
3. Click **Save**.

Selecting the Active Network Adapter

1. From the Embedded Web Server, click **Settings > Network/Ports > Network Overview > Active Adapter**.
2. Select the network adapter.

- **Auto:** Switch automatically to an available network connection.



Note: Ethernet connection takes precedence over wireless connection. Remove the Ethernet cable to allow the printer to detect the configured wireless network.

- **Standard Network:** Disable the wireless network connection and set the printer to connect only through Ethernet connection.
- **Wireless:** Disable the Ethernet network connection and set the printer to connect only through wireless connection.



Note: This setting appears only when a wireless network adapter is installed in the printer.

3. Click **Save**.

Connecting to a Wireless Network

Before you begin, ensure that:

- Your printer is connected temporarily to an Ethernet network.
 - A wireless network adapter is installed in your printer and working properly. For details, refer to the instruction sheet that came with your wireless network adapter.
1. From the Embedded Web Server, click **Settings > Network/Ports > Wireless**.
 2. Modify the settings to match the settings of your wireless router.



Note: Ensure that you type the correct network name.

3. Click **Save**.
4. Disconnect the Ethernet cable, then wait for at least one minute.
5. Ensure that your printer is connected to the network. Print a network setup page, then in the Wireless section, check if the Card Status is **Connected**.
For more information, refer to the Networking section of the *User Guide* for your printer model.

Securing Printers

This chapter contains:

Securing Network Connections	62
Managing Devices Remotely	65
Managing Login Methods	69
Managing Certificates	81
Managing Other Access Functions	83
Securing Data	89

Securing Network Connections

CONFIGURING THE TLS SETTINGS

Transport Layer Security (TLS) encrypts device communication over a network to provide privacy and integrity of customer data.

To configure TLS:

1. From the Embedded Web Server, click **Settings > Network/Ports > TCP/IP**.
2. For TLS Version for Secure Device Communication over a Network, enable TLSv1.0, TLSv1.1, or TLSv1.2. These settings pertain to the Embedded Web Server only. They do not pertain to clients using TLS.



Note: TLSv1.3 is supported by default, and cannot be disabled. Deselecting the other TLS settings will force the EWS to use TLSv1.3 only.

3. Click **Save**.



Note: For more information on each port, contact your system administrator.

CONFIGURING TCP/IP PORT ACCESS SETTINGS

You can control device network activities by configuring your device to filter out traffic on specific network connections. You can disable protocols, such as FTP, HTTP, and Telnet.

Port filtering on devices disables network connections individually. When a port is closed, a device does not respond to traffic on the specified port even if the corresponding network application is enabled.

We recommend that you close any ports that you do not plan to use during standard operation.

1. From the Embedded Web Server, click **Settings > Network/Ports > TCP/IP > TCP/IP Port Access**.
2. Enable access to the TCP/IP ports.
3. Click **Save**.



Note: For more information on each port, contact your system administrator.

CONFIGURING IP SECURITY SETTINGS


Apply IP Security (IPsec) between the printer and the workstation or server to secure traffic between the systems with a strong encryption. The printers support IPsec with pre-shared keys (PSKs) and certificates. You can use both options simultaneously.

When you use PSK authentication, printers are configured to establish a secure IPsec connection with up to seven other systems. The printers and systems are configured with a key or passphrase that is used to authenticate the systems and to encrypt the data.


When you use the CA certificate authentication, printers are configured to establish a secure IPsec connection with up to five systems or subnets. Printers exchange data securely with many systems, and the process is integrated with a PKI or CA infrastructure. Certificates provide a robust and scalable solution, without configuring or managing keys or passphrases.

1. From the Embedded Web Server, click **Settings > Network/Ports > IPsec**.


2. Select **Enable IPSec**.
3. To specify the encryption and authentication methods of the printer, configure the following settings:
 - Base Configuration
 - DH (Diffie-Hellman) Group Proposal

 Note: This feature is enabled when Base Configuration is set to **Compatibility**.


 - Proposed Encryption Method

 Note: This feature is enabled when Base Configuration is set to **Compatibility**.


 - Proposed Authentication Method

 Note: This feature is enabled when Base Configuration is set to **Compatibility**.


 - IPSec Device Certificate

 Note: Before you can select a device certificate, ensure that the certificate is installed. For details, refer to [Managing Certificates](#).

 - IKE SA Lifetime (Hours): By default, it is 24.


 Note: This feature is enabled when Base Configuration is set to **Secure**.

 - IPSec SA Lifetime (Hours): By default, it is 8.


 Note: This feature is enabled when Base Configuration is set to **Secure**.
4. Do one or more of the following:
 - In the Pre-Shared Key Authenticated Connections section, type the IP address of the client printer that you want to connect to the printer using Pre-Shared Key based IPSec Authentication.
 - In the Certificate Authenticated Connections section, type the IP address of the client printer that you want to connect to the printer using Certificate based IPSec Authentication.
5. Click **Save**.
 - If no CA certificates are added, then the default certificate is used.
 - If you are using PSK authentication, then type the corresponding key. Retain the key to use later when configuring client printers.

CONFIGURING 802.1X AUTHENTICATION


Though normally associated with wireless devices and connectivity, 802.1x authentication supports both wired and wireless environments.

 Note: If you are using digital certificates to establish a secure connection to the authentication server, then configure the certificates on the printer before changing 802.1x authentication settings.

For details, refer to [Managing Certificates](#).

 Note: Ensure that all printers on the same network using 802.1x are supporting the same EAP authentication type.


1. From the Embedded Web Server, click **> Settings > Network/Ports > 802.1x**.
2. In the 802.1x Authentication section, do the following:
 - a. Select **Active**.
 - b. Type the login name and password that the printer uses to log in to the authentication server.
 - c. Select **Validate Server Certificate**.

 Note: Server certificate validation is necessary when using Transport Layer Security (TLS), Protected Extensible Authentication Protocol (PEAP), and Tunneled Transport Security Layer (TTLS).

- d. Select **Enable Event Logging**.

Warning—Potential Damage: To reduce flash part wear, use this feature only when necessary.

- e. In the 802.1x Device Certificate list, select a digital certificate.

 Note: If only one certificate is installed, then Default is the only option that appears.

3. In the Allowable Authentication Mechanisms section, select one or more authentication protocols.
 - **EAP-MD5, EAP-MSCHAPv2, LEAP, and PEAP:** These options require a login name and password.
 - **EAP-TLS:** This option requires a login name, a CA certificate, and a signed printer certificate.
 - **EAP-TTLS:** This option requires a login name and password and a CA certificate.
4. From the TTLS Authentication Method menu, select an authentication method.
5. Click **Save**.

SETTING THE RESTRICTED SERVER LIST

You can configure printers to connect only from a list of specified TCP/IP addresses. This action blocks all TCP connections from other addresses, and protects the printer against unauthorized printing and configuration.

1. From the Embedded Web Server, click **Settings > Network/Ports > TCP/IP**.
2. In the Restricted Server List field, type up to 50 IP addresses, separated by commas, that are allowed to make TCP connections.
3. Click **Save**.
4. Configure the **Restricted Server List** options:

 Note: This setting is available only in some printer models.

- **Block All Ports:** This option addresses the ports that are not in the restricted server list, and blocks all access to the ports (default).
- **Block Printing Only:** This option addresses the ports that are not in the restricted sever list, and blocks only the printing.
- **Block Printing and HTTP Only:** This option addresses the ports that are not in the restricted server list and blocks only printing and HTTP.

Managing Devices Remotely

USING HTTPS FOR PRINTER MANAGEMENT

To restrict the access of the printer Embedded Web Server to HTTPS only, disable the HTTP port and leave the HTTPS port (443) active. This action ensures that all communication with the printer using the Embedded Web Server is encrypted.

1. From the Embedded Web Server, click **Settings > Network/Ports > TCP/IP > TCP/IP Port Access**.
2. Clear **TCP 80 (HTTP)**.
3. Click **Save**.

SETTING UP SNMP

Configuring Settings for SNMP Versions 1 or 2c

1. From the Embedded Web Server, click **Settings > Network/Ports > SNMP**.
2. In the SNMP Versions 1 and 2c section, select **Enabled > Allow SNMP Set**.
3. In the GET SNMP Community field, type a name for the GET SNMP Community identifier. The default community name is `public`.
4. In the SET SNMP Community field, type a variable for SET SNMP. The default variable is `private`.
5. To facilitate the automatic installation of print drivers and other printing applications, select **Enable PPM MIB** (Printer Port Monitor MIB).
6. Click **Save**.

Configuring Settings for SNMP Version 3

Before you begin, disable SNMP versions 1 and 2c.

1. From the Embedded Web Server, click **Settings > Network/Ports > SNMP**.
2. In the SNMP Version 3 section, select **Enabled**.
3. If required, to configure the following options, provide your authentication credentials.
 - **Set Read/Write Credentials:** Allow remote installation and configuration changes and printer monitoring.
 - **Set Read-only Credentials:** Allow printer monitoring only.
4. In the Authentication Hash menu, select the hash function of your SNMP server.
5. For Minimum Authentication Level, select **Authentication, Privacy**.
6. In the Privacy Algorithm menu, select the strongest setting that is supported by your network environment.
7. Click **Save**.

Configuring SNMP Traps

After configuring SNMP settings, you can customize which alerts are sent to the network management system by designating events (SNMP traps) that trigger an alert message.

1. From the Embedded Web Server, click **Settings > Network/Ports > SNMP > Set SNMP Traps**.
2. In one of the IP Address fields, type the IP address of the network management server or monitoring station.
3. Select the conditions for which you want to generate an alert.
4. Click **Save**.

CONFIGURING SECURITY AUDIT LOG SETTINGS

The security audit log allows administrators to monitor security-related events on a device, including failed user authorization, successful administrator authentication, and Kerberos file uploads to a device. By default, security logs are stored on the device, but can also be transmitted to a network system log (syslog) server for processing or storage.



Note: Security Audit Log settings are available for selected printer models only.

Xerox recommends that you enable audit in secure environments.

