JUNE 2026

Xerox® Embedded Web Server

Administrator's Guide

xerox™

Copyright and trademarks

BR42683

Contents

Change history

This chapter contains

1. Change history

Change history

June 2026

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

Overview

This chapter contains

2. Overview

Overview

This guide explains how to manage and configure printer, scan, fax, network, and security settings using the Embedded Web Server (EWS).

Use the EWS to:

- Monitor printer status and supplies
- Configure scan, fax, and network settings
- Manage users, access controls, and security features
- Configure the printer to meet Common Criteria certification requirements

Before configuring settings:

- Make sure the printer email settings are configured. For more information, see the printer *User's Guide*.
- Identify the login method to use:
  - Local accounts
  - LDAP
  - LDAP+GSSAPI
  - Kerberos
  - Active Directory
- Identify any additional security solutions, such as Smart Card Authentication or Card Authentication.
- Determine user groups and the applications, functions, and printer management settings that users can access.

  Note: Some settings may be available only in certain printer models.

Supported printer models

Multifunction printers

- Xerox® C245
- Xerox® C255a
- Xerox® C303a
- Xerox® C305ae
- Xerox® XC2432
- Xerox® ZC364

Printers

- Xerox® C240
- Xerox® C300
- Xerox® C2432

Supported web browsers

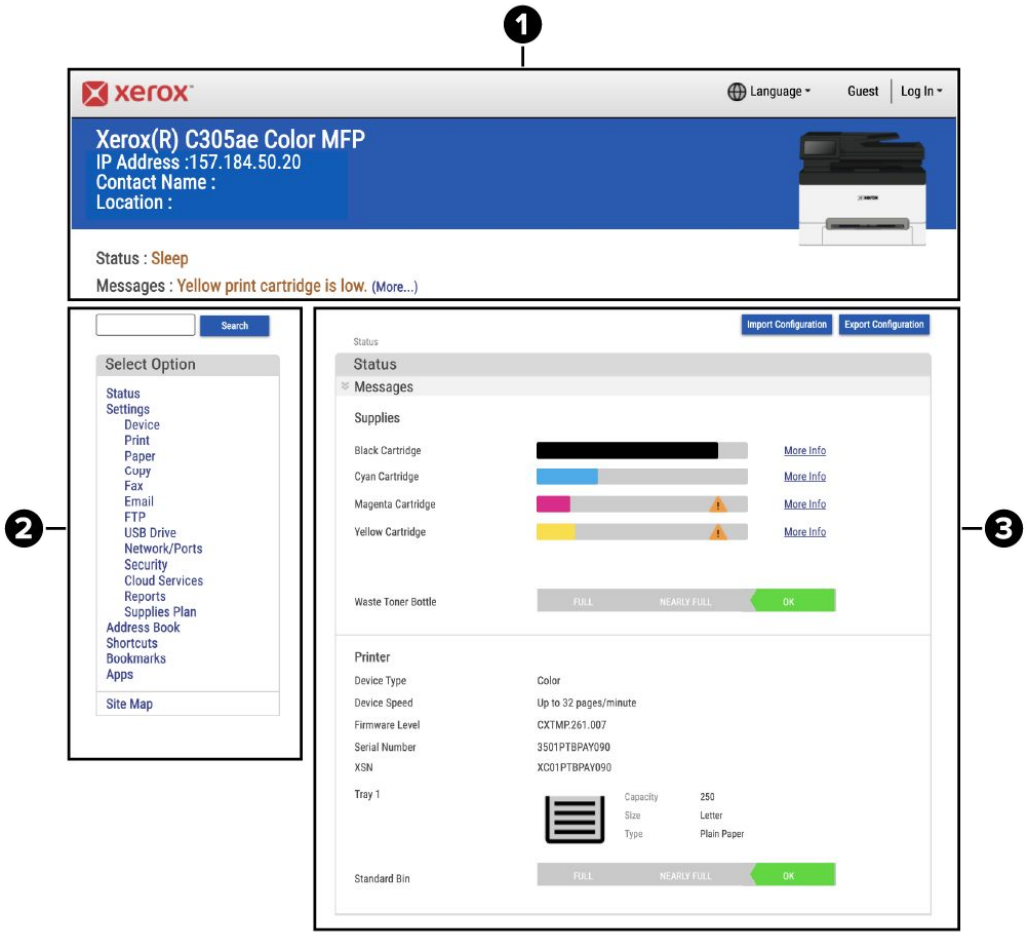
- Google Chrome™ (version 32 or later)
- Microsoft Edge
- Mozilla Firefox (version 24 or later)
- Apple Safari (version 6 or later)

Accessing the Embedded Web Server

1. Obtain the printer IP address. Do either of the following:
   - Locate the IP address at the top of the printer display.
   - From the control panel, navigate to **Settings › Network/Ports › Network Overview › IPv4**.
2. Open a web browser, and then enter the IP address in the address field.

Navigating the Embedded Web Server

The Embedded Web Server (EWS) provides access to printer information, settings, and configuration options through a web-based interface.



	Section	Description
1	Top	• Shows printer information and status. • Lets the user change the language of the EWS. Note: Changing the language of the EWS does not affect the language on the printer display. • Lets the users or admin log in to their accounts.
2	Left	• Lists all available sections and settings in the Embedded Web Server which are organized as clickable links. • Lets the user quickly access any configuration page or search for specific settings.
3	Center	• Shows detailed information for the selected section of the EWS. • Lets the user modify configurations and settings. • Lets the user import or export configuration files.

Understanding helper text

Helper text briefly explains a setting or page and how it affects printer behavior. It appears near the setting field—on the right, below headers, or at the bottom of the page—and shows acceptable data ranges.

Monitoring and basic management

This chapter contains

3. Monitoring and basic management

Finding the printer serial number or XSN (Xerox serial number)

1. In the Embedded Web server, click **Status**.
2. Under **Printer**, locate **Serial Number** or **XSN**.

   Note: The serial number contains 9, 10, or 13 digits.

Viewing part and supply status

1. Obtain the printer IP address. Do either of the following:
   - Locate the IP address at the top of the printer display.
   - From the control panel, navigate to **Settings › Network/Ports › Network Overview › IPv4**.
2. Open a web browser, and then type the IP address in the address field.
3. Click **Status**, and then look for the **Supplies** section.

Configuring supply notifications

1. In the Embedded Web Server, click **Settings › Device › Notifications**.
2. Under **Supplies**, click **Custom Supply Notifications**.
3. Configure the settings for each supply item, and then click **Save**.

Configuring remote control panel settings

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

     Note: This menu item appears only if **Authentication Type** is set to **Standard Authentication**.
3. To launch the remote control panel, click **Launch**.
4. Click **Save**.

