Embedded Web Server

Administrator's Guide

January 2023

www.lexmark.com

Contents

Change history..... 4

Overview..... 6

Supported printer models..... 6
Supported web browsers..... 9
Accessing the Embedded Web Server..... 9
Parts of the Embedded Web Server..... 10
Understanding helper text..... 11

Managing printers..... 12

Checking the status of parts and supplies from the Embedded Web Server..... 12
Generating reports and logs..... 12
Configuring supply notifications..... 13
Customizing the home screen..... 13
Managing contacts..... 15

Scanning..... 16

Configuring the scan settings..... 16
Creating a shortcut..... 25
Managing Scan Center destinations..... 25

Faxing..... 28

Configuring the fax settings..... 28

Networking..... 34

Configuring the HTTP/FTP Settings..... 34
Selecting the active network adapter..... 34
Connecting to a wireless network..... 35

Securing printers..... 36

Securing network connections..... 36
Managing devices remotely..... 38
Managing login methods..... 41
Managing certificates..... 52
Managing other access functions..... 54

Securing data....57

Troubleshooting....62

Login troubleshooting....62
LDAP troubleshooting....63
Scanning problems....64
Faxing problems....65
Networking problems....68

Notices....69

Index....74

Change history

January 2023

- Added information on the following:
  - Supported printer models
  - Scan, fax, network, and security settings
  - Managing printers

May 2022

- Added information on home screen customization.

April 2020

- Added information on the following:
  - Supported printer models
  - Scan, fax, network, and security settings
  - Managing printers

February 2019

- Added information on the following:
  - Supported printer models
  - Scan, fax, and network settings
  - Creating a shortcut
- Added instructions on configuring printer settings.

October 2018

- Added information on the following:
  - Supported printer models
  - Scan, fax, and network settings

April 2018

- Added information on supported printer models and web browsers.

August 2017

- Added information on supported printer models.

June 2017

- Added information on supported printer models.

February 2017

- Added information on supported printer models.

January 2017

- Updated information on the Common Criteria certified target of evaluation.

July 2016

- Added information on the following:
  - New and updated access controls
  - New LDAP attribute settings

January 2016

- Initial document release for multifunction products with a tablet-like touch-screen display.

Overview

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 they can use.

Using the Embedded Web Server, you can configure the Lexmark printer to conform to the Common Criteria certified target of evaluation. For more information, see the *Lexmark Common Criteria Installation Supplement and Administrator Guide*.

Before you begin, make sure that the printer settings have been configured for e-mail. For more information, see the printer *User's Guide*.

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 let you log in to a printer manually or using a smart card, and then securely send e-mails and release print jobs. You can also configure more security settings in an application, such as e-mail signing and encryption.
  - **Card Authentication**—Secure access to a printer using a card reader. When users badge in, their credentials are authenticated using a master printer, LDAP, Lexmark Document Distributor (LDD), or identity service providers (ISP).

  Note: For more information, see the *Administrator's Guide* for the solution.
- The group where the users belong to. You can create groups after creating the login methods.
- The applications, functions, and printer management settings that users can access.

You may need administrative rights to configure or troubleshoot the security settings.

Supported printer models

Multifunction products

- Lexmark CX331
- Lexmark CX421
- Lexmark CX431
- Lexmark CX522
- Lexmark CX531
- Lexmark CX622
- Lexmark CX625

- Lexmark CX635
- Lexmark CX725
- Lexmark CX727
- Lexmark CX820
- Lexmark CX825
- Lexmark CX827
- Lexmark CX860
- Lexmark CX920
- Lexmark CX921
- Lexmark CX922
- Lexmark CX923
- Lexmark CX924
- Lexmark MB2236
- Lexmark MB2338
- Lexmark MB2442
- Lexmark MB2546
- Lexmark MB2650
- Lexmark MB2770
- Lexmark MB3442
- Lexmark MC2325
- Lexmark MC2425
- Lexmark MC2640
- Lexmark MC3224
- Lexmark MC3326
- Lexmark MC3426
- Lexmark MX321
- Lexmark MX331
- Lexmark MX421
- Lexmark MX431
- Lexmark MX521
- Lexmark MX522
- Lexmark MX532
- Lexmark MX622
- Lexmark MX632
- Lexmark MX721
- Lexmark MX722
- Lexmark MX725
- Lexmark MX822
- Lexmark MX826
- Lexmark XC2235
- Lexmark XC2240

- Lexmark XC2335
- Lexmark XC4140
- Lexmark XC4150
- Lexmark XC4240
- Lexmark XC6152
- Lexmark XC8155
- Lexmark XC8160
- Lexmark XM3350
- Lexmark XM5365
- Lexmark XM5370
- Lexmark XM7355
- Lexmark XM7370

Printers

- Lexmark B2236
- Lexmark B2338
- Lexmark B2442
- Lexmark B2546
- Lexmark B2650
- Lexmark B2865
- Lexmark B3340
- Lexmark B3442
- Lexmark C2240
- Lexmark C2325
- Lexmark C2335
- Lexmark C2425
- Lexmark C2535
- Lexmark C3224
- Lexmark C3326
- Lexmark C4150
- Lexmark C6160
- Lexmark CS331
- Lexmark CS421
- Lexmark CS431
- Lexmark CS521
- Lexmark CS531
- Lexmark CS622
- Lexmark CS632
- Lexmark CS639
- Lexmark CS720
- Lexmark CS725

- Lexmark CS727
- Lexmark CS728
- Lexmark CS820
- Lexmark CS827
- Lexmark CS921
- Lexmark CS923
- Lexmark CS927
- Lexmark M3350
- Lexmark M5255
- Lexmark M5270
- Lexmark M5275
- Lexmark MS321
- Lexmark MS331
- Lexmark MS421
- Lexmark MS431
- Lexmark MS521
- Lexmark MS621
- Lexmark MS631
- Lexmark MS622
- Lexmark MS632
- Lexmark MS725
- Lexmark MS821
- Lexmark MS822
- Lexmark MS823
- Lexmark MS825
- Lexmark MS826

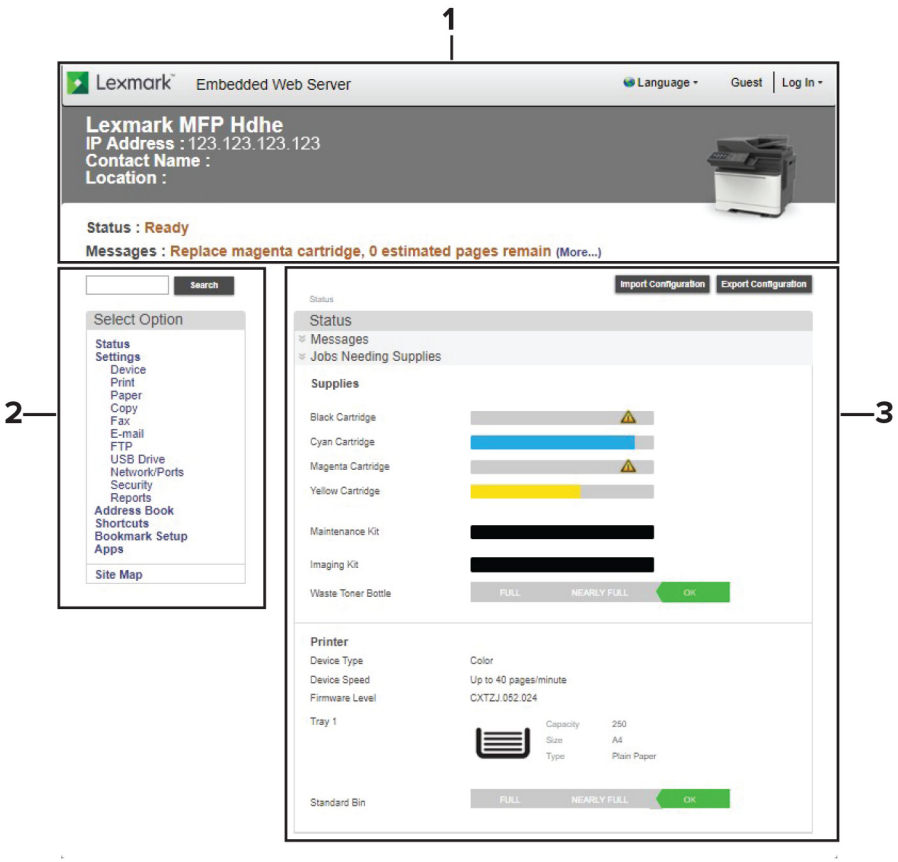
Supported web browsers

- 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 either of the following:
   - Locate the IP address on the printer home screen.
   - View the IP address in the Network Overview section or in the TCP/IP section of the Network/Ports menu.
2. Open a web browser, and then type the printer IP address.