1. From the Embedded Web Server, click **Settings > Security > Security Audit Log**.
2. To activate security audit logging, select **Enable Audit**.
The transmission to a network syslog server option lets you use both the remote syslog server and the internal logging.
3. Configure transmission to a network syslog server.
 - a. Select **Enable Remote Syslog**.
 - b. Configure the Remote Syslog settings.
 - **Remote Syslog Server:** Type the IP address or host name of the server.
 - **Remote Syslog Port:** Type the port number used for the destination server. The default number is 514.
 - **Remote Syslog Method:** To send log messages and events using a lower-priority transmission protocol, select **Normal UDP**. Otherwise, select **Stunnel**.
 - **Remote Syslog Facility:** Select a facility code for events logged to the destination server. All events sent from the device are tagged with the same code, which aids in sorting and filtering by network monitor or intrusion detection software.
 - **Severity of Events to Log:** Select the priority level cutoff for logging messages and events. The highest severity is 0. The lowest severity is 7. Events with the selected severity level and higher are logged. For example, if you select 4 - Warning, then severity levels 0-4 are logged.
 - **Remote Syslog Non-Logged Events:** Send all events to the remote server, regardless of severity.


4. Configure the email notification settings.
To ensure that the printer settings have been configured for email, in the Admin's Email Address field, type one or more email addresses separated by commas.
 - **Email Log Cleared Alert:** Send a notification when the user clicks the Delete Log button.
 - **Email Log Wrapped Alert:** Send a notification when the log becomes full and begins to overwrite the oldest entries.
 - **Log Full Behavior:** Wrap over oldest entries or email the log and then delete all entries.
 - **Email % Full Alert:** Send a notification when log storage space reaches a certain percentage of capacity.
 - **% Full Alert Level:** Specify how full the log is before an alert is triggered.
 - **Email Log Exported Alert:** Send a notification when the log file is exported.
 - **Email Log Settings Changed Alert:** Send a notification when the log settings are changed.
 - **Log Line Endings:** Specify how the log file terminates the end of each line.
 - **Digitally Sign Exports:** Add a digital signature to each exported log file.
5. Click **Save**.

MANAGING SECURITY AUDIT LOGS

1. To delete the syslog, in the Clear Log menu, click **Clear**.
2. To view or save the syslog, in the Export Log menu, select the file type, and then click **Export**.

UPDATING SOFTWARE

Printers inspect all downloaded firmware packages for some required attributes before they adopt and execute the packages. The firmware is packaged in a proprietary format and encrypted with a symmetric encryption algorithm through an embedded key that is known only to the manufacturer. However, the strongest security measure comes from the requirement that all firmware packages include multiple digital 2048-bit RSA signatures from the manufacturer. If these signatures are not valid, or if the message logs indicate a change in firmware after the signatures were applied, then the firmware is discarded.

 Note: Firmware downgrades are not permitted.

1. From the Embedded Web Server, click **Settings > Device > Software Update**.
2. Do one of the following:
 - Browse to the firmware file, then click **Upload**.
 - Click **Check now > I agree, start update**.

TPM Firmware Update

A Trusted Platform Module (TPM) is used to secure critical cryptographic keys. The TPM can be updated with the most recent available firmware.

 Note: This setting is available only in some printer models.

1. From the Embedded Web Server, click **Settings > Security > TPM Firmware Update**.

2. Following settings are displayed:
 - **Current Version:** Displays the current version of the firmware.
 - **Available Version:** Displays the available version of the firmware.
3. For Update TPM firmware, click **Start**.

A prompt appears which indicates that the device will shutdown and auto reboot.
4. Click **Proceed** or **Cancel**.

Managing Login Methods

RESTRICTING PUBLIC ACCESS ON THE GUEST ACCOUNT

The guest account can use the printer without logging in. To control the access of guest account users, restrict the functions, applications, printer management, and security options for the guest account.

1. From the Embedded Web Server, click **Settings > Security > Login Methods**.
2. In the Public section, click **Manage Permissions**.
3. Select the access controls that the guest account can access. For details, refer to [Understanding Access Controls](#).
4. Click **Save**.

USING LOCAL ACCOUNTS

Local accounts are stored in the printer memory and provide authentication-level security.

Creating Local Accounts

1. From the Embedded Web Server, click **Settings > Security > Login Methods**.
2. In the Local Accounts section, click **Add User**.
3. Select the type of authentication method that you want the account to use to log in to the printer.
 - **User Name/Password:** Add an account with a user name and password.
 - **User Name:** Add an account with a user name only.
 - **Password:** Add an account with a password only.
 - **PIN:** Add an account with a personal identification number (PIN) only.
4. From the User Information section, type the user information and authentication credentials.
5. From the Permission Groups section, select one or more groups.



Note: To create a group for the user, select **Add New Group**. For details, refer to [Creating Local Account Groups](#).

6. Click **Save**.

Editing and Deleting Local Accounts

1. From the Embedded Web Server, click **Settings > Security > Login Methods**.
2. In the Local Accounts section, click the authentication method to which the user account belongs.
3. Click the user account that you want to edit or delete.

4. Do one of the following:
 - To edit the user account, update the user information, then click **Save**.
 - To delete the user account, click **Delete User**.



Note: To delete multiple user accounts, select the accounts, then click **Delete**.

Creating Local Account Groups

Use groups to customize access for the user to applications and printer functions.

1. From the Embedded Web Server, click **Settings > Security > Login Methods**.
2. Do one of the following:
 - Add a group when managing permissions, or
 - Add a group when creating or editing a user account.
3. To add a group when managing permissions, perform the following:
 - a. From the Local Accounts section, click **Manage Groups/Permissions**.
 - b. Click **Add Group**.
4. To add a group when creating or editing a user account, perform the following:
 - a. Create or edit a user account.
 - b. In the Permission Groups section, select **Add New Group**.
5. Type a unique group name.
6. In the Access Controls section, select the functions, menus, and applications that the group can access.
7. Click **Save**.

To import access controls from another group, click **Import Access Controls**, then select a group. For details on access controls, refer to [Understanding Access Controls](#).

Editing or Deleting Local Account Groups

1. From the Embedded Web Server, click **Settings > Security > Login Methods**.
2. In the Local Accounts section, click **Manage Groups/Permissions**.
3. Click the group, then do one of the following:
 - Configure the access controls, then click **Save**.
 - Click **Delete Group**.

To import access controls from another group, click **Import Access Controls**, then select a group. To delete multiple groups, select the groups, then click **Delete**.

For details on access controls, refer to [Understanding Access Controls](#).

USING LDAP OR LDAP+GSSAPI


LDAP is a standards-based, cross-platform, extensible protocol that runs directly on top of the TCP/IP layer. LDAP is used to access information stored in a specially organized information directory. LDAP can interact with many different kinds of databases without special integration, which makes LDAP more flexible than other authentication methods.

When you want your transmission always to be secure, use LDAP+GSSAPI. Instead of authenticating directly with the LDAP server, the user is first authenticated using Kerberos to obtain a Kerberos ticket. This ticket is presented to the LDAP server using the GSSAPI protocol for access. LDAP+GSSAPI is typically used for networks that run Active Directory.

- LDAP+GSSAPI requires a Kerberos network account. For details, refer to [Creating a Kerberos Login Method](#).
- Supported printers can store a maximum of eight unique LDAP or LDAP+GSSAPI login methods. A unique name is required for each method.
- Administrators can create up to 32 user-defined groups that apply to each unique login method.
- LDAP and LDAP+GSSAPI rely on an external server for authentication. If the server is down, then users cannot access the printer using LDAP or LDAP+GSSAPI.
- To help prevent unauthorized access, log out from the printer after each session.

Creating an LDAP or LDAP+GSSAPI Login Method

1. From the Embedded Web Server, click **Settings > Security > Login Methods**.
2. In the Network Accounts section, click **Add Login Method > LDAP**.
3. Select the authentication type:
 - **LDAP**
 - **LDAP+GSSAPI**
4. Configure General Information settings.
 - **Setup Name:** Type a unique name for the LDAP network account.
 - **Server Address:** Type the IP address or the host name of the LDAP server.
 - **Server Port:** Type the port number to which LDAP queries are sent.

 Note: If you are using SSL, then use port 636. Otherwise, use port 389.

- **Required User Input:** Select the required LDAP authentication credentials to be used when a user logs in to the printer. This setting is available only in the LDAP setup.
- **Use Integrated Windows Authentication:** Select one of the following:
 - **Do not use**
 - **Use if available:** Use Windows operating system authentication credentials, if available.
 - **Require:** Use Windows operating system authentication credentials only.

 Note: This setting is available only in the LDAP+GSSAPI setup.

5. Configure Device Credentials settings.

- **Anonymous LDAP Bind:** Bind the printer with the LDAP server anonymously. This option is applicable only if your LDAP server allows anonymous binding. Enabling this option does not require you to provide authentication credentials. This option is available only in the LDAP setup.
- **Use Active Directory Device Credentials:** Use user credentials and group designations that are pulled from the existing network comparable to other network services. This option is available only in the LDAP +GSSAPI setup.
- If **Anonymous LDAP Bind** or **Use Active Directory Device Credentials** is disabled, then provide the authentication credentials used to bind the printer with the LDAP server.
 - **Device Username**
 - For LDAP setup, type the fully qualified distinguished name (DN) of a user registered to the LDAP server.
 - For LDAP+GSSAPI setup, type the DN of a user registered to the Kerberos server.
 - **Device Realm:** The realm used for the Kerberos server. This setting is available only for the LDAP +GSSAPI setup.
 - **Device Password:** Type the password for the user.

6. Configure Advanced Options settings.




Note: Some Advanced Options settings are available only in some printer models.

- **Use SSL/TLS:** If the LDAP server requires SSL, then select **SSL/TLS**.
- **Require Certificate:** If the LDAP server requires a certificate, then select **Yes**.
- **Userid Attribute:** Type the LDAP attribute to search for when authenticating user credentials. The default value is `sAMAccountName`, which is common in a Windows operating system environment. For other directories, you can type `uid`, `cn`, or a user-defined attribute. For details, contact your system administrator.
- **Mail Attribute:** Type the LDAP attribute that contains the email addresses for users. The default value is `mail`.
- **Fax number Attribute:** Type the LDAP attribute that contains the fax number for users. The default value is `facsimiletelephonenumber`.
- **Full Name Attribute:** Type the LDAP attribute that contains full names for users. The default value is `cn`.
- **Home Directory Attribute:** Type the LDAP attribute that contains the home directory for users. The default value is `homeDirectory`.
- **Group Membership Attribute:** Type the LDAP attribute required for group search. The default value is `memberOf`.
- **Search Base:** This setting is the node in the LDAP server where user accounts reside. You can type multiple search bases, separated by commas.



Note: A search base consists of multiple attributes separated by commas, such as `cn` (common name), `ou` (organizational unit), `o` (organization), `c` (country), and `dc` (domain).