Generating reports and logs

Printer reports show the printer status, toner levels, number of pages printed or scanned, and any errors.

1. In the Embedded Web Server, click **Reports**.
2. Select the report or log.
   - **Menu Settings Page**—Print a report that contains the printer menus.

- Device
  - **Device Information**—Print a report that contains information about the printer.
  - **Device Statistics**—Print a report about supply status, paper count, job information, and more.
  - **Profiles List**—Print a list of profiles that are stored in the printer.
- 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.
  - **Email Shortcuts**—Show a list of all email 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.
  - **Fax Call Log**—List the last 100 attempted, received, and blocked calls.
- Network
  - **Network Setup Page**—Print a page that shows the configured network and wireless settings on the printer.

    Note: This report is available only in network printers and printers connected to print servers.
  - **Wi-Fi Direct Connected Clients**—Print a page that shows the list of devices that are connected to the printer using Wi-Fi Direct®.

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

Customizing the home screen

EDITING THE HOME SCREEN

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

1. In the Embedded Web Server, click **Settings › Device › Home Screen Customization**.
2. Select an application from the list, and then do the following:
   a. Click **Edit**.
   b. In the **App Label** field, enter the new name.

Notes

- The label can have up to 20 characters.
- Click **Restore app label** to revert to the original name.

3. Click **Save**.

Note: The edit option is disabled for BLANK SPACE and certain applications.

ADDING APPLICATIONS TO THE HOME SCREEN

Depending on your printer model, do either of the following:

- For printers with 4.3-inch touch screen display or larger:
  1. In the Embedded Web Server, click **Settings** › **Device** › **Home Screen Customization**.
  2. Click **+**, and then select an application.
  3. Click **Add**.

     Note: When the maximum number of applications on a page is reached, the **Add** icon is disabled.

- For printers with 2.8-inch touch screen display:
  1. In the Embedded Web Server, click **Settings** › **Device** › **Visible Home Screen Icons**.
  2. Click the application, and then click **Save**.

ARRANGING APPLICATIONS ON THE HOME SCREEN

1. In the Embedded Web Server, click **Settings** › **Device** › **Home Screen Customization**.
2. Select an application, and then drag and drop it to the intended page.
3. Click **Save**.

Notes

- **Page 1** is the first home screen page. **Other Pages** are subsequent pages. You can move applications between **Page 1** and **Other Pages**.
- You can rearrange applications on **Page 1**, but not on **Other Pages**.
- You cannot drag applications to a page that has reached its application limit.
- If a page has only one application, then you cannot drag it out.

RESTORING THE HOME SCREEN

1. In the Embedded Web Server, click **Settings** › **Device** › **Home Screen Customization**.
2. Click **Restore home screen** to reset applications to their default labels and locations.
3. Click **Restore**.
4. Click **OK**.

Importing and exporting home screen settings

You can transfer home screen settings between printers. Unsupported applications appear as blank spaces on the destination printer.

EXPORTING SETTINGS

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

   The files are saved in ZIP format.

IMPORTING HOME SCREEN SETTINGS

1. In the Embedded Web Server, click **Import Configuration**.
2. Select **Browse**.
3. Select the folder, click **Open**, and then click **Import**.
4. Click **OK**.

Note: If the files fail to import, then a warning message appears.

Managing contacts

ADDING CONTACTS

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

1. In the Embedded Web Server, click **Address Book**.
2. Under **Contacts**, click **Add Contact**.

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

3. Edit the **Contact Information**.

   If necessary, specify a login method for application access.
4. Click **Save**.

ADDING CONTACT GROUPS

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

1. In the Embedded Web Server, click **Address Book**.
2. Under **Contacts Group**, click **Add Group**.

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

3. Type a group name.
4. Click **Save**.

EDITING CONTACTS OR CONTACT GROUPS

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

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

DELETING CONTACTS OR CONTACT GROUPS

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

1. In the Embedded Web Server, click **Address Book**.
2. Do either of the following:
   - Under **Contacts**, select a contact.
   - Under **Contact Groups**, select a group.
3. Click **Delete**.

Print configuration

This chapter contains

4. Print configuration

Configuring print settings

LAYOUT SETTINGS

Note: Certain settings may not be available on all printer models.

1. In the Embedded Web Server, click **Settings › Print › Layout**.
2. Configure the settings.
   - **Sides**—Specify whether to print on one side or two sides of the paper.
   - **Flip Style**—Specify whether the short edge or the long edge of the paper flips when performing two-sided printing.
   - **Blank Pages**—Print blank pages that are included in a print job.
   - **Collate**—Keep the pages of a print job stacked in sequence, particularly when printing multiple copies of the job.
   - **Separator Sheets**—Insert blank separator sheets when printing.
   - **Separator Sheet Source**—Specify the paper source for the separator sheet.
   - **Pages per Side**—Print multiple page on one side of a sheet of paper.
   - **Pages per Side Ordering**—Specify the positioning of multiple-page side when using the **Pages per Side** menu.
   - **Pages per Side Orientation**—Specify the orientation of a multiple-page side when using the **Pages per Side** menu.
   - **Pages per Side Border**—Print a border around each page when using the **Pages per Side** menu.
   - **Copies**—Specify the number of copies for each print job.

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

   - **Print Area**—Set the printable area on a sheet of paper.
3. Click **Save**.

SETUP SETTINGS

Note: Certain settings may not be available on all printer models.

1. In the Embedded Web Server, click **Settings › Print › Setup**.
2. Configure the settings.
   - **Printer Language**—Set the printer language.
   - **Job Waiting**—Preserve print jobs requiring supplies so that jobs not requiring the missing supplies can print.

     Note: This menu item appears only when a storage drive is installed.

   - **Job Hold Timeout**—Set the time in seconds that the printer waits for user intervention before it holds jobs that require unavailable resources.

     Note: This menu item appears only when a storage drive is installed.

- **Printer Usage**—Determine how the color print cartridges operate during printing.
- **Download Target**—Specify where to save all permanent resources that have been downloaded to the printer.

  Note: This menu item appears only when a storage drive is installed.

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

  Note: This menu item appears only when **Automatic Deletion of Suspended Print Jobs** is enabled.

3. Click **Save**.

QUALITY SETTINGS

Note: Certain settings may not be available on all printer models.

1. In the Embedded Web Server, click **Settings › Print › Quality**.
2. Configure the settings.
   - **Print Mode**—Set the printer to print either in color or black and white.
   - **Print Resolution**—Set the resolution for the printed output.