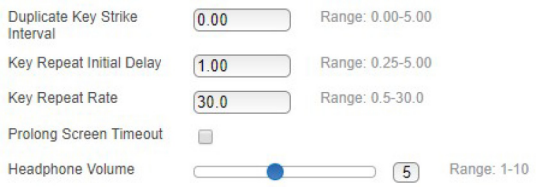
Parts of the Embedded Web Server



	Section	Description
1	Top	• Shows the printer information and current status. • Allows the user to change the language of the web page. **Note:** Changing the language of the web page does not affect the language on the printer display.
2	Left	• 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	• 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, see “Generating reports and logs” on page 12.

Understanding helper text

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



Managing printers

Checking the status of parts and supplies from the Embedded Web Server

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

1. Obtain the printer IP address. Do either of the following:
   - Locate the IP address on the printer home screen.
   - View the IP address in the Network Overview section or in the TCP/IP section of the Network/Ports menu.
2. Open a web browser, and then type the printer IP address.
3. You can view the status of the parts and supplies in the Supplies section.

Generating reports and logs

1. From the Embedded Web Server, click **Reports**.
2. Select the report or log.
   - **Menu Settings Page**—Show the current printer preferences, settings, and configurations.
   - **Device**
     - **Device Information**—Show information about the printer.
     - **Device Statistics**—Show printer usage and supply status.
     - **Profiles List**—Show a list of profiles that are stored on the printer.
   - **Print**
     - **Print Directory**—Show 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**—Show a list of all the shortcuts that are stored on the printer.
     - **Fax Shortcuts**—Show a list of all fax shortcuts that are stored on the printer.
     - **Copy Shortcuts**—Show a list of all copy shortcuts that are stored on the printer.
     - **E-mail Shortcuts**—Show a list of all e-mail shortcuts that are stored on the printer.
     - **FTP Shortcuts**—Show a list of all FTP shortcuts that are stored on the printer.
     - **Network Folder Shortcuts**—Show a list of all network folder shortcuts that are stored on the printer.
   - **Fax**
     - **Fax Job Log**—List the last 200 completed fax jobs.

       Note: This report is available only when Enable Job Log is enabled.
     - **Fax Call Log**—List 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**—Show 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**—Show 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 supply notifications

1. From the Embedded Web Server, click **Settings** > **Device** > **Notifications**.
2. From the Supplies menu, click **Custom Supply Notifications**.
3. Select a notification for each supply item.
4. Apply the changes.

Customizing the home screen

This feature lets users customize the applications in their printer display. Users can add, remove, or rearrange 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, and then do the following:
   a. Click **Edit**.
   b. In the App Label field, type the name of the application.

      Notes:

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

Notes:

- 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

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

Notes:

- 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

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

Notes:

- 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

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

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

   The files are exported in ZIP format.

Importing home screen settings

1. From the Embedded Web Server, click **Import Configuration**.
2. Select the folder, and 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. From the Embedded Web Server, click **Address Book**.
2. From the Contacts section, click **Add Contact**.

   Note: You can assign the contact to one or more groups.
3. If necessary, specify a login method to allow application access.
4. Click **Save**.

Adding groups

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

1. From the Embedded Web Server, click **Address Book**.
2. From the Contact Groups section, add a group name.

   Note: You can assign one or more contacts to the group.
3. Click **Save**.

Editing contacts or groups

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

1. From the Embedded Web Server, click **Address Book**.
2. Do either of the following:
   - From the Contacts section, click a contact name, and then edit the information.
   - From the Contact Groups section, click a group name, and then edit the information.
3. Click **Save**.

Deleting contacts or groups

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

1. From the Embedded Web Server, click **Address Book**.
2. Do either of the following:
   - From the Contacts section, select a contact that you want to delete.
   - From the Contact Groups section, select a group name that you want to delete.

Scanning

Configuring the scan settings

Configuring the copy settings

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

2 Configure the settings.

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

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**—Place a border around each image when printing multiple pages on a single page.
- **Collate**—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.
- **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.

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.
- **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.

    Notes:

    - 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.

Admin Controls

- **Allow Color Copies**—Print copies in color.
- **Allow Priority Copies**—Interrupt a print job to copy a page or document.
- **Custom Job Scanning**—Turn on scanning of custom jobs by default.
- **Allow Save as Shortcut**—Save custom copy settings as shortcuts.
- **Adjust ADF Skew**—Adjust the front-side and back-side skew angles.

  Note: Adjust ADF Skew is disabled if Express Mode (Express Scanning or Express Printing) is on and if electronic deskew is not supported on the device.
- **Sample Copy**—Print a sample copy.

3 Click **Save**.

Customize Settings List

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

1 Do either 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 e-mail settings

1 From the Embedded Web Server, click **Settings** > **E-mail**.

2 Configure the settings.

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

E-mail Setup

- **Primary SMTP Gateway**—Type the IP address or host name of the primary SMTP server for sending e-mail.
- **Primary SMTP Gateway Port**—Enter 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**—Enter 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 in the e-mail.
- **Always use SMTP default Reply Address**—Always use the default reply address in the SMTP server.
- **Use SSL/TLS**—Specify whether to send e-mail 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 E-mail**—Specify whether credentials are required for device-initiated e-mail.
- **User-Initiated E-mail**—Specify whether credentials are required for user-initiated e-mail.
- **Use Active Directory Device Credentials**—Enable 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 SMPT server not set up error message.
- **SMPT Connection Log**—Select to view the SMPT connection log details.
- **Test Connection**—Configure the settings for test connection.
  - **Recipient E-mail Address**—Type the e-mail address of the recipient.
  - **Send Test E-mail to Recipient**—Send test e-mail to the recipient e-mail address.
  - **Test**—Select to send the test e-mail.

    Note: This option is enabled after entering a valid address in the **Recipient E-mail Address** field.

Note: When SMTP Server is not configured, the settings under the **Setup E-mail Lists and Alerts** section are disabled.

E-mail Defaults

- **Subject**—Specify the e-mail subject.
- **Message**—Specify the e-mail message.
- **File Name**—Specify the file name for the scanned image.
- **Format**—Specify the file format for the scanned image.
- **Global OCR Settings**—Configure the settings for optical character recognition (OCR).
- **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.
  - **Highly Compressed**—Specify whether to compress the scanned image.

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

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.
  - **E-mail 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.

Admin Controls

- **Max E-mail Size**—Set the allowable file size for each e-mail.
- **Size Error Message**—Specify an error message that the printer sends when an e-mail exceeds its allowable file size.
- **Limit Destinations**—Limit sending of e-mail only to the specified list of domain names.

- **Send Me a Copy**—Send a copy of the e-mail to yourself.
- **Allow self e-mails only**—Enable the logged-in user's e-mail address to be the only recipient when sending e-mails.
- **Use cc:/bcc:**—Enable carbon copy and blind carbon copy in e-mail.
- **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 (Express Scanning or Express Printing) is on and if electronic deskew is not supported on the device.
- **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 e-mail transmission.
- **Log Paper Source**—Specify the paper source for printing logs.
- **Custom Job Scanning**—Turn on scanning of custom jobs by default.
- **Scan Preview**—Show the scan preview on the display.
- **Allow Save as Shortcut**—Save e-mail addresses as shortcuts.
- **E-mail Images Sent As**—Specify how to send the images in e-mail.
- **Reset E-mail Information After Sending**—Restore the default e-mail information after sending an e-mail.

Web Link Setup

- **Server**—Set the e-mail server to use for the web link.
- **Login**—Set the user name to use for the web link.
- **Password**—Set the password to use for the web link.
- **Path**—Set the printer network path to use for the web link.
- **File Name**—Set the file name to use for the web link.
- **Web Link**—Set the web link.