- **Search Timeout:** Type a value from 5 to 30 seconds or 5 to 300 seconds, depending on your printer model.
- **Follow LDAP Referrals:** Search the different servers in the domain for the logged-in user account.

7. Configure Search Specific Object Classes settings.
 - **person:** Search the person object class.
 - **Custom Object Classes:** Type the name of the custom object class to search.
-  Note: A maximum of three custom object classes can be searched. Type the other object class in the other Custom Object Class field.
8. Configure Address Book Setup settings.
The following settings are used to configure the address book used when scanning to an email address.
 - **Displayed Name:** Select the LDAP attribute that you want to show on the address book.
 - **Max Search Results:** Type the maximum search results shown on the address book.
 - **Use User Credentials:** Use the logged-in user credentials to connect to the LDAP server.
 - **Search Attributes:** Select LDAP attributes used as search filters.
 - **Custom Attributes:** Type LDAP custom attributes used as search filters.
 9. Click **Save and Verify**.

Editing or Deleting the LDAP or LDAP+GSSAPI Login Method

1. From the Embedded Web Server, click **Settings > Security > Login Methods**.
2. In the Network Accounts section, click the **LDAP** or **LDAP+GSSAPI** login method.
3. Do one of the following:
 - To edit the login method, update the LDAP or LDAP+GSSAPI settings, then click **Save and Verify**.
 - To delete the login method, click **Delete LDAP**.

USING KERBEROS

You can use the Kerberos login method alone or in conjunction with the LDAP+GSSAPI login method.



- Only one Kerberos configuration file can be saved to the printer memory. This configuration file can apply to multiple realms and Kerberos Domain Controllers.
- When you upload another configuration file or update the Kerberos settings, the saved configuration file is overwritten.
- If you want to delete a Kerberos file, before you delete the file, first delete the LDAP+GSSAPI login method that is using the file.
- Administrators are required to anticipate the different types of authentication requests the Kerberos server can receive, and to configure the configuration file to handle the requests.
- Kerberos relies on an external server for authentication. If the server is down, then users cannot access the printer using Kerberos.
- To help prevent unauthorized access, after each session, log out from the printer.

Creating a Kerberos Login Method

1. From the Embedded Web Server, click **Settings > Security > Login Methods**.
2. In the Network Accounts section, click **Add Login Method > Kerberos**.
3. Do one of the following:
 - Create a simple Kerberos configuration file.
 - Import a Kerberos configuration file.
4. To create a simple Kerberos configuration file, from the Generate Simple Kerberos File section, configure the following:
 - **KDC Address:** Type the IP address or host name of the KDC IP.
 - **KDC Port:** Enter the port number used by the Kerberos server.
 - **Realm:** Type the realm used by the Kerberos server. It is required that you type the realm in uppercase.
5. To import a Kerberos configuration file, in the Import Kerberos File field, browse to the `krb5.conf` file.
6. In the Miscellaneous Settings section, configure the following settings, as needed:
 - **Character Encoding:** Select the character encoding used for the configuration file.
 - **Disable Reverse IP Lookups**
7. Click **Save and Verify**.

Setting the Date and Time

When you use Kerberos authentication, ensure that the time difference between the printer and the domain controller does not exceed five minutes. You can update the date and time settings manually, or to sync the time with the domain controller automatically, you can use the Network Time Protocol (NTP).

1. From the Embedded Web Server, click **Settings > Device > Preferences > Date and Time**.
2. To configure the date and time manually, perform the following:
 -  Note: Manual configuration disables NTP.
 - a. From the Configure section, in the Manually Set Date and Time field, enter the appropriate date and time.
 - b. Select the date format, time format, and time zone.
 -  Note: For Time Zone, if you select **(UTC+user) Custom**, then specify the offset values for UTC (GMT) and DST.
3. To set the date and time automatically, configure NTP:
 - a. In the Network Time Protocol section, select **Enable NTP**, then type the IP address or host name of the NTP server.
 - b. If the NTP server requires authentication, then in the Enable Authentication menu, select **MD5 key**.
 - c. Depending on your printer model, either type the key ID and password, or browse to the file containing the NTP authentication credentials.
4. Click **Save**.

USING ACTIVE DIRECTORY

You can use the Active Directory login method alone or in conjunction with the LDAP+GSSAPI login method.

- Only one Kerberos configuration file can be saved in the printer memory. This configuration file can apply to multiple realms and Kerberos Domain Controllers.
- Administrators are required to anticipate the different types of authentication requests the Kerberos server can receive, and to configure the configuration file to handle the requests.
- Uploading another configuration file or updating the Kerberos settings overwrites the saved configuration file.
- Active Directory relies on an external server for authentication. If the server is down, then users cannot access the printer using Active Directory.
- To help prevent unauthorized access, after each session, log out from the printer.

Creating an Active Directory Login Method

1. From the Embedded Web Server, click **Settings > Security > Login Methods**.
2. In the Network Accounts section, click **Add Login Method > Active Directory**.
3. Configure the settings.
 - **Domain:** Type the realm or domain name of the Active Directory server.
 - **User Name:** Type the name of the user that can authenticate to the Active Directory.
 - **Password:** Type the password of the user.
 - **Organizational Unit:** Type the organizational unit attribute to which the user belongs.
4. Click **Join Domain**.

Editing or Deleting an Active Directory Login Method

1. From the Embedded Web Server, click **Settings > Security > Login Methods**.
2. In the Network Accounts section, click the **Active Directory** login method.
3. To delete the login method, click **Unjoin Domain**.
4. Configure the General Information settings.
 - **Setup Name:** Type a unique name for the Active Directory login method.
 - **Server Address:** Type the IP address or the host name of the LDAP server.
 - **Server Port:** Enter the port where queries are sent.
 - **Required User Input:** Select the required authentication credentials when logging in to the printer.
 - **Use Integrated Windows Authentication.** Select one of the following:
 - **Do not use**
 - **Use if available:** Use Windows operating system authentication credentials, if available.
 - **Require:** Use only Windows operating system authentication credentials.

5. Configure the Device Credentials options.
 - **Use Active Directory Device Credentials:** Use user credentials and group designations that are pulled from the existing network comparable to other network services.
 - If **Use Active Directory Device Credentials** is disabled, then provide the authentication credentials used to bind the printer with the Active Directory server.
 - **Device Username:** Type the fully qualified DN of a user registered to the Active Directory server.
 - **Device Realm:** The Active Directory domain name.
 - **Device Password:** Type the password for the user.
6. Configure the Advanced Options settings.



Note: Some Advanced Options settings are available only in some printer models.

- **Use SSL/TLS:** If the LDAP server requires SSL, then select **SSL/TLS**.
- **Require Certificate:** If the LDAP server requires a certificate, then select **Yes**.
- **Userid Attribute:** Type the LDAP attribute to search for when authenticating user credentials. The default value is `sAMAccountName`, which is common in a Windows environment. For other directories, you can type `uid`, `cn`, or a user-defined attribute. For more information, contact your system administrator.
- **Mail Attribute:** Type the LDAP attribute that contains the email addresses for users. The default value is `mail`.
- **Fax number Attribute:** Type the LDAP attribute that contains the fax number for users. The default value is `facsimiletelephonenumber`.
- **Full Name Attribute:** Type the LDAP attribute that contains the full names for users. The default value is `cn`.
- **Home Directory Attribute:** Type the LDAP attribute that contains the home directory for users. The default value is `homeDirectory`.
- **Group Membership Attribute:** Type the LDAP attribute required for group search. The default value is `memberOf`.
- **Search Base:** This setting is the node in the LDAP server where user accounts reside. You can type multiple search bases, separated by commas.



Note: A search base consists of multiple attributes separated by commas, such as `cn` (common name), `ou` (organizational unit), `o` (organization), `c` (country), and `dc` (domain).

- **Search Timeout:** Enter a value from 5 to 30 seconds or 5 to 300 seconds, depending on your printer model.
- **Follow LDAP Referrals:** Search the different servers in the domain for the logged-in user account.

7. Configure the Search Specific Object Classes settings.
 - **person:** Search the person object class.
 - **Custom Object Classes:** Type the name of the custom object class to search.



Note: You can search a maximum of three custom object classes. In the other Custom Object Class field, type the other object class.

8. Configure the Address Book Setup settings.
Use the following settings to configure the address book used when scanning to an email address:
 - **Displayed Name:** Select the LDAP attribute that you want to show on the address book.
 - **Max Search Results:** Type the maximum search results shown on the address book.
 - **Use User Credentials:** Connect to the LDAP server with the credentials for the logged-in user.
 - **Search Attributes:** Select LDAP attributes used as search filters.
 - **Custom Attributes:** Type LDAP custom attributes used as search filters.
9. Click **Save and Verify**.

CREATING LDAP, LDAP+GSSAPI, KERBEROS, OR ACTIVE DIRECTORY GROUPS

To customize user access to applications and printer functions, you can use groups.

1. From the Embedded Web Server, click **Settings > Security > Login Methods**.
2. In the Network Account section, click the **LDAP, LDAP+GSSAPI, Kerberos, or Active Directory** login method.
3. Click **Manage Groups > Add Group**.
4. Choose one of the following:
 - Search for the group name or user name, or
 - Add the group manually.
5. To search for the group name or user name, perform the following:
 - a. Select how you want to search for the group in your LDAP server.
 - b. Depending on the search scope selected, type the group name or the user name.
 - c. Click **Search**.
 - d. Select the group that you want to add.
 - e. Click **Add Selected**.
6. To add the group manually, perform the following:
 - a. Click **Manual Add**.
 - b. In the Group Name field, type the name of the group.
 - c. In the Group Identifier field, type the LDAP identifier for the group.
 - d. Click **Submit**.
7. Select the group, then in the Access Controls section, select the functions, menus, and applications that the group can access.
8. Click **Save**.

To import access controls from another group, click **Import Access Controls**, then select a group.

For details on access controls, refer to [Understanding Access Controls](#).

EDITING OR DELETING LDAP, LDAP+GSSAPI, OR ACTIVE DIRECTORY GROUPS

1. From the Embedded Web Server, click **Settings > Security > Login Methods**.
2. Click the **LDAP, LDAP+GSSAPI, or Active Directory** login method, then click **Manage Groups**.
3. Click the group, then do one of the following:
 - Configure the access controls, then click **Save**.
 - Click **Delete Group**.
 - To import access controls from another group, click **Import Access Controls**, then select a group.
 - To delete multiple groups, select the groups, then click **Delete**.