     Note: **Standard** provides high-quality output at maximum speed

   - **Toner Darkness**—Determine the lightness or darkness of text images.
   - **Halftone**—Enhance the printed output to have smoother lines with sharper edges.
   - **RGB Brightness**—Adjust the brightness for color output. The range is **-6** to **6** (including **0**).
   - **RGB Contrast**—Adjust the contrast for color output. The range is **0** to **5**.
   - **RGB Saturation**—Adjust the saturation for color output. The range is **0** to **5**.

   Advanced Imaging
   - **Color Balance**—Adjust the amount of toner that is used for each color.
     - **Reset Defaults**—Reset all color settings to their default values.
   - **Color Correction**—Modify the color settings that are used to print documents.
   - **Color Adjust**—Calibrate the printer to adjust color variations in the printed output.
3. Click **Save**.

JOB ACCOUNTING SETTINGS

Note: Certain settings may not be available on all printer models.

1. In the Embedded Web Server, click **Settings › Print › Job Accounting**.
2. Configure the settings.
   - **Job Accounting**—Set the printer to create a log of the print jobs that it receives.
   - **Accounting Log Frequency**—Specify how often the printer creates a log file.
   - **Log Action at End of Frequency**—Specify how the printer responds when the frequency threshold expires.
   - **Log Near Full Level**—Specify the maximum size of the log file before the printer executes the **Log Action at Near Full**.

     Note: This menu item appears only when a storage drive is installed.

   - **Log Action at Near Full**—Specify how the printer responds when a storage drive is nearly full.
   - **Log Action at Full**—Specify how the printer responds when a storage drive usage reaches the maximum limit (100MB).
   - **URL to Post Log**—Specify where the printer posts job accounting logs.
   - **Email Address to Send Logs**—Specify the email address to which the printer sends job accounting logs.

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

   - **Log File Prefix**—Specify the prefix for the log files.
3. Click **Save**.

PDF SETTINGS

Note: Certain settings may not be available on all printer models.

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

POSTSCRIPT SETTINGS

Note: Certain settings may not be available on all printer models.

1. In the Embedded Web Server, click **Settings › Print › PostScript**.
2. Configure the settings.
   - **Print PS Error**—Print a page that describes the PostScript® emulation error.
   - **Minimum Line Width**—Set the minimum stroke width.
   - **Lock PS Startup Mode**—Disable the SysStart file.

Note: Enabling the SysStart file exposes your printer or network to a security risk.

- **Image Smoothing**—Enhance the contrast and sharpness of low-resolution images.
- **Font Priority**—Establish the font search order.

  Note: This menu item appears only when a storage drive is installed.

- **Wait Timeout**—Enable the printer to wait for more data before canceling a print job. The range is **15** to **65535**.

3. Click **Save**.

PCL SETTINGS

Note: Certain settings may not be available on all printer models.

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

IMAGE SETTINGS

Note: Certain settings may not be available on all printer models.

1. In the Embedded Web Server, click **Settings › Print › Image**.
2. Configure the settings.
   - **Auto Fit**—Select the best available paper size and orientation setting for an image.

- **Invert**—Invert bitonal monochrome images.
- **Scaling**—Adjust the image to fit the printable area.
- **Orientation**—Specify the orientation of text and graphics on the page.

3. Click **Save**.

Scan configuration

This chapter contains

5. Scan configuration

Configuring scan settings

COPY SETTINGS

Note: Certain settings may not be available on all printer models.

1. In the Embedded Web Server, click **Settings › Copy**.
2. Configure the settings.

Copy Defaults
- **Content Type**—Select the content type of the original document.
- **Sides**—Set scanning behavior for single- or double-sided documents.
- **Separator Sheets**—Choose whether to insert blank separator sheets when printing.
- **Separator Sheet Source**—Select the paper source for separator sheets.
- **Color**—Choose whether to print in color or black and white.
- **Pages per Side**—Set the number of page images to print on one sheet.
- **Print Page Borders**—Add borders around each image when printing multiple pages on one sheet.
- **Collate**—Print multiple copies in sequence.
- **"Copy from" Size**—Set the paper size of the original document.
- **"Copy to" Source**—Select the paper source for the copy job.
- **Darkness**—Adjust the darkness of the scanned image.
- **Number of Copies**—Specify how many copies to print.

Header/Footer—Add text to the top (header) or bottom (footer) of each copied page.
- **Left Header**—Insert text in the left header area.
- **Middle Header**—Insert text in the center header area.
- **Right Header**—Insert text in the right header area.
- **Left Footer**—Insert text in the left footer area.
- **Middle Footer**—Insert text in the center footer area.
- **Right Footer**—Insert text in the center footer area.

Advanced Imaging
- **Color Balance**—Adjust toner levels for each color.
- **Auto Color Detect**—Control how much color 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.
- **Contrast**—Adjust the output contrast.
- **Background Removal**—Control how much background appears in a scanned image.
  - **Level**—Specify the background removal level.

- **Auto Center**—Center the content on the page.
- **Scan Edge to Edge**—Include the entire page without margins when copying.
- **Saturation**—Adjust the color intensity of the copy outputs.

Admin Controls

- **Allow Color Copies**—Enable color copying.
- **Allow Priority Copies**—Allow interrupting a print job to copy a page or document.
- **Custom Job Scanning**—Enable scanning of custom jobs by default.

  Note: This menu item appears only when a storage drive is installed.

- **Allow Save as Shortcut**—Save custom copy settings as shortcuts.
- **Sample Copy**—Print a sample copy.

  Note: This menu item appears only when a storage drive is installed.

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**.

EMAIL SCAN SETTINGS

Note: Certain settings may not be available on all printer models.

1. In the Embedded Web Server, click **Settings › Email**.
2. Configure the settings.

Email Setup

- **Primary SMTP Gateway**—Enter the IP address or hostname of the primary SMTP server.
- **Primary SMTP Gateway Port**—Enter the port number of the primary SMTP server.
- **Secondary SMTP Gateway**—Enter the IP address or hostname of the secondary SMTP server.
- **Secondary SMTP Gateway Port**—Enter the port number of the secondary SMTP server.
- **SMTP Timeout**—Set the time (in seconds) the SMTP server waits before stopping an email attempt.
- **Reply Address**—Specify a reply address for emails.