3 Click **Save**.

Customize Settings List

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

1 Do either 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

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

2 Configure the settings.

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

FTP Defaults

- **Format**—Specify the file format for the scanned image.
- **Global OCR Settings**—Configure the settings for optical character recognition (OCR).
- **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.
  - **Highly Compressed**—Specify whether to compress the scanned image.
  - **Secure**—Specify whether to enable security for the scanned image.
  - **Searchable**—Specify whether to enable searchability for the scanned image.
  - **Archival (PDF/A)**—Specify whether to enable archival for the scanned image.
- **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.

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 of detecting blank pages.

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.
- **Custom Job Scanning**—Turn on scanning of custom jobs by default.
- **Scan Preview**—Show the scan preview on the display.
- **Adjust ADF Skew**—Adjust the front-side and back-side skew angles.

  Note: Adjust ADF Skew is disabled if Express Mode (Express Scanning or Express Printing) is on and if electronic deskew is not supported on the device.
- **Allow Save as Shortcut**—Save custom FTP settings as shortcuts.
- **Use Passive FTP** —Select to specify the data port that the printer connects to.

3 Click **Save**.

Customize Settings List

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

1 Do either 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

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

2 Configure the settings.

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

Flash Drive Scan

- **Format**—Specify the file format for the scanned image.
- **Global OCR Settings**—Configure the settings for optical character recognition (OCR).
- **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.
  - **Highly Compressed**—Specify whether to compress the scanned image.
  - **Secure**—Specify whether to enable security for the scanned image.
  - **Searchable**—Specify whether to enable searchability for the scanned image.
  - **Archival (PDF/A)**—Specify whether to enable archival for the scanned image.
- **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.

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.

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.
- **Custom Job Scanning**—Turn on scanning of custom jobs by default.
- **Scan Preview**—Show the scan preview on the display.
- **Adjust ADF Skew**—Adjust the front-side and back-side skew angles.

  Note: Adjust ADF Skew is disabled if Express Mode (Express Scanning or Express Printing) is on and if electronic deskew is not supported on the device.

Customize Scan Settings List

This feature lets you customize the settings on the screen.

- Do either 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.

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 which side of the paper (long edge or short edge) 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**—Print a border around each page 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.

3 Click **Save**.

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

Customize Print Settings List

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

1. Do either 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: You may need administrative rights to create a shortcut.

1. From the Embedded Web Server, click **Shortcuts** > **Add Shortcut**.
2. Select a shortcut type, and then configure the settings.
3. Click **Save**.

Managing Scan Center destinations

You may need administrative rights to configure the application.

Configuring a network destination

1. From the Embedded Web Server, navigate to the configuration page for the application:

   Apps > **Scan Center** > **Configure**

   Note: This application is supported only in some printers.
2. Click **Network Folder** > **Create Network Folder**.
3. Select the connection type, and then do either 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**.

Notes:

- 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 it from the list.
- To delete a destination, click  beside it.

- You can also prevent users from creating or editing destinations using the printer control panel.

Configuring an e-mail destination

1. From the Embedded Web Server, navigate to the configuration page for the application:

   Apps > **Scan Center** > **Configure**

   Note: This application is supported only in some printer models.
2. Click **E-mail** > **Create E-mail**.
3. Configure the settings.
4. Click **Save**.

Notes:

- To edit a destination, select it from the list.
- To delete a destination, click beside it.
- You can also prevent users from creating or editing destinations using the printer control panel.

Configuring a fax destination

1. From the Embedded Web Server, navigate to the configuration page for the application:

   Apps > **Scan Center** > **Configure**

   Note: This application is supported only in some printer models.
2. Click **Fax** > **Create Fax**.
3. Configure the settings.
4. Click **Save**.

Notes:

- To edit a destination, select it from the list.
- To delete a destination, click beside it.
- You can also prevent users from creating or editing destinations using the printer control panel.

Configuring a remote printer destination

Scan documents on a supported printer and then send the scanned documents to another printer on the network.

1. From the Embedded Web Server, navigate to the configuration page for the application:

   Apps > **Scan Center** > **Configure**

   Note: This application is supported only in some printer models.
2. Click **Remote Printer** > **Create Remote Printer**.

3 Configure the settings.

4 Click **Save**.

Notes:

- To edit a destination, select it from the list.
- To delete a destination, click beside it.
- You can also prevent users from creating or editing destinations using the printer control panel.

Faxing

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.
- **Disabled**

3 Click **Save**.

Configuring analog fax

General Fax Settings

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

2 Configure the settings.

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

- **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

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

2 Configure the settings.

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

- **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.

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.

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 fax successfully.
- **Enable ECM**—Activate Error Correction Mode (ECM) for fax jobs.
- **Enable Fax Scans**—Fax documents that are scanned at the printer.
- **Driver to Fax**—Allow the print driver to send fax.
- **Allow Save as Shortcut**—Save fax numbers as shortcuts in the printer.
- **Max Speed**—Set the maximum speed for sending fax.
- **Custom Job Scanning**—Turn on scanning of custom jobs by default.
- **Scan Preview**—Show a preview of the scan on the display.

- **Adjust ADF Skew**—Adjust the front-side and back-side skew angles.

  Note: Adjust ADF Skew is disabled if Express Mode (i.e., Express Scanning and/or Express Printing) is On and if electronic deskew is not supported on the device.
- **Enable Color Fax Scans**—Enable color scans for fax.
- **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.

3 Click **Save**.

Fax Receive Settings

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

2 Configure the settings.

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

- **Fax Job Waiting**—Remove fax jobs that request specific unavailable resources from the print queue.
- **Rings to Answer**—Set the number of rings for incoming fax.
- **Auto Reduction**—Scale incoming fax to fit on the page.
- **Paper Source**—Set the paper source for printing 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.

Holding Faxes

- **Held Fax Mode**—Hold received faxes from printing until they are released.

Admin Controls

- **Enable Fax Receive**—Set the printer to receive fax.
- **Enable Color Fax Receive**—Set the printer to receive fax 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 fax.
- **Manual Answer Code**—Set the answer code for incoming manual fax.

  Note: Manual Answer Code is tied up to Manual Fax support.
- **Auto Answer**—Set the printer to receive fax automatically.
- **Fax Forwarding**—Specify how to forward received fax.
- **Forward to**—Specify where to forward received fax.

- **Confirmation E-mail**—Send a confirmation e-mail when fax forwarding is successful.
- **Max Speed**—Set the maximum speed for transmitting fax.

3 Click **Save**.

Fax Cover Page

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

2 Configure the settings.

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

- **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

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

2 Configure the settings.

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

- **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 e-mail a log for successful fax transmission or transmission error.
- **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

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 fax.
   - **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 E-mail Settings

1. From the Embedded Web Server, click **Settings** > **Fax** > **Fax Server Setup** > **Fax Server E-mail Settings**.
2. Configure the settings.

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

   - **Primary SMTP Gateway**—Type the IP address or host name of the primary SMTP server for sending e-mail.
   - **Primary SMTP Gateway Port**—Enter 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**—Enter 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 fax.
   - **Always use SMTP default Reply Address**—Specify the SMTP reply address for sending fax.
   - **Use SSL/TLS**—Specify whether to send 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 E-mail**—Specify whether credentials are required for device-initiated e-mail.
   - **User-Initiated E-mail**—Specify whether credentials are required for user-initiated e-mail.

- **Use Active Directory Device Credentials**—Enable 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 “SMPT server not set up” error message.
- **Test Connection**—Configure the settings for test connection.
  - **Recipient E-mail Address**—Type the e-mail address of the recipient.
  - **Send Test E-mail to Recipient**—Send a test e-mail to the recipient e-mail address.
  - **Test**—Select to send the test e-mail.

    Note: This option is enabled after you enter a valid address in the Recipient E-mail 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

Configuring the HTTP/FTP Settings

Note: These settings are available only in network printers or printers connected 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**—Access the Embedded Web Server to monitor and manage the printer.
- **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, make sure that:

- Your printer is connected temporarily to an Ethernet network.
- A wireless network adapter is installed in your printer and working properly. For more information, see 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 access point (wireless router).

Note: Make sure to enter the correct Network Name.

3 Click **Save**.

4 Disconnect the Ethernet cable, and then wait for at least one minute.

5 Check if your printer is connected to the network. Print a network setup page, and then in the Wireless section, see if the Card Status is “Connected.”