For details on access controls, refer to [Understanding Access Controls](#).

UNDERSTANDING ACCESS CONTROLS

Access controls allow you to limit user access to functions, applications, and printer management.



Note: Some access controls are available only in some printer models.

Function Access

The following access controls modify user access to available printer functions:

- **Access Address Book in Apps:** Use Address Book from eSF applications that support Address Book.
- **Manage Shortcuts:** Access the Manage Shortcuts menu, and enable the Save as Shortcut option available in the Copy, Email, Fax, and FTP functions.
- **Modify Address Book:** Enable the Search Address Book option available in the Email, Fax, and FTP functions when accessed from the printer home screen.
- **Create Profiles:** Create profiles for printing, copying, scanning, emailing, or faxing.
- **Manage Bookmarks**
- **Flash Drive Print:** Print from a flash drive.
- **Flash Drive Color Printing:** Print from a flash drive in color.
- **Flash Drive Scan:** Scan to a flash drive.
- **Copy Function:** Use the copy function.
- **Copy Color Printing:** Copy documents in color.
- **Color Dropout:** Specify the color to drop during scanning and copying, and adjust the dropout setting for each color threshold. If a user authentication fails for a protected scan or copy job, then the Color Dropout function is not used even when it is enabled.
- **Email Function:** Use the email function.
- **Fax Function:** Use the fax function. If the function is disabled, then:
 - All analog fax functions and the fax server are disabled.
 - The fax icon does not appear.

- No fax-related intervention-required messages appear on the printer display.
- The printer does not answer incoming calls or print driver faxes.



Note: The Embedded Web Server and control panel show fax-related settings even if this function is disabled.

- **FTP Function:** Scan to an FTP network folder from the printer home screen. The FTP icon is hidden by default. To show the FTP icon on the home screen:
 1. From the Embedded Web Server, click **Settings > Device > Visible Home Screen Icons**.
 2. Select **FTP**.
- **Release Held Faxes:** Enable the Held Faxes and Release Held Faxes options on the printer home screen.
- **Held Jobs Access:** Enable the Held Jobs and Search Held Jobs options on the printer home screen.
- **Use Profiles:** Restrict access to protected profiles. If a user accesses a protected profile, then the printer prompts for credentials to execute the profile. Enable this access control for the application that does not specify permission to access the profiles.
- **Cancel Jobs at the Device:** Cancel jobs from the printer home screen.
- **Change Language:** Enable the Change Language option on the printer home screen.
- **Internet Printing Protocol (IPP):** Allow authenticated users to configure and use the IPP port.
- **Initiate Scans Remotely:** Allow authenticated users to initiate remote scanning.
- **B/W Print:** Allow authenticated users to print in black and white.
- **Color Print:** Allow authenticated users to print in color.
- **Network Folder - Scan:** Scan to a network folder.

Administrative Menus

The following access controls modify user access to the menus in the Embedded Web Server that are used to manage functions, applications, and security:

- **Security Menu:** Manage login methods and configure other security options.
- **Network/Ports Menu:** Configure network connections.
- **Paper Menu:** Configure the paper settings.
- **Reports Menu:** View reports.
- **Function Configuration Menus:** Configure the settings for the functions that are available in the printer.
- **Supplies Menu:** Manage printer supplies.
- **Option Card Menu:** Configure the option cards installed in the printer. This control is available only when an option card is installed.
- **SE Menu:** View diagnostic logs.
- **Manage Shortcuts:** Manage shortcuts that are available in the printer.
- **Address Book:** Manage the address book.
- **Device Menu:** Configure the printer firmware settings.

Device Management

The following access controls modify user access to use printer management options:

- **Remote Management:** Access the printer remotely.
- **Firmware Updates:** Update the printer firmware through any port.
- **Apps Configuration:** Configure the installed applications. If this control is enabled, then users can configure, start/stop, uninstall, and view logs of applications that are installed in the printer.
- **Operator Panel Lock:** Configure the locking function of the printer home screen. If this control is enabled, then users can lock and unlock the printer home screen.
- **Import / Export All Settings:** Import or export a printer settings file (.zip and .ucf) from the Embedded Web Server.
- **Out of Service Erase:** Clear all settings, applications, and pending jobs stored in the printer memory, or erase all data in the printer hard disk.
- **Embedded Web Server Access:** Control access to the Embedded Web Server. If this control is restricted, then access to the EWS requires login.

Apps

- **New Apps:** Use applications from the printer home screen.
- **Card Copy:** Use Card Copy from the printer home screen.
- **Slideshow:** Use Slideshow from the printer home screen.
- **Change Wallpaper:** Use Change Wallpaper from the printer home screen.
- **Screen Saver:** Use Screen Saver from the printer home screen.
- **Forms and Favorites:** Use Forms and Favorites from the printer home screen.
- **Scan Center:** Use Scan Center from the printer home screen.

Managing Certificates

Certificates are used when you want the printer to establish an SSL/TLS, IPsec, or 802.1x connection and to identify other devices on the network securely. Printers can also use these certificates for LDAP over SSL authentication and address book lookups.

Certificate Authorities (CA) are trusted locations established on the network that are required in secure environments. Otherwise, the default printer certificate is used to identify devices on the network.

CONFIGURING PRINTER CERTIFICATE DEFAULTS

1. From the Embedded Web Server, click **Settings > Security > Certificate Management**.
2. In the Device Certificates section, click **Configure Certificate Defaults**.
3. Configure the settings.

- **Friendly Name:** Type a unique name for the certificate.
- **Common Name:** Type the name for the printer.

 Note: If you want to use the printer host name, then leave this field blank.

- **Organization Name:** Type the name of the company or organization that issues the certificate.
- **Unit Name:** Type the name of the unit within the company or organization that issues the certificate.
- **Country/Region:** Type the country or region where the company or organization that issues the certificate is located.
- **Province Name:** Type the name of the province or state where the company or organization that issues the certificate is located.
- **City Name:** Type the name of the city where the company or organization that issues the certificate is located.
- **Subject Alternate Name:** Type the alternate name and prefix that conforms to RFC 2459. For example, type an IP address using the format `IP : 1 . 2 . 3 . 4`, or a DNS address using the format `DNS : ldap . company . com`.

 Note: If your printer is using an IPv4 address, then leave this field blank.

4. Click **Save**.

CREATING A PRINTER CERTIFICATE

1. From the Embedded Web Server, click **Settings > Security > Certificate Management**.
2. In the Device Certificates section, click **Generate**.
3. Configure the settings. For details, refer to [Configuring Printer Certificate Defaults](#).
4. Click **Generate** or **Generate and Download**.

INSTALLING CERTIFICATES MANUALLY

For details on how to download the CA certificate automatically, refer to [Installing Certificates Automatically](#).

Before you configure Kerberos or domain controller settings, install the CA certificate used for domain controller validation. If you want to use chain validation for the domain controller certificate, then install the entire certificate chain. Each certificate requires a separate PEM (.cer) file.

1. From the Embedded Web Server, click **Settings > Security > Certificate Management**.
2. In the Manage CA Certificates section, click **Upload CA**, then browse to the PEM (.cer) file.

The following is a sample certificate:

```
-----BEGIN CERTIFICATE-----
MIIE1jCCA76gAwIBAgIQY6sV0KL3tIhBt1r4gHG85zANBgkqhkiG9w0BAQUFADBs
...
13DTbPe0mnIbTq0iWqKEaVne1vvaDt52iSpEQyevwgUcHD16rFy+sOnCaQ==
-----END CERTIFICATE-----
```

3. Click **Save**.

INSTALLING CERTIFICATES AUTOMATICALLY

1. From the Embedded Web Server, click **Settings > Security > Certificate Management > Configure Certificate Auto Update**.
2. If you are prompted to join an Active Directory domain, click **Join Domain**, then type the domain information.
3. Select **Enable Auto Update**.



Note: If you want to install the CA certificate without waiting for the scheduled run time, select **Fetch Immediately**.

4. Click **Save**.

VIEWING, DOWNLOADING, AND DELETING CERTIFICATES

1. From the Embedded Web Server, click **Settings > Security > Certificate Management**.
2. Select a certificate from the list.
3. Select one or more of the following:
 - **Delete:** Remove a previously stored certificate.



Note: To delete multiple certificates, select the certificates, then click **Delete**.

- **Download To File:** Download or save the certificate as a PEM (.cer) file.
- **Download Signing Request:** Download or save the signing request as a .csr file.
- **Install Signed Certificate:** Upload a previously signed certificate.

Managing Other Access Functions

UNIVERSAL PRINT

Universal Print is a cloud-based print protocol that provides a simple and secure print solution for Microsoft® 365 users. Universal Print allows administrators to manage printers without the need for on-premises print servers. Universal Print enables users to access cloud printers without the need for print drivers.

You can use the Universal Print page to enable and register your Xerox® device for Universal Print.

Prerequisites

- Microsoft Azure AD Account
- Windows 10 Client version 1903 or higher or Windows 11 Client

Universal Print Status

The Universal Print area displays the registration status of your device for Universal Print. The statuses include the following:

- `Device is not currently registered with Universal Print`: This status appears when Universal Print is not registered.
- `Waiting for user to authenticate`: This status appears when registration is in process and the device is waiting for the user to authenticate to Microsoft.com.
- `Waiting to finish registration`: This status appears when registration is in process and the user has authenticated to Microsoft.com.
- `Device is online and registered with Universal Print`: This status appears when registration is successful.
- `Successfully deregistered printer from Universal Print`: This status appears when your local device deregistration is successful.

Registering a Device for Universal Print

1. In the Embedded Web Server, click **Settings > Network/Ports > Universal Print**.
2. To change the default printer name, in the Printer Name field, enter a new name.
3. Click **Register**.

The registration process authenticates the device with Microsoft® Azure® Active Directory.

4. The Register Device window appears. To copy the registration code, click **Copy**, then click the displayed link: <https://microsoft.com/devicelogin>.



Note:

- The registration process needs to complete before the code expires.
 - The registration code expires after 15 minutes.
5. A Microsoft-managed Web page opens. Do the following:

- a. At the Enter code window, paste the registration code into the Code field, then click **Next**.
- b. At the Pick an account window, select the appropriate Microsoft® account.



Note: For registration, select an available Microsoft® account. The selected account is used solely to establish a trusted connection for the device with the Universal Print service. After registration, Universal Print does not use the account again.