- **Always use SMTP default Reply Address**—Use the default reply address in the SMTP server.
- **Use SSL/TLS**—Specify whether to use SSL/TLS for communication with the SMTP server.
- **Require Trusted Certificate**—Require a trusted certificate when connecting to the SMTP server.
- **SMTP Server Authentication**—Set the authentication type for the SMTP server.
- **Device-Initiated Email**—Set whether credentials are required for device-initiated emails.
- **User-Initiated Email**—Set whether credentials are required for user-initiated emails.
- **Use Active Directory Device Credentials**—Enable the use of Active Directory Credentials and group designations for SMTP authentication.
- **Device Userid**—Enter the user ID to log in to the SMTP server.
- **Device Password**—Enter the password to log in to the SMTP server.
- **Kerberos 5 Realm**—Enter the Kerberos realm name required for certain authentication types.
- **NTLM Domain**—Enter the domain name required for NTLM (NT LAN Manager) authentication.

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

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

    Note: Test email supports device-initiated emails only.

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

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

Set Up OAuth 2.0 for Email Server

- **Status**—Indicates the status of the OAuth 2.0 for email server.
- **Email Service Provider**—Indicates the email service provider registered for OAuth 2.0.
- **Register**—Click to register the email server to OAuth 2.0.
- **Copy**—Click to copy the code to complete OAuth 2.0 registration.

  Note: This menu item appears only after **Register** is clicked.

Email Defaults

- **Subject**—Enter the email subject.
- **Message**—Enter the email message.
- **File Name**—Select the file format for the scanned image.
- **Format**—Select the file format for the scanned image.
- **Global OCR Settings**—Configure optical character recognition (OCR) settings.

  Note: This menu item appears only if you have purchased and installed an OCR solution.

- **PDF Settings**—Set the PDF format of the scanned image.
  - **PDF Version**—Select the PDF version for all scan functions.
  - **Archival (PDF/A)**—Specify whether to enable archival for the scanned image.

    Note: Available only for **PDF Version 1.4** or **1.7**.

  - **Archival Version**—Choose the archival compliance level (active only when **Archival** is enabled).

    Note: **Archival Version A2-u** is only available for **PDF Version1.7**.

  - **Highly Compressed**—Reduce file size by applying high compression.

    Note: This menu item appears only when a storage drive is installed.

  - **Secure**—Enable security features.

    Note: This setting is available only for **PDF Version 1.4** or higher.

  - **Searchable**—Make the PDF text searchable.

    Note: This menu item appears only if you have purchased and installed an OCR solution.

- **Split Job by Pages**—Enter the number of pages per split. Each split is sent as a separate email. To disable, enter **0**. The range is **1** to **999**.
- **Content Type**—Select the content type of the original document.
- **Color**—Select the color mode for scanning.
- **Resolution**—Set the image resolution.
- **Darkness**—Adjust the darkness of the scanned image.
- **Orientation**—Set the page orientation for text and graphics.
- **Original Size**—Specify the paper size of the original document.
- **Sides (Duplex)**—Specify the orientation of the original document when scanning on both sides of the document.

Advanced Imaging

- **Color Balance**—Adjust toner levels for each color.
- **Auto Color Detect**—Control how much color the printer detects from the original document.
  - **Color Sensitivity**—Specify the color sensitivity when scanning the original document.
  - **Area Sensitivity**—Specify the area sensitivity when scanning the original document.
  - **Email Bit Depth**—Specify the bit depth to use for images detected as mono when the Color setting is set to **Auto**.
  - **Minimum Scan Resolution**—Set the minimum resolution for images detected as mono when the Color setting is set to **Auto**.
- **JPEG Quality**—Set the quality of JPEG-format scanned images.
- **Contrast**—Adjust the output contrast.
- **Background Removal**—Control how much background appears in a scanned image.
  - **Level**—Specify the background removal level.

- **Scan Edge to Edge**—Include the entire page without margins when copying.
- **Saturation**—Adjust the intensity of colors in the scanned document.

Admin Controls

- **Max Email Size**—Set the allowable file size for each email.
- **Size Error Message**—Specify an error message that the printer sends when an email exceeds its allowable file size.
- **Limit Destinations**—Limit sending of email only to the specified list of domain name.
- **Send Me a Copy**—Send a copy of the email to yourself.
- **Allow self emails only**—Set the printer to send emails to yourself only.
- **Use cc:/bcc:**—Enable carbon copy and blind carbon copy in email.
- **Use Multi-Page TIFF**—Enable scanning of multiple TIFF images in one TIFF file.
- **TIFF Compression**—Specify the compression type for TIFF files.
- **Text Default**—Set the text quality of the content being scanned.
- **Text/Photo Default**—Set the text and photo quality of the content being scanned.
- **Photo Default**—Set the photo quality of the content being scanned.
- **Transmission Log**—Print a transmission log for email scans.
- **Log Paper Source**—Specify the paper source for printing logs.
- **Custom Job Scanning**—Set the printer to scan the first set of original documents using the specified settings, and then scan the next set with the same or different settings.

  Note: This menu item appears only when a storage drive is installed.

- **Scan Preview**—Show a scan preview of the original document.

  Note: This menu item appears only when a storage drive is installed.

- **Allow Save as Shortcut**—Save an email address as a shortcut.
- **Email Images Sent As**—Specify how to send the images that are included in the email.
- **Reset Email Information After Sending**—Reset the **To**, **Subject**, **Message**, and **Filename** fields to their default values after sending an email.

Web Link Setup

- **Server**—Set the email server to use for the web link.
- **Login**—Set the username 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 customize the scan 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**.

FTP SCAN SETTINGS

Note: Certain settings may not be available on all printer models.

1. In the Embedded Web Server, click **Settings › FTP**.
2. Configure the settings.

FTP Defaults

- **Format**—Specify the file format for the scanned image.
- **Global OCR Settings**—Configure the settings for optical character recognition (OCR).

  Note: This menu item appears only if you have purchased and installed an OCR solution.

- **PDF Settings**—Set the PDF format of the scanned image.
  - **PDF Version**—Select the PDF version for all scan functions.
  - **Archival (PDF/A)**—Specify whether to enable archival for the scanned image.
  - **Archival Version**—Choose the archival compliance level.
  - **Highly Compressed**—Reduce file size by applying high compression.

    Note: This menu item appears only when a storage drive is installed.

  - **Secure**—Enable security features.

    Note: This setting is available only for **PDF Version 1.4** or higher.

  - **Searchable**—Make the PDF text searchable.

    Note: This menu item appears only if you have purchased and installed an OCR solution.

- **Split Job by Pages**—Set the number by which the pages are split and then sent as separate files.
- **Content Type**—Select the content type of the original document.
- **Color**—Set the printer to capture file content in color or in mono.
- **Resolution**—Set the resolution of the scanned image.
- **Darkness**—Adjust the darkness of the scanned image.
- **Orientation**—Specify the orientation of the original document.
- **Original Size**—Set the paper size of the original document.

- **Sides (Duplex)**—Specify the orientation of the original document when scanning on both sides of the document.
- **File Name**—Specify the file name of the scanned image.