For more information, see the “Networking” section of the printer *User’s Guide*.

Securing printers

Note: For information on the latest security advisories for Lexmark products, go to http://support.lexmark.com/alerts.

Securing network connections

Configuring TCP/IP port access settings

You can control your network device activities by configuring your device to filter out traffic on specific network connections. Protocols (such as FTP, HTTP, and Telnet) can be disabled.

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

We recommend closing any ports that you do not plan to use under standard operation by clearing them.

1. From the Embedded Web Server, click **Settings** > **Network/Ports** > **TCP/IP** > **TCP/IP Port Access**.
2. Enable the 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 preshared keys (PSKs) and certificates. You can use both options simultaneously.

When using 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 pass phrase that is used to authenticate the systems and to encrypt the data.

When using 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 and pass phrases.

1. From the Embedded Web Server, click **Settings** > **Network/Ports** > **IPSec**.
2. Select **Enable IPSec**.
3. Configure the following settings to specify the encryption and authentication methods of the printer:
   - Base Configuration
   - DH (Diffie-Hellman) Group Proposal
   - 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

4 Do one or more of the following:
- From the Pre-Shared Key Authenticated Connections section, type the IP address of the client printer that you want to connect to the printer.
- From the Certificate Authenticated Connections section, type the IP address of the client printer that you want to connect to the printer.

5 Click **Save**.

Notes:

- 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.

Notes:

- If 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 more information, see “Managing certificates” on page 52.
- Make sure 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 From 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 the digital certificate that you want to use.

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

3 From the Allowable Authentication Mechanisms section, select one or more authentication protocols.
- EAP-MD5, EAP-MSCHAPv2, LEAP, and PEAP require a login name and password.
- EAP-TLS requires a login name, CA certificate, and signed printer certificate.
- EAP-TTLS requires a login name and password and CA certificate.

4 In the TTLS Authentication Method menu, select the authentication method to use.

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, protecting the printer against unauthorized printing and configuring.

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**.

Managing devices remotely

Using HTTPS for printer management

To restrict the access of the printer Embedded Web Server to HTTPS only, turn off the HTTP port, leaving 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 SNMP versions 1 or 2c settings

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

2 From the SNMP Versions 1 and 2c section, select **Enabled** > **Allow SNMP Set**.

3 In the SNMP Community field, type a name for the SNMP Community identifier. The default community name is **`public`**.

4 Select **Enable PPM MIB** (Printer Port Monitor MIB) to facilitate the automatic installation of printer drivers and other printing applications.

5 Click **Save**.

Configuring SNMP version 3 settings

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

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

2 From the SNMP Version 3 section, select **Enabled**.

3 If necessary, configure the following by providing your authentication credentials:
   - **Set Read/Write Credentials**—Allow remote installation and configuration changes and printer monitoring.
   - **Set Read-only Credentials**—Allow only printer monitoring.
4 In the Authentication Hash menu, select the hash function of your SNMP server.
5 In the Minimum Authentication Level, select **Authentication, Privacy**.
6 In the Privacy Algorithm menu, select the strongest setting 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 that you want to generate an alert.
4 Click **Save**.

Configuring security audit log settings

The security audit log lets you 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 may also be transmitted to a network system log (syslog) server for processing or storage.

We recommend enabling audit in secure environments.

1 From the Embedded Web Server, click **Settings** > **Security** > **Security Audit Log**.
2 Do one or more of the following:

Activate security audit logging

Select **Enable Audit**.

Configure transmission to a network syslog server

This option lets you use both the remote syslog server and the internal logging.

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**—Select **Normal UDP** to send log messages and events using a lower-priority transmission protocol. 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 to aid 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, and the lowest is 7. The selected severity level and anything 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 regardless of severity to the remote server.

Configure e-mail notification

Before you begin, make sure that the printer settings have been configured for e-mail.

a In the Admin's E-mail Address field, type one or more e-mail addresses, separated by commas.

b Configure the notification settings.

- **E-mail Log Cleared Alert**—Send a notification when the Delete Log button is clicked.
- **E-mail 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 e-mail the log and then delete all entries.
- **E-mail % Full Alert**—Send a notification when log storage space reaches a certain percentage of capacity.
- **% Full Alert Level**—Specify how full the log must be before an alert is triggered.
- **E-mail Log Exported Alert**—Send a notification when the log file is exported.
- **E-mail 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.

3 Click **Save**.

Managing security audit logs

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

Updating firmware

Printers inspect all downloaded firmware packages for required attributes before adopting and executing 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 Lexmark. However, the strongest security measure comes from requiring all firmware packages to include multiple digital 2048-bit RSA signatures from Lexmark. 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.

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

2 Do either of the following:

- Browse to the firmware file, and then click **Upload**.
- Click **Check for updates now** > **I agree, start update**.

Managing login methods

Restricting the access of guest account users

The guest account can use the printer without logging in. Control the guest account users from accessing the printer functions and applications, as well as managing the printer and its security options.

1. From the Embedded Web Server, click **Settings** > **Security** > **Login Methods**.
2. From the Public section, click **Manage Permissions**.
3. Select the access controls that the guest account can access. For more information, see "Understanding access controls" on page 50.
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. From the Local Accounts section, click **Add User**.
3. Select the type of authentication method that you want the account to use when logging 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 more information, see "Creating local account groups" on page 42.
6. Click **Save**.

Editing and deleting local accounts

1. From the Embedded Web Server, click **Settings** > **Security** > **Login Methods**.
2. From the Local Accounts section, click the authentication method where the user account belongs to.
3. Click the user account that you want to edit or delete.
4. Do either of the following:
   - To edit the user account, update the user information, and then click **Save**.
   - To delete the user account, click **Delete User**.

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

Creating local account groups

Use groups to customize users' access to applications and printer functions.

1. From the Embedded Web Server, click **Settings** > **Security** > **Login Methods**.
2. Do either of the following:

   Add a group when managing permissions

   a. From the Local Accounts section, click **Manage Groups/Permissions**.

   b. Click **Add Group**.

   Add a group when creating or editing a user account

   a. Create or edit a user account.

   b. From the Permission Groups section, select **Add New Group**.
3. Type a unique group name.
4. From the Access Controls section, select the functions, menus, and applications that the group can access.
5. Click **Save**.

Notes:

- To import access controls from another group, click **Import Access Controls**, and then select a group.
- For more information on access controls, see "Understanding access controls" on page 50.

Editing or deleting local account groups

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

Notes:

- To import access controls from another group, click **Import Access Controls**, and then select a group.
- To delete multiple groups, select the groups, and then click **Delete**.
- For more information on access controls, see "Understanding access controls" on page 50.

Using LDAP or LDAP+GSSAPI

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

LDAP+GSSAPI is used when you want your transmission to be always secure. 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 running Active Directory.

Notes:

- LDAP+GSSAPI requires a Kerberos network account. For more information, see "Creating a Kerberos login method" on page 45.
- Supported printers can store a maximum of eight unique LDAP or LDAP+GSSAPI login methods. Each method must have a unique name.
- Administrators can create up to 32 user-defined groups that apply to each unique login method.
- LDAP and LDAP+GSSAPI relies on an external server for authentication. If the server is down, then users are not able to 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. From the Network Accounts section, click **Add Login Method** > **LDAP**.
3. Select the authentication type.
   - LDAP
   - LDAP+GSSAPI
4. Configure the settings.

   General Information

   - **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**—Enter the port where 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 used when logging 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 only Windows operating system authentication credentials.

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

   Device Credentials

   - **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 in the LDAP +GSSAPI setup.
  - **Device Password**—Type the password for the user.

Advanced Options

- **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 users' 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 more information, contact your system administrator.
- **Mail Attribute**—Type the LDAP attribute that contains the users' e-mail addresses. The default value is **`mail`**.
- **Fax number Attribute**—Type the LDAP attribute that contains the users' fax number. The default value is **`facsimiletelephonenumber`**.
- **Full Name Attribute**—Type the LDAP attribute that contains the users' full names. The default value is **`cn`**.
- **Home Directory Attribute**—Type the LDAP attribute that contains the users' home directory. The default value is **`homeDirectory`**.
- **Group Membership Attribute**—Type the LDAP attribute required for group search. The default value is **`memberOf`**.
- **Search Base**—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.