- c. The Xerox Universal Print window appears. Click **Continue**, then close the window.
6. If the code expires or registration fails, the status appears as *Device is not currently registered with Universal Print* in the Universal Print area. Repeat the registration process.
7. If registration is successful, the status appears as *Device is online and registered with Universal Print* in the Universal Print area. The device is available as a cloud printer in the Universal Print service.
8. To allow users to access the device, the Azure® administrator needs to share the printer in the Microsoft® Azure® portal.
 - a. In a Web browser, go to <https://portal.azure.com/#home>, then log in using the account previously used to register the device.
 - b. For Azure services, click **Universal Print**.
 - c. In the Manage area, click **Printers**.

The list of registered printers appears.
 - d. Select your printer, then click **Share**.

The Share printers window appears.
 - e. To change the default printer name, update the Share name field for the cloud printer. A unique share name allows the users to easily identify the cloud printer in the network.
 - f. To allow access to the cloud printer for everyone in the organization, click the toggle button.
 - g. To select the users that you need to share the printer with, in the Select member(s) area, click the names of the users. To locate users, use the search by name option.
 - h. Click **Share Printer**. When printer sharing is complete, a confirmation message appears.

After the printer is shared, an authorized user can discover the device using the Add Printer feature in Windows 10. The device appears as a cloud printer in the discovered printers list.
9. To add a cloud printer in Windows 10 and later or Windows 10 and 11:
 - a. Click **Settings > Printers & Scanners > Add a printer or scanner**.
 - b. Select the cloud printer in the list of discovered printers, then click **Add device**.

Administrator Functions for Universal Print

To Deregister your local device from Universal Print:

1. In the Embedded Web Server, click **Settings > Network/Ports > Universal Print**.
2. In the Registration area, click **Deregister**.
3. At the prompt, click **OK**.

4. Wait a few minutes until the displayed status changes to `Successfully deregistered printer from Universal Print`.
5. Click **Continue**.
6. To remove the printer from the Universal Print server, in a Web browser, go to the Azure portal <https://portal.azure.com/#home>, then log in with your credentials.
7. In the Azure portal, for Manage, click **Printers**, then select your printer.
8. Click **Delete Printer Share**, then click **OK**.
9. Click **Unregister**, then at the prompt, click **Unregister Printer**.

Upon completion, a message appears stating that `This printer has been successfully unregistered`. Additionally, the printer is removed from the list of registered devices.

SCHEDULING ACCESS TO USB DEVICES

In secure environments, you can configure devices to limit or disable the capabilities of USB host ports.

You can disable the front USB port using access control restrictions. Devices also have a rear USB port designed for card readers and human interface devices, such as a keyboard.

1. From the Embedded Web Server, click **Settings > Security > Schedule USB Devices**.
2. Select a device action, then specify when the device performs the action.
3. Click **Save**.

To reactivate use of the USB host ports, for each Disable schedule entry, create an Enable schedule entry.

You can create multiple schedules.

SETTING LOGIN RESTRICTIONS

To prevent malicious access to a device, you can restrict the number of invalid login attempts and require a lockout time before a user can try to log in again.


Many organizations establish login restrictions for information assets such as workstations and servers. Ensure that device login restrictions also comply with organizational security policies.

1. From the Embedded Web Server, click **Settings > Security > Login Restrictions**.
2. Set the login restrictions.
 - **Login Failures:** Specify the number of times a user can attempt to log in before being locked out.
 - **Failure Time Frame:** Specify how long a user can attempt to log in before lockout takes place.
 - **Lockout Time:** Specify how long the lockout lasts.
 - **Web Login Timeout:** Specify how long a user can be logged in remotely before being logged out automatically.
3. Click **Save**.


CONFIGURING CONFIDENTIAL PRINTING

Users that print confidential or sensitive information can use the confidential print option. This option allows print jobs to remain in the print queue until the user enters a PIN on the printer control panel.


1. From the Embedded Web Server, click **Settings > Security > Confidential Print Setup**.
2. Enter an option for the following:
 - **Max Invalid PIN:** Set the number of times an invalid PIN can be entered.
 - When the limit is reached, the print jobs for that user name and PIN are deleted.
 - This setting appears only when a formatted, working printer hard disk is installed.
 - To turn off this setting, type 0.
 - **Confidential Job Expiration:** Set the expiration time for confidential print jobs.
 - Confidential held jobs are stored in the printer until they are released or deleted manually.
 - Changes in this setting do not affect the expiration time for confidential print jobs that are already in the printer memory or hard disk.
 - If the printer is powered off, then all confidential jobs held in the printer memory are deleted.
 - **Repeat Job Expiration:** Set the expiration time for a repeat print job.

 Note: Repeat held jobs are stored in the printer memory for reprinting.

 - **Verify Job Expiration:** Set the expiration time for job verification. After the printer prints the first copy, the printer waits until the expiration time, then prints the remaining copies.

 Note: The Verify Jobs option prints one copy to ensure that the quality is satisfactory before printing the remaining copies.


 - **Reserve Job Expiration:** Set the expiration time for reserve job storage. The printer stores print jobs until the expiration time.

 Note: Reserve held jobs are automatically deleted after printing.

 - **Require All Jobs to be Held:** Set the printer to hold all print jobs.
 - **Keep Duplicate Documents:** Set the printer to print other documents with the same file name without overwriting any of the print jobs.
3. Click **Save**.

ENABLING SOLUTIONS LDAP SETTINGS

1. From the Embedded Web Server, click **Settings > Security > Solutions LDAP Settings**.
2. Select one or more of the following:
 - **Follow LDAP Referrals:** Search the different servers in the domain for the logged-in user account.
 - **LDAP Certificate Verification**

 Note: To effectuate the changes, restart the device.
3. Click **Save**.

SHOWING SECURED APPLICATIONS OR FUNCTIONS ON THE HOME SCREEN

By default, the secured applications or functions are hidden from the printer home screen.

1. From the Embedded Web Server, click **Settings > Security > Miscellaneous**.
2. From the Protected Features menu, select **Show**.
3. Click **Save**.


ENABLING PRINT PERMISSION

Use this feature for cost control. Whether users are allowed to print color or black and white depends on the permission configuration for the user. For details, refer to [Managing Login Methods](#).

1. From the Embedded Web Server, click **Settings > Security > Miscellaneous**.
2. Select **Print Permission**.
3. Click **Save**.

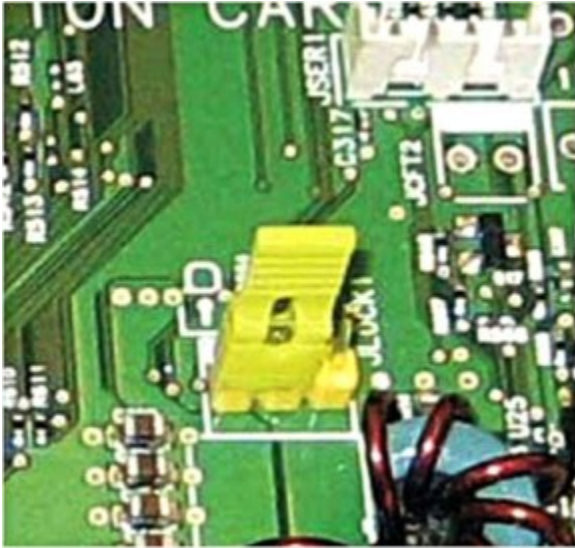
ENABLING THE SECURITY RESET JUMPER

If the device is locked down because of a forgotten administrator password or lost network connectivity, to recover the device, you can reset it. Access the controller board and move the reset jumper to cover the middle and exposed prongs.

 Note: If you forget the administrator password, for instructions, contact Xerox Technical Support.

To ensure that the device is not maliciously reset, secure access to the controller board with a cable lock.

Warning—Potential Damage: Resetting the device deletes all customer data.



The secure reset feature requires that, in the Embedded Web Server, you specify the effect of using the security reset jumper, which is on the controller board.

 Note: Some settings are available only in some printer models.

1. From the Embedded Web Server, click **Settings > Security > Miscellaneous**.
2. From the Security Reset Jumper menu, select one of the following:
 - **Enable Guest Access:** Provide guests with full access control.
 - **No Effect:** All protected access controls remain protected.

Warning—Potential Damage: If this option is selected, then the device is locked down and you cannot access the security menus. To replace the device controller board and regain access to the security menus, a service call is required.

3. If required, in the Minimum Password Length field, type a value.
4. To enable the password or to reveal the PIN, click **Enable Password/PIN Reveal**.
5. To encrypt non-volatile storage components, enable **Allow Encryption of Service Nonvolatile Memory**.
6. Click **Save**.

Securing Data

CONFIGURING PRINTER SETTINGS



Note: Some settings are available only in some printer models.

1. From the Embedded Web Server, click **Settings > Device > Maintenance**.
2. Depending on the printer model, click **Config Menu** or **Configuration Menu**.
3. Configure the USB Configuration settings.
 - **USB PnP:** Change the USB driver mode of the printer to improve its compatibility with a personal computer.
 - **USB Scan to Local:** Set whether the USB device driver enumerates as a USB Simple device (single interface) or as a USB Composite device (multiple interfaces).
 - **USB Speed:** Set the USB port to run at full speed and disable its high-speed capabilities.
4. Configure the Tray Configuration settings.
 - **Tray Linking:** Specify if the tray is linked automatically.
 - **Show Tray Insert Message:** Show a message about the tray status.
 - **A5 Loading:** Specify the page orientation when loading A5 paper size.
 - **Paper Prompts:** Set the paper source that the user fills when a prompt to load paper appears.
 - **Envelope Prompts:** Set the paper source that the user fills when a prompt to load envelope appears.
 - **Action for Prompts:** Set the printer to resolve paper- or envelope-related change prompts.
 - **Multiple Universal Sizes:** Enables each tray to support a unique universal (custom) size.



Note: This setting is visible only for printer models configured with optional trays.

5. Configure the Reports settings.
Print reports about printer menu settings, status and event logs.
 - **Menu Settings Page**
 - **Event Log**
 - **Event Log Summary**
6. Configure the Supply Usage and Counters setting.
 - **Clear Supply Usage History:** Reset the supply page counter or view the total printed pages.
 - **Reset Maintenance Counter:** Reset the maintenance counter of the total printed pages.
 - **Fuser Reset:** Reset the counter after installing a new supply.
 - **ITM Reset:** Reset the counter after installing a new supply.
 - **Tiered Coverage Ranges:** Adjust the range for the amount of color coverage on the printed page.
7. Configure Fax Configuration setting.
For the **Fax Low Power Support**, specify the printer power setting when it is in fax mode.