Advanced Imaging

- **Color Balance**—Adjust the color intensity for cyan, magenta, and yellow.
- **Auto Color Detect**—Configure the auto color detection setting.
  - **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 JPEG quality of the scanned image.
- **Contrast**—Specify the contrast for the scanned image.
- **Background Removal**—Remove the background color or image noise from the original document.
  - **Level**—Specify the background removal level.
- **Scan Edge to Edge**—Scan the original document from edge to edge.
- **Saturation**—Adjust the color intensity of the outputs.

Admin Controls

- **Text Default**—Set the quality of text on a scanned image.
- **Text/Photo Default**—Set the quality of text and photo on the scanned image.
- **Photo Default**—Set the quality of photo on the scanned image.
- **Use Multi-Page TIFF**—Enable scanning of multiple TIFF images in one TIFF file.
- **TIFF Compression**—Specify the compression type for TIFF files.
- **Transmission Log**—Print a transmission log for FTP scans.
- **Log Paper Source**—Specify the paper source for printing FTP logs.
- **Custom Job Scanning**—Set the printer to scan the first set of original documents using the specified settings, and then scan the next set with the same or different settings.

  Note: This menu item appears only when a storage drive is installed.
- **Scan Preview**—Show a scan preview of the original document.

  Note: This menu item appears only when a storage drive is installed.
- **Allow Save as Shortcut**—Save an FTP address as a shortcut.
- **Use Passive FTP**—Let the FTP server specify the data port that the printer connects to.

3. Click **Save**.

Customize Settings List

This feature lets you customize the scan 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**.

SCAN TO FLASH DRIVE SETTINGS

Flash Drive Scan

Note: Certain settings may not be available on all printer models.

1. In the Embedded Web Server, click **Settings › USB Drive**.
2. Configure the settings.
   - **Format**—Specify the file format for the scanned image.
   - **Global OCR Settings**—Configure the settings for OCR.

     Note: This menu item appears only if you have purchased and installed an OCR solution.
   - **PDF Settings**—Set the PDF format of the scanned image.
     - **PDF Version**—Select the PDF version for all scan functions.
     - **Archival (PDF/A)**—Specify whether to enable archival for the scanned image.
     - **Archival Version**—Choose the archival compliance level (active only when **Archival** is enabled).
     - **Highly Compressed**—Reduce file size by applying high compression.

       Note: This menu item appears only when a storage drive is installed.
     - **Secure**—Enable security features.

       Note: This setting is available only for **PDF Version 1.4** or higher.
     - **Searchable**—Make the PDF text searchable.

       Note: This menu item appears only if you have purchased and installed an OCR solution.
   - **Split Job by Pages**—Set the number by which the pages are split and then scanned as separate files.
   - **Content Type**—Select the content type of the original document.
   - **Color**—Set the printer to capture file content in color or in mono.
   - **Resolution**—Set the resolution of the scanned image.
   - **Darkness**—Adjust the darkness of the scanned image.
   - **Orientation**—Specify the orientation of the original document.

- **Original Size**—Set the paper size of the original document.
- **Sides (Duplex)**—Specify the orientation of the original document when scanning on both sides of the document.
- **File Name**—Specify the file name of the scanned image.

Advanced Imaging

- **Color Balance**—Adjust the color intensity for cyan, magenta, and yellow.
- **Auto Color Detect**—Configure the auto color detection setting.
  - **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 JPEG quality of the scanned image.
- **Contrast**—Specify the contrast for the scanned image.
- **Background Removal**—Remove the background color or image noise from the original document.
  - **Level**—Specify the background removal level.
- **Scan Edge to Edge**—Scan the original document from edge to edge.
- **Saturation**—Adjust the color intensity of the outputs.

Admin Controls

- **Text Default**—Set the quality of text on a scanned image.
- **Text/Photo Default**—Set the quality of text and photo on the scanned image.
- **Photo Default**—Set the quality of a photo on the scanned image.
- **Use Multi-Page TIFF**—Enable scanning of multiple TIFF images in one TIFF file.
- **TIFF Compression**—Specify the compression type for TIFF files.
- **Custom Job Scanning**—Set the printer to scan the first set of original documents using the specified settings, and then scan the next set with the same or different settings.

  Note: This menu item appears only when a storage drive is installed.
- **Scan Preview**—Show a scan preview of the original document.

  Note: This menu item appears only when a storage drive is installed.

3. Click **Save**.

Customize Print Settings List

This feature lets you customize the scan 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. **Save**.

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

Flash Drive Print

Note: Certain settings may not be available on all printer models.

1. In the Embedded Web Server, click **Settings › USB Drive**.
2. Configure the settings.
   - **Number of Copies**—Set the number of copies in a print job.
   - **Paper Source**—Set the paper source for the print job.
   - **Color**—Print the flash drive file in color.
   - **Collate**—Keep the pages of a print job stacked in sequence, particularly when printing multiple copies of the job.
   - **Sides**—Specify whether to print on one side or both sides of the paper.
   - **Flip Style**—Determine which side of the paper is bound when performing two-sided printing.
   - **Pages per Side**—Print multiple page images on one side of a sheet of paper.
   - **Pages per Side Ordering**—Specify the positioning of multiple page images when using the **Pages per Side** menu.
   - **Pages per Side Orientation**—Specify the orientation of multiple page images when using the **Pages per Side** menu.
   - **Pages per Side Border**—Print a border around each page image when using the **Pages per Side** menu.
   - **Separator Sheets**—Insert blank separator sheets when printing.
   - **Separator Sheet Source**—Specify the paper source for the separator sheet.
   - **Blank Pages**—Print blank pages in a print job.
3. Click **Save**.

Customize Print Settings List

This feature lets you customize the print 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 scan shortcut

1. In 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

CONFIGURING A NETWORK DESTINATION

Note: Scan Center is available only in certain printer models.

1. In the Embedded Web Server, click **Apps › Scan Center › Configure**.
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 EMAIL DESTINATION

Note: Scan Center is available only in certain printer models.

1. In the Embedded Web Server, navigate to **Apps › Scan Center › Configure**
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 restrict users from creating or editing destinations through the printer control panel.

CONFIGURING A FAX DESTINATION

Note: Scan Center is available only in certain printer models.

1. In the Embedded Web Server, navigate to the configuration page for the application: **Apps › Scan Center › Configure**
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

Note: Scan Center is available only in certain printer models.

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

1. In the Embedded Web Server, navigate to the configuration page for the application: **Apps › Scan Center › Configure**
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.

Fax configuration

This chapter contains

6. Fax configuration

Configuring fax settings

SELECTING THE FAX MODE

Note: Certain settings may not be available on all printer models.