Search Specific Object Classes

- **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.

Address Book Setup

The following settings are used to configure the address book used when scanning to an e-mail 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.

5 Click **Save and Verify**.

Editing or deleting LDAP or LDAP+GSSAPI login methods

1 From the Embedded Web Server, click **Settings** > **Security** > **Login Methods**.

2 From the Network Accounts section, click the LDAP or LDAP+GSSAPI login method.

3 Do either of the following:

- To edit the login method, update the LDAP or LDAP+GSSAPI settings, and then click **Save and Verify**.
- To delete the login method, click **Delete LDAP**.

Using Kerberos

You can use this login method by itself or in conjunction with the LDAP+GSSAPI login method.

Notes:

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

Creating a Kerberos login method

1 From the Embedded Web Server, click **Settings** > **Security** > **Login Methods**.

2 From the Network Accounts section, click **Add Login Method** > **Kerberos**.

3 Do one of the following:

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. The realm must be typed in uppercase.

Import a Kerberos configuration file

In the Import Kerberos File field, browse to the krb5.conf file.

4 If necessary, from the Miscellaneous Settings section, configure the following settings:
   - **Character Encoding**—Select the character encoding used for the configuration file.
   - **Disable Reverse IP Lookups**

5 Click **Save and Verify**.

Setting the date and time

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

1 From the Embedded Web Server, click **Settings** > **Device** > **Preferences** > **Date and Time**.

Configuring manually

Note: Configuring the date and time manually 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: If you select **(UTC+user) Custom**, then specify the offset values for UTC (GMT) and DST.

Configuring NTP

a From the Network Time Protocol section, select **Enable NTP**, and 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 enter the key ID and password, or browse to the file containing the NTP authentication credentials.

2 Click **Save**.

Using Active Directory

You can use this login method by itself or in conjunction with the LDAP+GSSAPI login method.

Notes:

- Only one Kerberos configuration file can be saved in the printer memory. This configuration file can apply to multiple realms and Kerberos Domain Controllers.
- You must anticipate the different types of authentication requests the Kerberos server may receive, and 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 are not able to access the printer using Active Directory.
- To help prevent unauthorized access, log out from the printer after each session.

Creating an Active Directory login method

1. From the Embedded Web Server, click **Settings** > **Security** > **Login Methods**.
2. From 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 the user belongs to.
4. Click **Join Domain**.

Editing or deleting an Active Directory login method

1. From the Embedded Web Server, click **Settings** > **Security** > **Login Methods**.
2. From the Network Accounts section, click the Active Directory login method.
3. Do either of the following:
   - To delete the login method, click **Unjoin Domain**.
   - Configure the following settings, and then click **Save and Verify**.

     General Information
     - **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.

Device Credentials

- **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.

Advanced Options

- **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 users' 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 users' e-mail addresses. The default value is **`mail`**.
- **Fax number Attribute**—Type the LDAP attribute that contains the users' fax number. The default value is **`facsimiletelephonenumber`**.
- **Full Name Attribute**—Type the LDAP attribute that contains the users' full names. The default value is **`cn`**.
- **Home Directory Attribute**—Type the LDAP attribute that contains the users' home directory. The default value is **`homeDirectory`**.
- **Group Membership Attribute**—Type the LDAP attribute required for group search. The default value is **`memberOf`**.
- **Search Base**—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.

Search Specific Object Classes

- **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.

Address Book Setup

The following settings are used to configure the address book used when scanning to an e-mail 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.

Creating LDAP, LDAP+GSSAPI, Kerberos, or Active Directory groups

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

1. From the Embedded Web Server, click **Settings** > **Security** > **Login Methods**.
2. From the Network Account section, click **LDAP**, **LDAP+GSSAPI**, **Kerberos**, or **Active Directory** as the login method.
3. Click **Manage Groups** > **Add Group**.
4. Do either of the following:

   Search for the group name or user name

   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 user name.
   c. Click **Search**.
   d. Select the group that you want to add.
   e. Click **Add Selected**.

   Add a group manually

   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**.
5. Select the group, and then from the Access Controls section, select the functions, menus, and applications that the group can access.
6. Click **Save**.

Notes:

- To import access controls from another group, click **Import Access Controls**, and then select a group.
- For more information on access controls, see “Understanding access controls” on page 50.

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, and then click **Manage Groups**.
3. Click the group, and then do either of the following:
   - Configure the access controls, and then click **Save**.
   - Click **Delete Group**.

Notes:

- To import access controls from another group, click **Import Access Controls**, and then select a group.
- To delete multiple groups, select the groups, and then click **Delete**.
- For more information on access controls, see “Understanding access controls” on page 50.

Understanding access controls

Access controls let you limit users’ 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 users’ access to available printer functions:

- **Access Address Book in Apps**—Use Address Book from eSF applications that support it.
- **Manage Shortcuts**—Access the Manage Shortcuts menu, and enable the “Save as Shortcut” option available in the Copy, E-mail, Fax, and FTP functions.
- **Modify Address Book**—Enable the Search Address Book option available in the E-mail, Fax, and FTP functions when accessed from the printer home screen.
- **Create Profiles**—Create profiles for printing, copying, scanning, e-mailing, or faxing.
- **Manage Bookmarks**
- **Flash Drive Print**—Print from a flash drive.
- **Flash Drive Color Printing**—Print in color from a flash drive.
- **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 to 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 if it is enabled.
- **E-mail Function**—Use the e-mail function.
- **Fax Function**—Use the fax function. If this function is disabled, then:
  - All analog fax functions and the fax server are disabled.
  - The fax icon is removed.
  - 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, do the following:
  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.
- **Internal 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 users' 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 users' 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.
- **Cloud Services Enrollment**—Control access to the enrollment of the Lexmark cloud services.

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. From 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 issuing the certificate.
   - **Unit Name**—Type the name of the unit within the company or organization issuing the certificate.
   - **Country/Region**—Type the country or region where the company or organization issuing the certificate is located.
   - **Province Name**—Type the name of the province or state where the company or organization issuing the certificate is located.
   - **City Name**—Type the name of the city where the company or organization issuing 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. From the Device Certificates section, click **Generate**.
3. Configure the settings. For more information, see "Configuring printer certificate defaults" on page 52.
4. Click **Generate** or **Generate and Download**.

Installing certificates manually

Note: To download the CA certificate automatically, see "Installing certificates automatically" on page 53.

Before configuring 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 must be in a separate PEM (.cer) file.

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

   Sample certificate:

   ```
   -----BEGIN CERTIFICATE-----
   MIIE1jCCA76gAwIBAgIQY6sV0KL3tIhBtlr4gHG85zANBgkqhkiG9w0BAQUFADBs
   …
   l3DTbPe0mnIbTq0iWqKEaVne1vvaDt52iSpEQyevwgUcHD16rFy+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, then click **Join Domain**, and 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, then select **Fetch Immediately**.
4. Click **Save**.

Viewing, downloading, and deleting a certificate

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

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

Managing other access functions

Scheduling access to USB devices

In secure environments, devices can be configured 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, and then specify when the device performs the action.
3. Click **Save**.

Notes:

- For each Disable schedule entry, create an Enable schedule entry to reactivate use of the USB host ports.
- You can create multiple schedules.

Setting login restrictions

To prevent malicious access to a device, restrict the number of invalid login attempts and require a lockout time before letting users retry logging in.

Many organizations establish login restrictions for information assets such as workstations and servers. Make sure 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 may be logged in remotely before being logged out automatically.
3. Click **Save**.

Configuring confidential printing

Users printing confidential or sensitive information may use the confidential print option. This option lets print jobs 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.

     Notes:

     - 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, enter **0**.
   - **Confidential Job Expiration**—Set the expiration time for confidential print jobs.

     Notes:

     - 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 turned 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 that the printer prints a copy before printing the remaining copies.

     Note: Verify jobs print one copy to check if it is satisfactory before printing the remaining copies.
   - **Reserve Job Expiration**—Set the expiration time that the printer stores print jobs.

     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: You need to restart the device for the changes to take effect.
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. In 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) or not depends on the user's permission configuration. For more information, see "Managing login methods" on page 41.

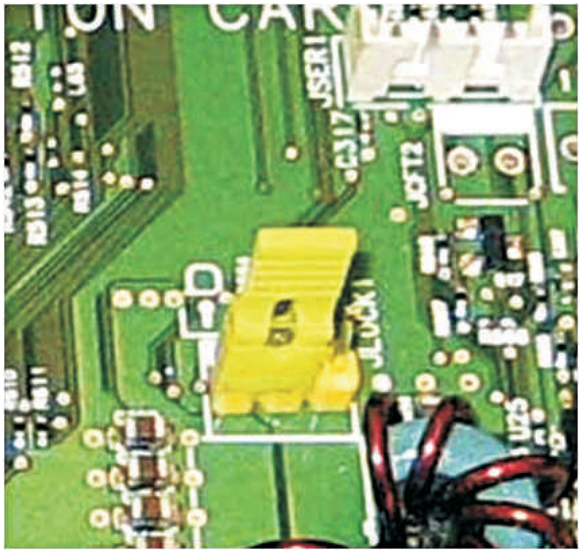
1. From the Embedded Web Server, click **Settings** > **Security** > **Miscellaneous**.
2. Select **Print Permission**.
3. Click **Save**.

Enabling the security reset jumper

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

Using a cable lock to secure access to the controller board ensures that the device is not maliciously reset.

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



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

1. From the Embedded Web Server, click **Settings** > **Security** > **Miscellaneous**.
2. In the Security Reset Jumper menu, select either 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 necessary, enter a value in the **Minimum Password Length** field.
4. To enable the password or to reveal the PIN, click **Enable Password/PIN Reveal**.
5. Click **Save**.

Securing data

Configuring printer settings

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 settings.

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

   ### USB Configuration

   - **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.

   ### Tray Configuration

   - **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**—Specify if the tray has multiple universal sizes.

Reports

Print reports about printer menu settings, status, and event logs.

- **Menu Settings Page**
- **Event Log**
- **Event Log Summary**

Supply Usage and Counters

- **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.

Fax Configuration

- **Fax Low Power Support**—Specify the printer power setting when it is in fax mode.

Print Configuration

- **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.

Device Operations

- **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.

Scanner Configuration

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

    Note: Make sure that the margin spacing on the target page is uniform all the way around the target. If it is not, then the printer margins may need to be reset.
  - **Front ADF Registration**—Manually register the ADF after replacing the ADF, scanner glass, or controller board.
  - **Rear ADF Registration**—Manually register the Rear after replacing the ADF, scanner glass, or controller board.
  - **Flatbed Registration**—Manually register the scanner glass after replacing the ADF, scanner glass, or controller board.

- **Edge Erase**—Set the size, in millimeters, of the no-print area around a scan job.
  - **ADF Edge Erase**
  - **Flatbed Edge Erase**
- **ADF Deskew**—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**—Disable the scanner if it is not working properly.
- **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 before a user is prompted to clean the scanner glass.

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

4 Click **Save**.

Erasing printer memory

To erase volatile memory or buffered data in your printer, turn 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**.

2 From the Erase Printer Memory section, select **Sanitize all information on nonvolatile memory**.

3 If necessary, from the After erasing all nonvolatile memory section, select either **Start initial setup wizard** or **Leave printer offline** after erasing the printer memory.

4 Click **Start**.

Erasing printer storage drive

1 From the Embedded Web Server, click **Settings** > **Device** > **Maintenance**.

2 Depending on the storage drive that is installed on your printer, do either of the following:
- Select **Sanitize all information on nonvolatile memory**, and then select either of the following:
  - **Start initial setup wizard**
  - **Leave printer offline**

  Note: The process to sanitize the hard disk can take from several minutes to more than an hour, making the printer unavailable for other tasks.
- For intelligent storage drive (ISD), select **Cryptographically erase all user data on ISD**.

3 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, on selecting Sanitize all information on nonvolatile memory, the above three settings get selected automatically.

4 Click **Start**.

Note: Click **Reset** to change the configuration.

Configuring the intelligent storage drive

1 From the Embedded Web Server, click **Settings** > **Security** > **Miscellaneous**.

2 Select **Use Intelligent Storage Drive for User Data** to save the user data.

3 Click **Save**.

Restoring factory default settings

1 From the Embedded Web Server, click **Settings** > **Device** > **Restore Factory Defaults**.

2 Select the settings that you want to restore.

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

- 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

Type of memory	Description
Volatile memory	The printer uses standard random access memory (RAM) to buffer temporarily user data during simple print and copy jobs.
Nonvolatile memory	The printer may use two forms of non-volatile memory: EEPROM and NAND (flash memory). Both types store the operating system, printer settings, and network information. They also store scanner and bookmark settings and embedded solutions.
Hard disk storage drive	Some printers may 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.
Intelligent storage drive (ISD)	Some printers may have an ISD installed. ISD uses non-volatile flash memory to store 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 decommissioned.
- The printer hard disk or ISD is replaced.
- The printer is moved to a different department or location.
- The printer is serviced by someone from outside your organization.
- The printer is removed from your premises for service.
- The printer is sold to another organization.

Note: To dispose a storage drive, follow the policies and procedures of your organization.

Troubleshooting

Login troubleshooting

User is locked out

Try one or more of the following:

Update the allowed number of login failures and lockout time

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

The user may have reached the allowed number of login failures.

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

   Note: Wait for the lockout time to pass before the new settings take effect.

Reset or replace the smart card

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

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

Make sure that the user is assigned to a group that has access to the applications and functions

For more information, see “Managing login methods” on page 41.

KDC and MFP clocks are out of sync

Make sure that the date and time settings on the printer are correct

For more information, see “Setting the date and time” on page 46.

Domain controller certificate is not installed

Make sure that the correct certificate is installed on the printer

For more information, see “Managing certificates” on page 52.

KDC is not responding within the required time

Try one or more of the following:

Make sure that the IP address or host name of the KDC is correct

Make sure that the KDC is available in the configuration file

You can add multiple KDCs in the configuration file.

Make sure that the server and firewall settings are configured to allow communication between the printer and the KDC server on port 88

LDAP troubleshooting

LDAP lookups fail

Try one or more of the following:

Make sure 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 it in the Kerberos settings

1. From the Embedded Web Server, click **Settings** > **Security**.
2. From the Network Accounts section, click **Kerberos**.
3. From the Miscellaneous Settings section, select **Disable Reverse IP Lookups**.
4. Click **Save and Verify**.

If the LDAP server requires SSL, then enable SSL for LDAP lookups

Some solutions that provide authentication may require you to enable SSL for LDAP lookups. For more information, see the administrator’s guide for the solution.

Narrow the LDAP search base to the lowest possible scope that includes all necessary users

Make sure that all LDAP attributes that are being searched for are correct

Scanning problems

Cannot scan to the selected destination