8. Configure the Print Configuration settings.

- **Font Sharpening:** Set a text point-size value below which the high-frequency screens are used when printing font data. For example, if the value is 24, then all fonts sized 24 points or less use the high-frequency screens.
- **Print Density:** Adjust the toner density when printing documents.
- **Copy Density:** Adjust the toner density when copying documents.

9. Configure the Device Operations settings.

- **Quiet Mode:** Set the printer to reduce the amount of noise that it makes when printing.



Note: This setting slows down the overall performance of the printer.

- **Panel Menus:** Set the printer to show the control panel menus.
- **Safe Mode:** Set the printer to safe mode.
- **Minimum Copy Memory:** Specify the minimum copy memory of the device.
- **Clear Custom Status:** Erase all custom messages.
- **Clear all remotely-installed messages:** Erase all remotely installed messages.
- **Automatically Display Error Screens:** Set the printer to show error messages automatically.
- **Honor orientation on fast path copy:** Set the printer to determine if it will honor (or not) the page image orientation on a fast path copy.

10. Configure the Scanner Configuration settings.


- **Scanner Manual Registration**
 - **Print Quick Test:** Print a Quick Test target page.




Note: Ensure that the margin spacing on the target page is uniform all the way around the target. If it is not, then reset the printer margins.

- **Front ADF Registration:** After you replace the ADF, scanner glass, or controller board, register the front ADF manually.
- **Rear ADF Registration:** After you replace the ADF, scanner glass, or controller board, register the rear ADF manually.

- **Flatbed Registration:** After you replace the ADF, scanner glass, or controller board, register the flatbed manually.
- **Edge Erase:** Set the size, in millimeters, of the no-print area around an ADF, or flatbed scan job.
 - **ADF Edge Erase**
 - **Flatbed Edge Erase**
- **ADF Des skew:** Set to adjust the front side and back side of the skew angles separately of the device.

 Note: The maximum amount of skew correction that can be applied to media of Letter/A4 width is 5%.

- **Disable Scanner:** If the scanner is not working properly, disable the scanner.
- **Tiff Byte Order:** Set the byte order of a TIFF-formatted scan output.
- **Exact Tiff Rows Per Strip:** Set the RowsPerStrip tag value of a TIFF-formatted scan output.
- **Scanner Glass Cleaning Threshold:** Specify the number of scans from the ADF before a user is prompted to clean the scanner glass.

 Note: The range of the number of scans is from 1000 to 3000.

11. Click **Save**.

ERASING PRINTER MEMORY

To erase volatile memory or buffered data in your printer, power off the printer.


To erase nonvolatile memory or individual settings, printer and network settings, security settings, and embedded solutions, do the following:

1. From the Embedded Web Server, click **Settings > Device > Maintenance > Out of Service Erase**.
2. In the Erase Printer Memory section, select **Sanitize all information on nonvolatile memory**.
3. If required, in the After erasing all nonvolatile memory section, select either **Start initial setup wizard** or **Leave printer offline after erasing the printer memory**.
4. To further configure Erase Printer Memory settings, select the following:
 - **Erase all printer and network settings**
 - **Erase all apps and app settings**
 - **Erase all shortcuts and shortcut settings**

 Note: By default, if you select **Sanitize all information on nonvolatile memory**, the above three settings gets selected automatically.

5. Click **Start**.

ERASING PRINTER HARD DISK MEMORY

 Note: This process can take from several minutes to more than an hour. During this time, the printer is unavailable for other tasks.

The following instructions are available only in printer models with a hard disk installed.

1. From the Embedded Web Server, click **Settings > Device > Maintenance > Out of Service Erase**.
2. In the Erase Hard Disk section, select **Sanitize all information on hard disk**.
3. Click **Start**.

CONFIGURING PRINTER HARD DISK ENCRYPTION



Note: Before performing this procedure, read the following information.

- Disk encryption erases the contents of the hard disk. If needed, back up important data from the printer before starting the encryption.
- Do not power off the printer during the encryption process. Loss of data can occur.
- Disk encryption can take from several minutes to more than an hour. During this time, the printer is unavailable for other tasks.

The following instructions are available only in printer models with a hard disk installed.

1. From the Embedded Web Server, click **Settings > Security > Disk Encryption**.
2. Click **Start encryption**.



Note: In the latest firmware version, disk encryption is by default disabled without the option to enable it.

RESTORING FACTORY DEFAULT SETTINGS



Note: Some settings are available only in some printer models.

1. From the Embedded Web Server, click **Settings > Device > Restore Factory Defaults**.
2. Select the settings that you want to restore.
 - **Restore printer settings:** Restore all the printer settings to their default values.
 - **Restore network settings:** Restore all the network settings to their default values.
 - **Restore fax settings:** Restore all the fax settings to their default values.
 - **Restore app settings:** Restore all the app settings to their default values.
3. Click **Start**.

STATEMENT OF VOLATILITY

Your printer contains various types of memory that can store printer and network settings and user data.

TYPE OF MEMORY	DESCRIPTION
Volatile memory	Your printer uses standard random access memory (RAM) to buffer user data temporarily during simple print jobs.
Nonvolatile memory	Your printer can use two forms of nonvolatile memory: EEPROM and NAND (flash memory). Both types are used to store the operating system, printer settings, network information and bookmark settings, and embedded solutions.
Hard disk memory	Some printers have a hard disk drive installed. The printer hard disk is designed for printer-specific functionality. The hard disk lets the printer retain buffered user data from complex print jobs, form data, and font data.

Erase the content of any installed printer memory in the following circumstances:

- The printer is being decommissioned.
- The printer hard disk is being replaced.
- The printer is being moved to a different department or location.
- The printer is being serviced by someone from outside your organization.
- The printer is being removed from your premises for service.
- The printer is being sold to another organization.

Disposing of a printer hard disk



Note: Some printer models do not have a printer hard disk installed.

In high-security environments, extra steps are needed to ensure that confidential data stored in the printer hard disk cannot be accessed. This precaution is necessary when the printer, or its hard disk, is removed from your premises.

- **Degaussing:** Flushes the hard disk with a magnetic field that erases stored data
- **Crushing:** Physically compresses the hard disk to break component parts and render them unreadable
- **Milling:** Physically shreds the hard disk into small metal bits



Note: Most data can be erased electronically, but the only way to guarantee that all data are completely erased is to destroy physically each hard disk where data is stored.

Troubleshooting

This chapter contains:

Application Error	96
Login Troubleshooting	97
Authentication Issues	99
LDAP Troubleshooting.....	104
Scanning Problems.....	105
Faxing Problems	107
Networking Problems.....	110

Application Error

To resolve the problem, try one or more of the following:

1. To check the diagnostic log, perform the following:
 - a. Open a web browser, then type `IP/se`, where `IP` is the printer IP address.
 - b. Click **Embedded Solutions**, then do the following:
 1. Clear the log file.
 2. Set the logging level to **Yes**.
 3. Analyze the log, then resolve the problem.



Note: After resolving the problem, set the logging level to **No**.

2. Contact customer support.

Login Troubleshooting

CANNOT DETECT THE CARD READER OR THE SMART CARD

To resolve the problem, try one or more of the following:

- Ensure that the card reader is connected properly to the printer.
- Ensure that the card reader and the smart card are compatible.

For a list of supported card readers, refer to the *Readme* file.

- Ensure that the card reader driver is installed on the printer.
- Contact customer support.

USER IS LOCKED OUT


To resolve the problem, try one or more of the following:

1. Update the allowed number of login failures and lockout time.


 Note: This solution is applicable only to some printer models.

It is possible that the user has reached the maximum allowed number of login failures.

2. From the Embedded Web Server, click **Settings > Security > Login Restrictions**.
3. Update the allowed number of login failures and the lockout time.
4. Click **Save**.

 Note: The new settings take effect after the lockout time expires.

5. Reset or replace the smart card.

 Note: Check whether the type of smart card that you are using can be reset. If the card cannot be reset, then replace the card.

USER IS LOGGED OUT AUTOMATICALLY

To resolve the problem, increase the Screen Timeout value.

1. From the Embedded Web Server, click **Settings > Device > Preferences**.
2. Increase the Screen Timeout value.
3. Click **Save**.

USER CANNOT ACCESS APPLICATIONS OR FUNCTIONS

Ensure that the user is assigned to a group that has access to the applications and functions.

For details, refer to [Managing Login Methods](#).

KDC AND MFP CLOCKS ARE OUT OF SYNC

Ensure that the date and time settings on the printer are correct.

For details, refer to [Setting the Date and Time](#).

DOMAIN CONTROLLER CERTIFICATE IS NOT INSTALLED

Ensure that the correct certificate is installed on the printer.

For details, refer to [Managing Certificates](#).

KDC IS NOT RESPONDING WITHIN THE REQUIRED TIME


To resolve the problem, try one or more of the following:

- Ensure that the IP address or host name of the KDC is correct.
- Ensure that the KDC is available in the configuration file. You can add multiple KDCs in the configuration file.
- Ensure that the server and firewall settings are configured to allow communication between the printer and the KDC server on port 88.


Authentication Issues

KERBEROS AUTHENTICATION FAILED

To resolve the problem, try one or more of the following:

1. To check the diagnostic log, perform the following:
 - a. Open a web browser, then type `IP/se`, where `IP` is the printer IP address.
 - b. Click **Embedded Solutions**, then do the following:
 1. Clear the log file.
 2. Set the logging level to **Yes**.
 3. Generate the log file.
 - c. Analyze the log, then resolve the problem.
-  Note: After resolving the problem, set the logging level to **No**.
2. Ensure that the configuration file is installed on the printer.
 - If you are using simple Kerberos setup to create the Kerberos configuration file, then do the following:
 1. From the Embedded Web Server, to navigate to the configuration page for the application, click **Apps > Smart Card Authentication Client > Configure**.
 2. From the Simple Kerberos Setup section, ensure that the realm, domain controller, domain, and timeout values are correct.
 - If you are using the device Kerberos setup file, then for more information, refer to [Creating a Kerberos Login Method](#).
 3. Ensure that the configuration file content and format are correct.
 - If you are using simple Kerberos setup, then modify the simple Kerberos setup settings.
 - If you are using the device Kerberos setup file, then modify and reinstall the file.
 4. Ensure that the Kerberos realm is in uppercase.
 - If you are using simple Kerberos setup, then do the following:
 1. From the Embedded Web Server, to navigate to the configuration page for the application, click **Apps > Smart Card Authentication Client > Configure**.
 2. From the Simple Kerberos Setup section, ensure that the realm is correct and that it is typed in uppercase.
 3. Click **Apply**.
 - If you are using the device Kerberos setup file, then for more information, refer to [Creating a Kerberos Login Method](#).