1. In the Embedded Web Server, click **Settings › Fax › Fax Defaults**.
2. In the **Fax Mode** menu, select a fax mode.
   - **Fax**—Send fax jobs through a telephone line.
   - **Fax Server** —Send fax jobs through a fax server.
   - **Disabled**—Disable the fax feature.
3. Click **Save**.

CONFIGURING ANALOG FAX

General Fax Settings

Note: Certain settings may not be available on all printer models.

1. In the Embedded Web Server, click **Settings › Fax › Fax Setup › General Fax Settings**.
2. Configure the settings.
   - **Fax Name**—Specify your fax ID.
   - **Fax Number**—Specify your fax number.
   - **Fax ID**—Set the fax ID to use during fax negotiation.
   - **Enable Manual Fax**—Turn on the manual fax function in the printer.
   - **Memory Use**—Set the amount of internal printer memory allocated for faxing.
   - **Cancel Faxes**—Cancel outgoing or incoming faxes.
   - **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 the correct port on the printer.
   - **Enable Extension In Use Support**—Determine whether a telephone line is used by another device, such as another phone on the same line.

     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 fax transport method.
3. Click **Save**.

Fax Send Settings

Note: Certain settings may not be available on all printer models.

1. In the Embedded Web Server, click **Settings › Fax › Fax Setup › Fax Send Settings**.
2. Configure the settings.
   - **Resolution**—Set the resolution of the scanned image.
   - **Original Size**—Specify the size of the original document.
   - **Orientation**—Specify the orientation of the original document.
   - **Sides (Duplex)**—Specify the orientation of the original document when scanning on both sides of the document.
   - **Content Type**—Select the content type 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 color intensity during scanning.
   - **Contrast**—Set the contrast of the output.
   - **Background Removal**—Adjust the amount of background visible on a scanned image.
     - **Level**—Specify the background removal level.
   - **Scan Edge to Edge**—Allow edge-to-edge scanning of the original document.
   - **Saturation**—Adjust the color intensity of the fax outputs.

   Admin Controls
   - **Automatic Redial**—Specify the number of attempts that the printer redials before it cancels sending the fax to a specified destination.
   - **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**—Create faxes using the printer scanner.
   - **Allow Save as Shortcut**—Save fax numbers as shortcuts on the printer.
   - **Max Speed**—Set the maximum speed for sending fax
   - **Custom Job Scanning**—Turn on scanning of custom jobs by default.

     Note: This menu item appears only when a storage drive is installed.
   - **Scan Preview**—Show a preview of the scan on the display.

     Note: This menu item appears only when a storage drive is installed.
   - **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

Note: Certain settings may not be available on all printer models.

1. In the Embedded Web Server, click **Settings › Fax › Fax Setup › Fax Receive Settings**.
2. Configure the settings.
   - **Fax Job Waiting**—Remove fax jobs that request specific unavailable resources from the print queue.

     Note: This menu item appears only when a storage drive is installed.

   - **Rings to Answer**—Set the number of rings required before the printer answers the incoming calls.
   - **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.
   - **Fax Holding Schedule**—Assign a schedule for holding faxes.

   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 caller ID information of the incoming call on the printer display.
   - **Block No Name Fax**—Block incoming faxes without fax IDs.
   - **Banned Fax List**—Add the phone numbers that you want to block.
   - **Answer On**—Set a distinctive ring pattern for incoming fax.
   - **Auto Answer**—Set the printer to receive fax automatically.
   - **Manual Answer Code**—Manually enter a code on the telephone number pad to begin receiving fax.

Notes

- This menu item appears only when the printer shares a line with a telephone.
- This menu item appears only when you set the printer to receive fax manually.
- This menu item appears only when **Fax Transport** is set to **Analog**.

- **Fax Forwarding**—Specify whether to forward received fax.
- **Forward to**—Specify where to forward received fax.
- **Confirmation Email**—Send a confirmation email when fax forwarding is successful.
- **Max Speed**—Set the maximum speed for transmitting fax.

3. Click **Save**.

Fax Cover Page

Note: Certain settings may not be available on all printer models.

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

Fax Log Settings

Note: Certain settings may not be available on all printer models.

1. In the Embedded Web Server, click **Settings › Fax › Fax Setup › Fax Log Settings**.
2. Configure the settings.
   - **Transmission Log Frequency**—Specify how often the printer creates a transmission log.
   - **Transmission Log Action**—Print or email a log for successful fax transmission or transmission error.

     Note: This menu item appears only if **Transmission Log Frequency** is set to **Always** or **Only For 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 the fax call history.
- **Log Output Bin**—Specify the output bin for printed logs.

3. Click **Save**.

Speaker Settings

Note: Certain settings may not be available on all printer models.

1. In 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 FAX SERVER

General Fax Settings

Note: Certain settings may not be available on all printer models.

1. In 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 fax receive**—Set the printer to receive analog, FoIP, or etherFAX faxes.
3. Click **Save**.

Fax Server Email Settings

Note: Certain settings may not be available on all printer models.

1. In the Embedded Web Server, click **Settings › Fax › Fax Server Setup › Fax Server Email Settings**.
2. Configure the settings.

- **Use Email SMTP Server**—Use the Simple Mail Transfer Protocol (SMTP) settings for email in receiving and sending faxes.

  Note: When set to **On**, all other settings of the **Fax Server Email Settings** menu are not shown.

- **Primary SMTP Gateway**—Type the IP address or host name of the primary SMTP server.
- **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 if the SMTP server does not respond.
- **Reply Address**—Specify a reply address for sending fax.
- **Use SSL/TLS**—Specify whether to send fax using an encrypted link.
- **Require Trusted Certificate**—Specify a trusted certificate when accessing the SMTP server.
- **SMTP Server Authentication**—Set the authentication type for the SMTP server.
- **Device-Initiated Email**—Specify whether credentials are required for device-initiated email.
- **User-Initiated Email**—Specify whether credentials are required for user-initiated email.
- **Use Active Directory Device Credentials**—Enable user credentials and group destinations to connect to the SMTP server.
- **Device Userid**—Specify the user ID to connect to the SMTP server.
- **Device Password**—Specify the password to connect to the SMTP server.
- **Kerberos 5 Realm**—Specify the realm for the Kerberos 5 authentication protocol.
- **NTLM Domain**—Specify the domain name for the NTLM security protocol.
- **Disable "SMTP server not set up" error**—Disable the SMTP setup error message.
- **Test Connection**—Configure the settings for test connection.
  - **Recipient Email Address**—Type the email address of the recipient.
  - **Send Test Email to Recipient**—Send a test email to the **Recipient Email Address**.
  - **Test**—Select to send the test email.