Make sure that the destination is valid

From the Embedded Web Server, access the configuration page for the application, and then confirm the destination network address.

If the printer and destination are in different domains, then make sure 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.

Make sure that the printer is connected to the network

Make sure that the user name and password are correct

Make sure that the user has permission to save scans to the destination

1. From the Embedded Web Server, access the configuration page for the application.
2. From the Scan Destination section, select the destination to configure.
3. From the Authentication Options section, select the correct authentication type, and if necessary, type the correct authentication credentials.
4. Apply the changes.

Make sure that a file with the default file name does not exist in the destination

Remove the old file from the destination, or configure the application to:

- Allow users to type a file name.
- Append the time stamp.
- Overwrite the existing file.

Configure the firewall to allow communication with the subnet in which the printer is located

For more information, contact your system administrator.

Make sure that the printer and destination have the same subnet

For more information, contact your system administrator.

Make sure that the LDAP settings are configured properly in your printer setup and in the setup dialog

For more information, contact your system administrator.

Contact your system administrator

License error

Contact your Lexmark representative

An error occurs when opening a secure PDF file

Make sure that the PDF version for the device is not set to A-1a

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

Faxing problems

Cannot receive fax from one sender

Try one or more of the following:

Make sure that the sender used the correct fax number

Check if the fax has no caller ID and station name

Make sure that the sender is not using a private caller ID and has configured the fax station name.

Check if the sender fax number is not blocked

1. From the Embedded Web Server, click **Settings** > **Fax** > **Fax Setup**.
2. From the Fax Receive Settings menu, click **Admin Controls**, and then select **Banned Fax List**. If the fax sender number is listed, then remove the number.
3. Click **Save**.

Generate fax logs and identify the status message

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

Cannot receive fax from all senders

Try one or more of the following:

Make sure that the printer is configured to receive faxes

1. From the Embedded Web Server, click **Settings** > **Fax** > **Fax Setup**.
2. From the Fax Receive Settings menu, click **Admin Controls**, and then select **Enable Fax Receive**.

3 Click **Save**.

If using a distinctive ring service, then confirm that the printer is configured properly to pick up the correct ring pattern

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

2 From the Fax Receive Settings menu, click **Admin Controls**, and then select the Answer On setting that matches the phone number intended for faxes.

3 Click **Save**.

Reduce the Max Receive speed

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

2 From the Fax Receive Settings menu, click **Admin Controls**, and then reduce the Max Speed.

3 Click **Save**.

Check the fax forwarding setting

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

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

2 From the Fax Receive Settings menu, click **Admin Controls**, and then select any setting for Fax Forwarding except **Forward**.

3 Click **Save**.

Make sure that no other phone number is competing with the printer

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

2 From the Fax Receive Settings menu, change the “Rings to Answer” value.

3 Click **Save**.

Generate fax logs and identify the status message

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

Cannot send fax to one destination

Try one or more of the following:

Make sure that you entered the correct fax number

Reduce the maximum send speed

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

2 From the Fax Send Settings menu, click **Admin Controls** > **Max Speed**, and then select a lower setting.

3 Click **Submit**.

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:

Make sure that the printer is not configured for Fax Server mode

1. From the Embedded Web Server, click **Settings** > **Fax**.
2. Make sure that **Fax** is selected in Fax Mode.

Make sure that the printer is configured to send faxes

1. From the Embedded Web Server, click **Settings** > **Fax** > **Fax Setup**.
2. From the Fax Send Settings menu, click **Admin Controls**, and then select **Enable Fax Scans**.
3. Click **Save**.

Check if you are using a PABX telephone system

Private Automated Branch Exchange (PABX) is a telephone network that allows a single access number to offer multiple lines to outside callers. It also provides a range of external lines to internal callers or personnel. If you are using a PABX, then do the following:

1. From the Embedded Web Server, click **Settings** > **Fax** > **Fax Setup**.
2. From the Fax Send Settings menu, select **Behind a PABX**.
3. Click **Save**.

Check if you have entered the proper dialing prefix

1. From the Embedded Web Server, click **Settings** > **Fax** > **Fax Setup**.
2. From the Fax Send Settings menu, click **Admin Controls**, and then check the value entered in the Dial Prefix field.
3. If necessary, add the dialing prefix that you want to use, and then click **Save**.

Reduce the Max Send speed

1. From the Embedded Web Server, click **Settings** > **Fax** > **Fax Setup**.
2. From the Fax Send Settings menu, click **Admin Controls** > **Max Speed**, and then select a lower setting.
3. Click **Save**.

Make sure that you have entered a station ID and station number

1. From the Embedded Web Server, click **Settings** > **Fax** > **Fax Setup**.
2. From the General Fax Settings menu, make sure that the Fax Name and Fax Number fields are not blank.

3 Click **Save**.

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:

Check the network status

1 From the Embedded Web Server, click **Reports** > **Network** > **Network Setup Page**.

2 From the Standard Network Card section, check the Card Status.

3 If the printer is disconnected, then do one of the following:

- For wired connection, make sure that the Ethernet cable is properly connected.
- For wireless connection, check the printer wireless connection. For more information, see "Connecting to a wireless network" on page 35.

Check the printer port access

1 From the Embedded Web Server, click **Settings** > **Network/Ports** > **TCP/IP** > **TCP/IP Port Access**.

2 If necessary, enable ports. For more information, see "Configuring TCP/IP port access settings" on page 36.

3 Click **Save**.

Check the Restricted Server List

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

2 Locate the Restricted Server List, and then check for the printer IP address.

3 If the printer IP address is listed, then remove it.

4 Click **Save**.

Make sure that communication is not blocked by a firewall or workplace VPN

Notices

Edition notice

January 2023

The following paragraph does not apply to any country where such provisions are inconsistent with local law: LEXMARK INTERNATIONAL, INC., PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions; therefore, this statement may not apply to you.

This publication could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in later editions. Improvements or changes in the products or the programs described may be made at any time.

References in this publication to products, programs, or services do not imply that the manufacturer intends to make these available in all countries in which it operates. Any reference to a product, program, or service is not intended to state or imply that only that product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any existing intellectual property right may be used instead. Evaluation and verification of operation in conjunction with other products, programs, or services, except those expressly designated by the manufacturer, are the user’s responsibility.

For Lexmark technical support, go to **http://support.lexmark.com**.

For information on Lexmark's privacy policy governing the use of this product, go to **www.lexmark.com/privacy**.

For information on supplies and downloads, go to **www.lexmark.com**.

© **2016 Lexmark International, Inc.**

All rights reserved.

GOVERNMENT END USERS

The Software Program and any related documentation are "Commercial Items," as that term is defined in 48 C.F.R. 2.101, "Computer Software" and "Commercial Computer Software Documentation," as such terms are used in 48 C.F.R. 12.212 or 48 C.F.R. 227.7202, as applicable. Consistent with 48 C.F.R. 12.212 or 48 C.F.R. 227.7202-1 through 227.7207-4, as applicable, the Commercial Computer Software and Commercial Software Documentation are licensed to the U.S. Government end users (a) only as Commercial Items and (b) with only those rights as are granted to all other end users pursuant to the terms and conditions herein.

Trademarks

Lexmark and the Lexmark logo are trademarks or registered trademarks of Lexmark International, Inc. in the United States and/or other countries.

Google Chrome is a trademark of Google LLC.

Microsoft, Internet Explorer, Microsoft Edge, and Windows are trademarks of the Microsoft group of companies.

Safari is a trademark of Apple Inc.

Wi-Fi Direct is a registered trademark of Wi-Fi Alliance®.

All other trademarks are the property of their respective owners.

GifEncoder

GifEncoder - writes out an image as a GIF. Transparency handling and variable bit size courtesy of Jack Palevich. Copyright (C) 1996 by Jef Poskanzer * <jef@acme.com>. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. Visit the ACME Labs Java page for up-to-date versions of this and other fine Java utilities: http://www.acme.com/java/

ZXing 1.7

This project consists of contributions from several people, recognized here for convenience, in alphabetical order.