5. Specify the Microsoft® Windows® operating system domain.
 - If you are using simple Kerberos setup, then do the following:
 1. From the Embedded Web Server, to navigate to the configuration page for the application, click **Apps > Smart Card Authentication Client > Configure**.
 2. From the Simple Kerberos Setup section, in the Domain field, add the Windows domain in the Domain field.

For example, if the Domain field value is `DomainName, .DomainName`, and the Windows domain is `x.y.z`, then change the Domain field value to `DomainName, .DomainName, x.y.z`.
 -  Note: The domain is case sensitive.
 - 3. Click **Apply**.
 - If you are using the device Kerberos setup file, then add an entry to the `domain_realm` section of the file. Type the Windows domain realm in uppercase, then reinstall the file on the printer.
6. Contact customer support.

CANNOT GENERATE OR READ CERTIFICATE INFORMATION FROM THE SMART CARD

Try one or more of the following:

- Ensure that the certificate information on the smart card is correct.
- Contact customer support.

CANNOT VALIDATE THE DOMAIN CONTROLLER

Try one or more of the following:

1. Ensure that the realm, domain controller, and domain in the Kerberos configuration file are correct.
 - If you are using simple Kerberos setup to create the Kerberos configuration file, then do the following:
 1. From the Embedded Web Server, to navigate to the configuration page for the application, click **Apps > Smart Card Authentication Client > Configure**.
 2. From the Simple Kerberos Setup section, ensure that the realm, domain controller, domain, and timeout values are correct.
 - If you are using the device Kerberos setup file, then for more information, refer to [Creating a Kerberos Login Method](#).

2. Increase the domain controller timeout value.
 - If you are using simple Kerberos setup, then do the following:
 1. From the Embedded Web Server, to navigate to the configuration page for the application, click **Apps > Smart Card Authentication Client > Configure**.
 2. From the Simple Kerberos Setup section, in the Timeout field, enter a value from 3 to 30 seconds.
 3. Click **Apply**.
 - If you are using the device Kerberos setup file, then enter a value from 3 to 30 seconds. When you are finished, reinstall the file on the printer. For more information on configuring the smart card settings, refer to [Configuring the Smart Card Settings](#).
3. Ensure that the domain controller is available.
Use commas to separate multiple values. The domain controllers are validated in the order listed.
4. Ensure that port 88 is not blocked between the printer and the domain controller.


CANNOT VALIDATE THE DOMAIN CONTROLLER CERTIFICATE

Try one or more of the following:

1. Ensure that the certificates that are installed on the printer are correct.
For more information, refer to [Installing Certificates Manually](#).
2. Ensure that the domain controller validation method is configured properly.
 - a. From the Embedded Web Server, to navigate to the configuration page for the application, click **Apps > Smart Card Authentication Client > Configure**.
 - b. From the Smart Card Setup section, in the Domain Controller Validation menu, select the appropriate validation method.
3. Click **Apply**.

CANNOT FIND REALM IN THE KERBEROS CONFIGURATION FILE

To add or change the realm, perform the following:

- If you are using simple Kerberos setup, then do the following:
 1. From the Embedded Web Server, to navigate to the configuration page for the application, click **Apps > Smart Card Authentication Client > Configure**.
 2. From the Simple Kerberos Setup section, in the Realm field, add or change the realm. The realm must be typed in uppercase.
-  Note: The simple Kerberos setup does not support multiple Kerberos realm entries. If multiple realms are needed, then install a Kerberos configuration file containing the necessary realms.
3. Click **Apply**.
- If you are using the device Kerberos setup file, then add or change the realm in the file. The realm must be typed in uppercase. When you are finished, reinstall the file on the printer.

DOMAIN CONTROLLER AND DEVICE CLOCKS ARE OUT OF SYNC

Ensure that the time difference between the printer and the domain controller does not exceed five minutes. For more information, refer to [Setting the Date and Time](#).

CANNOT VALIDATE THE DOMAIN CONTROLLER CERTIFICATE CHAIN

Try one or more of the following:

1. Ensure that the certificates that are installed on the printer are correct.
For more information, refer to [Installing Certificates Manually](#).
2. Ensure that the certificate chain is from the domain controller to the root CA.
3. Ensure that all certificates are not expired.
 - a. From the Embedded Web Server, click **Settings > Security > Certificate Management**.
 - b. Ensure that the Valid From and Valid To dates have not expired.
4. Allow users to log in even if the status of one or more certificates is unknown
 - a. From the Embedded Web Server, to navigate to the configuration page for the application, click **Apps > Smart Card Authentication Client > Configure**.
 - b. From the Online Certificate Status Protocol (OCSP) section, select **Allow Unknown Status**.
 - c. Click **Apply**.
5. Contact customer support.

CANNOT CONNECT TO THE OCSP RESPONDER

Try one or more of the following:

1. Ensure that the OCSP responder URL is correct.
 - a. From the Embedded Web Server, to navigate to the configuration page for the application, click **Apps > Smart Card Authentication Client > Configure**.
 - b. From the Online Certificate Status Protocol (OCSP) section, ensure that the responder URL is correct.
 - c. Click **Apply**.
2. Increase the responder timeout value.
 - a. From the Embedded Web Server, to navigate to the configuration page for the application, click **Apps > Smart Card Authentication Client > Configure**.
 - b. From the Online Certificate Status Protocol (OCSP) section, in the Responder Timeout field, enter a value from 5 to 30.
 - c. Click **Apply**.

CANNOT VALIDATE THE DOMAIN CONTROLLER CERTIFICATE AGAINST THE OCSP RESPONDER

Try one or more of the following:

1. Ensure that the OCSP responder URL and the responder certificate are configured correctly.

- a. From the Embedded Web Server, to navigate to the configuration page for the application, click **Apps > Smart Card Authentication Client > Configure**.
 - b. From the Online Certificate Status Protocol (OCSP) section, in the Responder URL field, specify the following:
 - IP address or host name of the OCSP responder or repeater
 - Port number usedFor example, `http://x:y`, where `x` is the IP address and `y` is the port number.
 - c. In the Responder Certificate field, browse to the appropriate certificate.
 - d. Click **Apply**.
2. Ensure that the domain controller returns the correct certificate.
 3. Ensure that the OCSP responder validates the correct domain controller certificate.

CANNOT ACCESS INDIVIDUAL APPLICATIONS AND FUNCTIONS ON THE PRINTER

Try one or more of the following:

- Allow secure access to applications or functions.
- If the user belongs to an Active Directory group, then ensure that the group is authorized to access the applications and functions.

LDAP Troubleshooting

LDAP LOOKUPS FAIL

To resolve the problem, try one or more of the following:

1. Ensure that the server and firewall settings are configured to allow communication between the printer and the LDAP server on port 389 and port 636.
The default ports are port 389 and port 636.

If reverse DNS lookup is not used in your network, then disable Reverse IP Lookups in the Kerberos settings.
2. To disable Reverse IP Lookups:
 - a. From the Embedded Web Server, click **Settings > Security**.
 - b. In the Network Accounts section, click **Kerberos**.
 - c. In the Miscellaneous Settings section, select **Disable Reverse IP Lookups**.
 - d. Click **Save and Verify**.
3. If the LDAP server requires SSL, then enable SSL for LDAP lookups.
Some solutions that provide authentication require you to enable SSL for LDAP lookups.
4. Narrow the LDAP search base to the lowest possible scope that includes all necessary users.
5. Ensure that all LDAP attributes that are being searched for are correct.

Scanning Problems



Note: This application is supported only in some printer models.

CANNOT SCAN TO THE SELECTED DESTINATION

1. Ensure that the destination is valid.
From the Embedded Web Server, access the configuration page for the application, then confirm the destination network address.
2. If the printer and destination are in different domains, then ensure that the domain information is specified.
From the Embedded Web Server, access the configuration page for the application, and then enter the appropriate domain information.
3. Ensure that the printer is connected to the network.
4. Ensure that the user name and password are correct.
5. Ensure that the user has permission to save scans to the destination.
 - a. From the Embedded Web Server, access the configuration page for the application.
 - b. In the Scan Destination section, select the destination to configure.
 - c. In the Authentication Options section, select the correct authentication type, and if necessary, type the correct authentication credentials.
 - d. Apply the changes.
6. Ensure that a file with the default file name does not exist in the destination.
7. Remove the old file from the destination, or configure the application to do the following:
 - a. Allow users to type a file name.
 - b. Append the time stamp.
 - c. Overwrite the existing file.
8. Configure the firewall to allow communication with the subnet in which the printer is located.
For details, contact your system administrator.
9. Ensure that the printer and destination have the same subnet.
For details, contact your system administrator.
10. Ensure that the LDAP settings are configured properly in your printer setup and in the setup dialog.
For details, contact your system administrator.

LICENSE ERROR

Contact customer support.


AN ERROR OCCURS WHEN OPENING A SECURE PDF FILE

Ensure that the PDF version for the device is not set to A-1a.

Troubleshooting

1. From the Embedded Web Server, do one of the following:
 - Click **Settings > Email > Email Defaults**.
 - Click **Settings > FTP**.
2. In the PDF Settings section, select a PDF Version, except A-1a.
3. Click **Save**.

Faxing Problems

 Note: This application is supported only in some printer models.

CANNOT RECEIVE FAXES FROM ONE SENDER

If you cannot receive faxes from one sender, try one or more of the following:

1. Ensure that the sender used the correct fax number.
2. Check if the fax has no caller ID and station name.
Ensure that the sender is not using a private caller ID and has configured the fax station name.
3. Ensure that the sender fax number is not blocked.
 - a. From the Embedded Web Server, click **Settings > Fax > Fax Setup**.
 - b. In the Fax Receive Settings menu, click **Admin Controls**, then select **Banned Fax List**.
If the fax sender number is listed, then remove the number.
 - c. Click **Save**.
4. Generate fax logs and identify the status message.
From the Embedded Web Server, click **Reports > Fax > Fax Job Log**.