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

3. Click **Save**.

Set Up OAuth 2.0 for Fax Server settings

Note: Certain settings may not be available on all printer models.

1. In the Embedded Web Server, click **Settings › Fax › Fax Server Setup › Set Up OAuth 2.0 for Fax Server**.
2. Configure the settings.
   - **Status**—Indicates the status of the OAuth 2.0 for email server.
   - **Email Service Provider**—Indicates the email service provider registered for OAuth 2.0.

- **Register**—Click to register the email server to OAuth 2.0.
- **Copy**—Click to copy the code to complete OAuth 2.0 registration.

  Note: This menu item appears only after **Register** is clicked.

3. Click **Save**.

Fax Server Scan Settings

Note: Certain settings may not be available on all printer models.

1. In 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**—Select the content type of the original document.
   - **Fax Resolution**—Set the fax resolution.
   - **Sides (Duplex)**—Specify the orientation of the original document when scanning on both sides of the document.
   - **Darkness**—Set 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.
   - **Use Multi-Page TIFF**—Choose between single- and multiple-page TIFF files.
3. Click **Save**.

Networking

This chapter contains

7. Networking

Configuring the HTTP/FTP Settings

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

1. In 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**—Configure the HTTP default IP port address. The factory default port for HTTP is 80.
   - **FTP Proxy IP Address**—Configure the FTP settings.
   - **FTP Default IP Port**—Configure the FTP default IP port address. The factory default port for FTP is 21.
   - **Authentication**—Specify the authentication credentials.
   - **Username**—Specify the unique username.
   - **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**—Enable Hypertext Transfer Protocol Secure (HTTPS) to encrypt data transferring to and from the print server.
   - **Force HTTPS Connections**—Force the printer to use HTTPS connections.
   - **Enable FTP/TFTP**—Send files using FTP/TFTP.
   - **HTTPS Device Certificate**—View the HTTP device certificate used on the printer.
   - **Timeout for HTTP/FTP Requests**—Specify the amount of 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. In 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.

3. Click **Save**.

Connecting to a wireless network

Before you begin, make sure that your printer is connected temporarily to an Ethernet network.

1. In the Embedded Web Server, click **Settings › Network/Ports › Wireless**.
2. Modify the **Wireless** 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*.

Printer security

This chapter contains

8. Printer security

Securing network connections

CONFIGURING TLS SETTINGS

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

1. In the Embedded Web Server, click **Settings › Network/Ports › TCP/IP**.
2. Under **TLS Support**, click **Enable TLSv1.0**, **Enable TLSv1.1**, or **Enable TLSv1.2**. These settings pertain to the Embedded Web Server only. They do not pertain to clients using TLS.

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

3. Click **Save**.

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

CONFIGURING TCP/IP PORT ACCESS SETTINGS

You can control 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. In 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. In 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**

     Note: This feature is enabled when **Base Configuration** is set to **Compatibility**.
   - **Proposed Encryption Method**

     Note: This feature is enabled when **Base Configuration** is set to **Compatibility**.
   - **Proposed Authentication Method**

     Note: This feature is enabled when **Base Configuration** is set to **Compatibility**.
   - **IPSec Device Certificate**

     Note: Before you can select a device certificate, ensure that the certificate is installed. For more information, see the **Managing certificates** section.
   - **IKE SA Lifetime (Hours)**: The default value is **24**.

     Note: This feature is enabled when **Base Configuration** is set to **Secure**.
   - **IPSec SA Lifetime (Hours)**: The default value is **8**.

     Note: This feature is enabled when **Base Configuration** is set to **Secure**.
4. Do one or more of the following:
   - Under **Pre-Shared Key Authenticated Connections**, type the IP address of the client printer that you want to connect to the printer using Pre-Shared Key based IPSec Authentication.
   - Under **Certificate Authenticated Connections**, type the IP address of the client printer that you want to connect to the printer using Certificate based IPSec Authentication.
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 the **Managing certificates** section.
- Make sure that all printers on the same network using 802.1x are supporting the same EAP authentication type.

1. In the Embedded Web Server, click **Settings › Network/Ports › 802.1x**.
2. Select **Active**.
3. Under **802.1x Authentication**, do the following:
   a. Type the login name and password that the printer uses to log in to the authentication server.
   b. 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).

   c. Select **Enable Event Logging**.

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

   d. 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.

4. Under **Authentication Mechanism**, 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.
5. In the **TTLS Authentication Method** menu, select the authentication method to use.
6. Click **Save**.

CONFIGURING RESTRICTED SERVER ACCESS

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. In 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. Configure the **Restricted Server List Options**.
   - **Block All Ports**—This option addresses the ports that are not in the restricted server list, and blocks all access to the ports (default).

- **Block Printing Only**—This option addresses the ports that are not in the restricted sever list, and blocks only the printing.
- **Block Printing and HTTP Only**—This option addresses the ports that are not in the restricted server list and blocks only printing and HTTP.

4. Click **Save**.

Managing printers 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. In the Embedded Web Server, click **Settings › Network/Ports › TCP/IP › TCP/IP Port Access**.
2. Clear **TCP 80 (HTTP)**.
3. Click **Save**.

CONFIGURING SNMP

Configuring SNMP versions 1 or 2c settings

1. In the Embedded Web Server, click **Settings › Network/Ports › › SNMP**.
2. Under **SNMP Versions 1 and 2c**, select **Enabled › Allow SNMP Set**.
3. In the **GET 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. In the Embedded Web Server, click **Settings › Network/Ports › SNMP**.
2. Under **SNMP Version 3**, 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** menu, select **Authentication, Privacy**.
6. In the **Privacy Algorithm** menu, select the strongest setting supported by your network environment.
7. Click **Save**.

Configuring SNMP traps for monitoring

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. In 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. In the Embedded Web Server, click **Settings › Security › Security Audit Log**.
2. Do one or more of the following:
   - **Activate security audit log**

     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**—Specify the remote syslog server.
     - **Remote Syslog Port**—Specify the port over which the printer sends logged events to a remote server. The default number is **514**.
     - **Remote Syslog Method**—Identify the protocol that the printer uses to transmit logged events to a remote server. Select **Normal UDP** to send log messages and events using a lower-priority transmission protocol. Otherwise, select **Stunnel**.
     - **Remote Syslog Facility**—Specify a Facility value that the printer uses when sending log events to the remote syslog 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 minimum severity level of system events to record. The printer logs events at the chosen level and all more severe levels. 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** to**4** are logged.
     - **Remote Syslog Non-Logged Events**—Set the printer to send any applicable events.