Agustín Delgado (Servinform S.A.), Aitor Almeida (University of Deusto), Alasdair Mackintosh (Google), Alexander Martin (Haase & Martin GmbH), Andreas Pillath, Andrew Walbran (Google), Andrey Sitnik, Androida.hu / http://www.androida.hu/, Antonio Manuel Benjumea (Servinform S.A.), Brian Brown (Google), Chang Hyun Park, Christian Brunschen (Google), crowdin.net, Daniel Switkin (Google), Dave MacLachlan (Google), David Phillip Oster (Google), David Albert (Bug Labs), David Olivier, Diego Pierotto, drejc83, Eduardo Castillejo (University of Deusto), Emanuele Aina, Eric Kobrin (Velocitude), Erik Barbara, Fred Lin (Anobiit), gcstang, Hannes Erven, hypest (Barcorama project), Isaac Potoczny-Jones, Jeff Breidenbach (Google), John Connolly (Bug Labs), Jonas Petersson (Prisjakt), Joseph Wain (Google), Juho Mikkonen, jwicks, Kevin O'Sullivan (SITA), Kevin Xue (NetDragon Websoft Inc., China), Lachezar Dobrev, Luiz Silva, Luka Finžgar, Marcelo, Mateusz Jędrasik, Matrix44, Matthew Schulkind (Google), Matt York (LifeMarks), Mohamad Fairol, Morgan Courbet, Nikolaos Ftylitakis, Pablo Orduña (University of Deusto), Paul Hackenberger, Ralf Kistner, Randy Shen (Acer), Rasmus Schrøder Sørensen, Richard Hřivňák, Romain Pechayre, Roman Nurik (Google), Ryan Alford, Sanford Squires, Sean Owen (Google), Shiyuan Guo / 郭世元, Simon Flannery (Ericsson), Steven Parkes, Suraj Supekar, Sven Klinkhamer, Thomas Gerbet, Vince Francis (LifeMarks), Wolfgang Jung, Yakov Okshtein (Google)

Apache License Version 2.0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1 Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2 Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3 Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:
   a. (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and
   b. (b) You must cause any modified files to carry prominent notices stating that You changed the files; and
   c. (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and
   d. (d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

   You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.
5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.
6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.
7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.
8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.
9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

Index

Numerics

802.1x authentication 37

A

access controls 50
accessing the Embedded Web Server 9
Active Directory
  creating groups 49
  creating login method 47
  deleting groups 49
  deleting login method 47
  editing groups 49
  editing login method 47
active network adapter
  selecting 34
adding contacts 15
adding groups 15

C

cannot scan to selected destination 64
card is locked out 62
certificate
  deleting 53
  downloading 53
  viewing 53
certificate error 63
certificates
  installing 53
  installing manually 53
change history 4
checking the status of parts and supplies 12
confidential printing
  configuring 55
configuring
  TCP/IP port access settings 36
configuring copy settings 16
configuring e-mail settings 17
configuring fax cover page 31
configuring fax log settings 31
configuring fax receive settings 30
configuring fax send settings 29
configuring fax server e-mail settings 32
configuring fax server scan settings 33
configuring flash drive settings 22
configuring FTP settings 21
configuring general fax settings 28, 32
configuring HTTP/FTP settings 34
configuring intelligent storage drive 60
configuring IP Security settings 36
configuring printer certificate defaults 52
configuring security audit log settings 39
configuring SNMP traps 39
configuring SNMP version 1 settings 38
configuring SNMP version 2c settings 38
configuring SNMP version 3 settings 38
configuring speaker settings 32
configuring supply notifications 13
connecting to a wireless network 35
contacts
  adding 15
  deleting 15
  editing 15
controlling access 50
copy settings
  configuring 16
creating a printer certificate 53
creating a shortcut 25
creating an Active Directory login method 47
creating groups
  local accounts 42
creating Kerberos login method 45
creating LDAP login method 43
creating LDAP+GSSAPI login method 43
creating local accounts
  password 41
  PIN 41
  user name 41
  user name and password 41
customizing
  home screen 13
customizing home screen 13

D

date and time settings
  configuring manually 46
  configuring NTP 46
deleting a certificate 53
deleting Active Directory groups 49
deleting an Active Directory login method 47
deleting contacts 15
deleting groups 15
deleting LDAP groups 49
deleting LDAP login method 45
deleting LDAP+GSSAPI groups 49
deleting LDAP+GSSAPI login method 45
deleting local account groups 42
deleting local accounts
  password 41
  PIN 41
  user name 41
  user name and password 41
digital certificates
  installing 53
  installing manually 53
domain certificate error 63
domain controller certificate not installed 63
downloading a certificate 53

E

editing Active Directory groups 49
editing an Active Directory login method 47
editing contacts 15
editing groups 15
editing LDAP groups 49

editing LDAP+GSSAPI groups 49
editing local account groups 42
editing local accounts
password 41
PIN 41
user name 41
user name and password 41
Embedded Web Server
accessing 9
checking the status of parts 12
checking the status of supplies 12
parts 10
enabling print permission 56
enabling solutions LDAP settings 55
erasing printer memory 59, 60
erasing printer storage drive 59
error occurs when opening a secure PDF 65
e-mail destination
adding 26
configuring from the Embedded Web Server 26
deleting 26
editing 26
e-mail settings
configuring 17

F

failure to receive fax from all senders 65
failure to receive fax from one sender 65
failure to send fax to one destination 66
failure to send to all fax destinations 67
fax cover page
configuring 31
fax destination
adding 26
configuring from the Embedded Web Server 26
deleting 26
editing 26
fax log settings
configuring 31
fax mode
setting 28
fax receive settings
configuring 30
fax send settings
configuring 29
fax server e-mail settings
configuring 32
fax server scan settings
configuring 33
firmware
updating 40
flash drive settings
configuring 22
FTP settings
configuring 21

G

general fax settings
configuring 28, 32
generating reports and logs 12
groups
adding 15
deleting 15
editing 15
GSSAPI
understanding 42
guest account users
restricting access 41

H

hard disk
erasing 59
hard disk storage drive 60
helper text 11
HTTP/FTP settings
configuring 34
HTTPS
printer management 38

I

installing certificates automatically 53
installing certificates manually 53
intelligent storage drive 60
configuring 60
erasing 59
IP Security
configuring settings 36
IPsec 36

K

KDC and MFP clocks out of sync 62
KDC is not responding within the required time 63
Kerberos
creating login method 45

L

LDAP 42
creating groups 49
creating login method 43
deleting groups 49
deleting login method 45
editing groups 49
LDAP and GSSAPI 42
LDAP lookups fail 63
LDAP+GSSAPI
creating groups 49
creating login method 43
deleting groups 49
deleting login method 45
editing groups 49
license error 65
local accounts
creating groups 42
creating password 41
creating PIN 41
creating user name 41
creating user name and password 41
deleting groups 42
deleting password 41
deleting PIN 41
deleting user name 41
deleting user name and password 41
editing groups 42
editing password 41
editing PIN 41
editing user name and password 41
login method
creating Active Directory 47
creating LDAP 43
creating LDAP+GSAAPI 43
deleting Active Directory 47
deleting LDAP 45
deleting LDAP+GSSAPI 45
editing Active Directory 47
login restrictions
setting 54
logs
generating 12

M

managing security audit log settings 39
MFP clock out of sync 62
multifunction products 6

N

network destination
adding 25
configuring from the Embedded Web Server 25
deleting 25
editing 25
Network Time Protocol
configuring 46
nonvolatile memory
erasing 59
non-volatile memory 60

O

overview 6

P

parts
checking status 12
checking, using the Embedded Web Server 12
parts of the Embedded Web Server 10
print permission
enabling 56
printer certificate
configuring defaults 52
creating 53
printer clock out of sync 62
printer management
using HTTPS 38
printer not communicating on the network 68
printer settings
configuring 57
maintaining 57
restoring to factory defaults 60
printers 6
protected features
showing on the home screen 56

R

remote printer destination
adding 26
configuring from the Embedded Web Server 26
deleting 26
editing 26
reports
generating 12
reset jumper 56
restoring factory default settings 60
restricted server list
setting 38
restricting
guest account users access 41
restricting guest account users 41

S

scheduling access to USB devices 54
secured applications or functions
showing on the home screen 56
securing printer data 60
security
802.1x authentication 37
confidential printing 55
reset jumper on controller board 56
security advisory 36
security audit logs
configuring 39
deleting 39
e-mail notification 39
managing 39
viewing or saving 39
security certificates
installing 53
installing manually 53
security reset jumper
enabling 56
selecting the active network adapter 34
servers
restricting 38
setting fax mode 28
setting login restrictions 54
setting the restricted server list 38
shortcuts
creating 25
SNMP traps
configuring 39
SNMP version 1 settings
configuring 38
SNMP version 2c settings
configuring 38
SNMP version 3 settings
configuring 38
solutions LDAP settings
enabling 55
speaker settings
configuring 32
statement of volatility 60
storage drive
erasing 59
supplies
checking status 12
checking, using the Embedded Web Server 12
supply notifications
configuring 13
supported printers 6
supported web browsers 9

T

TCP/IP port access
configuring 36
troubleshooting
cannot scan to selected destination 64
certificate error 63
domain certificate error 63
domain controller certificate not installed 63
error occurs when opening a secure PDF 65
failure to receive fax from all senders 65
failure to receive fax from one sender 65
failure to send fax to one destination 66
failure to send to all fax destinations 67
KDC and MFP clocks out of sync 62
KDC is not responding within the required time 63
LDAP lookups fail 63
license error 65

MFP clock out of sync 62
printer clock out of sync 62
printer not communicating on the network 68
unexpected logout 62
user cannot access applications or functions 62
user is locked out 62
user is logged out automatically 62

U

unexpected logout 62
updating firmware 40
USB devices
scheduling access 54
USB ports
disabling 54
enabling 54
user cannot access applications or functions 62
user is locked out 62
user is logged out automatically 62

V

viewing a certificate 53
volatile memory 60
erasing 59

W

web browsers
supported 9
wireless network
connecting 35