CANNOT RECEIVE FAXES FROM ALL SENDERS

Try one or more of the following:

1. Ensure that the printer is configured to receive faxes.
 - a. From the Embedded Web Server, click **Settings > Fax > Fax Setup**.
 - b. From the Fax Receive Settings menu, click **Admin Controls**, then select **Enable Fax Receive**.
 - c. Click **Save**.
2. If using a distinctive ring service, then confirm that the printer is configured properly to pick up the correct ring pattern.
 - a. From the Embedded Web Server, click **Settings > Fax > Fax Setup**.
 - b. From the Fax Receive Settings menu, click **Admin Controls**, then select the Answer On setting that matches the phone number that is intended for faxes.
 - c. Click **Save**.
3. Reduce the maximum receive speed.
 - a. From the Embedded Web Server, click **Settings > Fax > Fax Setup**.
 - b. From the Fax Receive Settings menu, click **Admin Controls**, then reduce the Max Speed.
 - c. Click **Save**.
4. Check the Fax Forwarding setting.

 Note: This feature is available only in some printer models.

- a. From the Embedded Web Server, click **Settings > Fax > Fax Setup**.

- b. From the Fax Receive Settings menu, click **Admin Controls**, then select any setting for Fax Forwarding, except for Forward.
 - c. Click **Save**.
5. Ensure that no other phone number is competing with the printer.
 - a. From the Embedded Web Server, click **Settings > Fax > Fax Setup**.
 - b. From the Fax Receive Settings menu, change the value for Rings to Answer.
 - c. Click **Save**.
6. Generate fax logs and identify the status message.
From the Embedded Web Server, click **Reports > Fax > Fax Job Log**.

CANNOT SEND FAXES TO ONE DESTINATION

Try one or more of the following:

1. Ensure that you entered the correct fax number.
2. Reduce the maximum send speed.
 - a. From the Embedded Web Server, click **Settings > Fax > Fax Setup**.
 - b. From the Fax Send Settings menu, click **Admin Controls > Max Speed**, then select a lower setting.
 - c. Click **Submit**.
3. Generate fax logs and identify the status message.
From the Embedded Web Server, click **Reports > Fax > Fax Job Log**.

CANNOT SEND TO ALL FAX DESTINATIONS

Try one or more of the following:

1. Ensure that the printer is not configured for Fax Server mode.
 - a. From the Embedded Web Server, click **Settings > Fax**.
 - b. Ensure that **Fax** is selected in Fax Mode.
2. Ensure that the printer is configured to send faxes.
 - a. From the Embedded Web Server, click **Settings > Fax > Fax Setup**.
 - b. From the Fax Send Settings menu, click **Admin Controls**, then select **Enable Fax Scans**.
 - c. Click **Save**.
3. Check if you are using a Private Automated Branch Exchange (PABX) telephone system.
PABX is a telephone network that allows a single access number to offer multiple lines to outside callers. PABX also provides a range of external lines to internal callers or personnel.

If you are using a PABX, then do the following:

- a. From the Embedded Web Server, click **Settings > Fax > Fax Setup**.
- b. From the Fax Send Settings menu, select **Behind a PABX**.
- c. Click **Save**.

4. Check if you have entered the proper dialing prefix.
 - a. From the Embedded Web Server, click **Settings > Fax > Fax Setup**.
 - b. From the Fax Send Settings menu, click **Admin Controls**, and then check the value entered in the Dial Prefix field.
 - c. If necessary, add the dialing prefix that you want to use, and then click **Save**.
5. Reduce the maximum send speed.
 - a. From the Embedded Web Server, click **Settings > Fax > Fax Setup**.
 - b. From the Fax Send Settings menu, click **Admin Controls > Max Speed**, and then select a lower setting.
 - c. Click **Save**.
6. Ensure that you have entered a station ID and station number.
 - a. From the Embedded Web Server, click **Settings > Fax > Fax Setup**.
 - b. From the Fax Send Settings menu, make sure that the Fax Name and Fax Number fields are not blank.
 - c. Click **Save**.
7. Generate fax logs and identify the status message.

From the Embedded Web Server, click **Reports > Fax > Fax Job Log**.

Networking Problems

PRINTER IS NOT COMMUNICATING ON THE NETWORK

Try one or more of the following:

1. Check the network status.
 - a. From the Embedded Web Server, click **Reports > Network > Network Setup Page**.
 - b. In the Ethernet and/or Wireless section, check the Card Status.
 - c. If the printer is disconnected, for a wired connection, ensure that the Ethernet cable is properly connected.
 - d. If the printer is disconnected, for a wireless connection, check the printer wireless connection.
For details, refer to [Connecting to a Wireless Network](#).
2. Check the printer port access.
 - a. From the Embedded Web Server, click **Settings > Network/Ports > TCP/IP > TCP/IP Port Access**.
 - b. If necessary, enable ports.
For details, refer to [Configuring TCP/IP Port Access Settings](#).
 - c. Click **Save**.
3. Check the Restricted Server List.
 - a. From the Embedded Web Server, click **Settings > Network/Ports > TCP/IP**.
 - b. Locate the Restricted Server List, then check for the printer IP address.
 - c. If the printer IP address is listed, then remove it.
 - d. Click **Save**.
4. Ensure that communication is not blocked by a firewall or workplace VPN.

Configuring Smart Card Authentication

This appendix contains:

- Configuring the Login Screen Settings..... 112
- Configuring the Manual Login Settings 113
- Configuring the Smart Card Settings 114
- Configuring Advanced Settings..... 116

Administrator rights are required to configure the application.

Configuring the Login Screen Settings

Use the login screen settings to set how you want users to log in to the printer.


1. From the Embedded Web Server, to navigate to the configuration page for the application, click **Apps > Smart Card Authentication Client > Configure**.
2. From the Login Screen section, select the login type.
3. In the User Validation Mode menu, select the method for validating user certificates.
 - **Active Directory:** The user certificate on the smart card is validated using Kerberos authentication. This setting may require LDAP lookups.
 - **Active Directory with guest access:** Users who have smart cards but are not in the Active Directory can access some of the printer functions. A properly configured Online Certificate Status Protocol (OCSP) server is required. If the Active Directory authentication fails, then the application queries the OCSP server.
 - **Pin-Only:** Users can access only the applications or functions that do not require Kerberos authentication.
4. In the Validate Smart Card menu, select the method for authenticating users after tapping a smart card.
5. If required, allow users to change the login method.
6. Click **Apply**.

Configuring the Manual Login Settings

For manual login, the printer uses the default domain specified in the Kerberos configuration file. If you use a different domain, then specify the domain name in the manual login settings.

1. From the Embedded Web Server, to navigate to the configuration page for the application, click **Apps > Smart Card Authentication Client > Configure**.
2. From the Manual Login Setup section, in the Manual Login Domains field, type one or more domains.
3. Click **Apply**.

Configuring the Smart Card Settings

 Note: Ensure that the network connection between the printer and the authenticating server is configured properly. For more information, contact system administrator.

1. From the Embedded Web Server, to navigate to the configuration page for the application, click **Apps > Smart Card Authentication Client > Configure**.

2. From the Smart Card Setup section, in the Kerberos Information menu, select one of the following:

- **Use device Kerberos setup file:** A Kerberos configuration file must be installed on the printer manually.

Perform the following:

1. From the Embedded Web Server, click **Settings > Security > Login Methods**.
2. From the Network Accounts section, click **Add Login Method > Kerberos**.
3. From the Import Kerberos File section, browse to the appropriate `krb5.conf` file.
4. If your network does not use reverse DNS lookup, then from the Miscellaneous Settings section, select **Disable Reverse IP Lookups**.
5. Click **Save** and **Verify**.


- **Use simple Kerberos setup:** A Kerberos file is created on the printer automatically. Specify the following:

- **Realm:** The realm must be typed in uppercase.
- **Domain Controller:** Use commas to separate multiple values. The domain controllers are validated in the order listed.
- **Domain:** The domain that must be mapped to the Kerberos realm specified in the Realm field. Use commas to separate multiple domains.

 Note: The domain is case sensitive.

- **Timeout:** Enter a value from 3 to 30 seconds.

3. In the Domain Controller Validation menu, select the method for validating the domain controller certificate.

 Note: Before configuring this setting, ensure that the appropriate certificates are installed on the printer. For more information, refer to [Installing Certificates Manually](#).

- **Use device certificate validation:** The CA certificate that is installed on the printer is used.
- **Use device chain validation:** The entire certificate chain that is installed on the printer is used.
- **Use OCSP validation:** The OCSP server is used. Ensure that the entire certificate chain is installed on the printer. From the Online Certificate Status Protocol (OCSP) section, configure the following:

- **Responder URL:** The IP address or host name of the OCSP responder or repeater, and the port number used. Use commas to separate multiple values.

For example, `http://x:y`, where `x` is the IP address or host name, and `y` is the port number.

- **Responder Certificate:** The X.509 certificate is used.
- **Responder Timeout:** Enter a value from 5 to 30 seconds.
- **Allow Unknown Status:** Users can log in even if the status of one or more certificates is unknown.

4. Click **Apply**.

Configuring Advanced Settings

1. From the Embedded Web Server, to navigate to the configuration page for the application, click **Apps > Smart Card Authentication Client > Configure**.
2. From the Advanced Settings section, select a session user ID.



Note: Some applications, such as Secure Held Print Jobs and Secure Email, require a value for the session user ID.

3. In the Email From Address menu, select where the printer retrieves the user email address.
4. If required, select **Wait for user information** to retrieve all user information before the user is allowed to access the home screen or secure application.
If the following settings are set to LDAP Lookup, then select this option.

- Session User ID
- Email From Address

If the following settings are not empty, then select this option.

- Other User Attributes
- Group Authorization List



Note: If you are using manual login for Secure Email, then select this option to store the user email address in the login session. To allow manual login users to send email to themselves, enable **Send me a copy** in the printer email settings.

5. If required, select **Use SSL for User Info** to retrieve user information from the domain controller using an SSL connection.
6. If required, in the Other User Attributes field, type other LDAP attributes that must be added to the session. Use commas to separate multiple values.
7. In the Group Authorization List, type the Active Directory groups that can access applications or functions. Use commas to separate multiple values.



Note: The groups must be in the LDAP server.

8. If DNS is not enabled in your network, then upload a hosts file.
Type the mappings in the text file in the format of `x.y`, where `x` is the IP address and `y` is the host name. You can assign multiple host names to an IP address. For example, `255.255.255.255 HostName1
HostName2 HostName3`.

You cannot assign multiple IP addresses to a host name. To assign IP addresses to groups of host names, type each IP address and its associated host names on a separate line of the text file.

For example:

```
123.123.123.123 HostName1 HostName2
```

```
456.456.456.456 HostName3
```

9. Click **Apply**.