   - **Configure email notification**

     Before you begin, make sure that the printer settings have been configured for email.

a. In the **Admin's Email Address** field, type one or more email addresses. separated by commas.

b. Configure the notification settings.

- **Email Log Cleared Alert**—Set the printer to send an email to the administrator every time a log is deleted.
- **Email Log Wrapped Alert**—Set the printer to send the administrator an email when log entries are wrapping.
- **Log Full Behavior**—Determine how the printer resolves log storage issues when the log fills its allotted memory.
- **Email % Full Alert**—Set the printer to send the administrator an email when the log fills its allotted memory.
- **% Full Alert Level**—Determine if the space occupied by the log equals or exceeds the value of the full alert level.
- **Email Log Exported Alert**—Send an email notification to the administrator when a log is exported.
- **Email Log Settings Changed Alert**—Set the printer to send an email to the administrator when the value of the **Enable Audit** menu is changed.
- **Log Line Endings**—Determine how the printer handles line endings in the log file, depending on the operating system that the file is parsed or viewed.
- **Digitally Sign Exports**—Set the printer to sign exported security logs automatically.

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 Xerox. However, the strongest security measure comes from requiring all firmware packages to include multiple digital 2048-bit RSA signatures from Xerox. If these signatures are not valid, or if the message logs indicate a change in firmware after the signatures were applied, then the firmware is discarded.

Note: Firmware downgrades are not permitted.

1. In the Embedded Web Server, click **Settings › Device › Firmware Update**.
2. Do either of the following:
   - Click **Check for Updates › Install Now**.

     Note: When updating firmware from the server, the printer may install required intermediate firmware. You may need to check for updates multiple times to complete the update.

   - Under **Update Firmware from File**, click **Browse**, click the firmware file, and then click **Upload**.

TPM Firmware Update

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

1. In the Embedded Web Server, click **Settings › Security › TPM Firmware Update**.

   The following settings are displayed:

   - **Current Version**: Displays the current version of the firmware.
   - **Available Version**: Displays the available version of the firmware.

2. Click **Start**.

   A prompt appears which indicates that the device will shutdown and auto reboot.

3. Click **Proceed**.

Managing login and authentication methods

RESTRICTING GUEST ACCOUNT ACCESS

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. In the Embedded Web Server, click **Settings › Security › Login Methods**.
2. Under **Public**, click **Manage Permissions**.
3. Select the access controls that the guest account can access. For more information, see Understanding access controls on page 64.
4. Click **Save**.

CONFIGURING LOCAL ACCOUNTS AND GROUPS

Creating local accounts

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

1. In the Embedded Web Server, click **Settings › Security › Login Methods**.
2. Under **Local Accounts**, click **Add User**.
3. Select the type of authentication method that you want the account to use when logging in to the printer.

   - **Username/Password**—Add an account with a username and password.
   - **Username**—Add an account with a username only.
   - **Password**—Add an account with a password only.
   - **PIN**—Add an account with a personal identification number (PIN) only.

4. Under **User Information**, type the user information and authentication credentials.

5. Under **Permission Groups**, 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 55.

6. Click **Save**.

Editing and deleting local accounts

1. In the Embedded Web Server, click **Settings › Security › Login Methods**.
2. Under **Local Accounts**, 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 accounts, and then click **Delete**.

Creating local account groups

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

1. In the Embedded Web Server, click **Settings › Security › Login Methods**.
2. Do either of the following:
   - **Add a group when managing permissions**
     a. Under **Local Accounts**, 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. For more information, see Creating local accounts on page 54 and Editing and deleting local accounts on page 55.
     b. Under **Permission Groups**, select **Add New Group**.
3. Type a unique group name.
4. Under **Access Controls**, select the functions, menus, and applications that the group can access. If you are adding a new group, then click **Create**.
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 64.

Editing or deleting local account groups

1. In the Embedded Web Server, click **Settings › Security › Login Methods**.
2. Under **Local Accounts**, 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 64.

USING LDAP+GSSAPI AUTHENTICATION

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 Kerberos login methods on page 59.
- 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. In the Embedded Web Server, click **Settings › Security › Login Methods**.
2. Under **Network Accounts**, 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.

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

   - **Use Integrated Windows Authentication**—Select one of the following:

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

     - **Do not use**
     - **Use if available**—Use Windows operating system authentication credentials, if available.
     - **Require**—Use only Windows operating system authentication credentials.

   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.

     Note: This setting 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.

     Note: This setting 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.

       Note: 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**.
- **User ID 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 **300** seconds.
- **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 email address.

- **Displayed Name**—Select the LDAP attribute that you want to show on the address book.
- **Max Search Results**—Type the maximum search results shown on the address book.
- **Use user credentials**—Use the logged-in user credentials to connect to the LDAP server.
- **Search Attributes**—Select LDAP attributes used as search filters.
- **Custom Attributes**—Type LDAP custom attributes used as search filters.
- **Custom Filter**—Type custom filters.

5. Click **Save and Verify**.

Editing or deleting LDAP or LDAP+GSSAPI login methods

1. In the Embedded Web Server, click **Settings › Security › Login Methods**.

2. Under **Network Accounts**, 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 AUTHENTICATION

Creating Kerberos login methods

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.

1. In the Embedded Web Server, click **Settings › Security › Login Methods**.
2. Under **Network Accounts**, click **Add Login Method › Kerberos**.
3. Do one of the following:
   - **Create a simple Kerberos configuration file**

     Under **Generate Simple Kerberos File**, 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**

     Under **Import Kerberos File**, click **Browse** and click the krb5.conf file.
4. If necessary, under **Miscellaneous Settings**, configure the following settings:
   - **Character Encoding**—Select the character encoding used for the configuration file.
   - **Disable Reverse IP Lookups**
5. Click **Save and Verify**.

Configuring date and time for Kerberos authentication

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. In the Embedded Web Server, click **Settings › Device › Preferences › Date and Time**.
2. Do one of the following:
   - **Configuring manually**

     Note: Configuring the date and time manually disables NTP.

     a. Under **Configure**, 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**

     Note: Configuring the NTP settings helps the printer keep the current date and time even after it is turned off.

     a. Under **Network Time Protocol**, select **Enable NTP**, and then type the IP address or host name of the NTP server.

     Note: Most NTP servers are publicly available online. You can use any IP address from these servers.

     b. If the NTP server requires authentication, then in the **Enable Authentication** menu, select **MD5 key**.

     c. Enter the key ID and password.
3. Click **Save**.

USING ACTIVE DIRECTORY

Creating an Active Directory login method

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.

1. In the Embedded Web Server, click **Settings › Security › Login Methods**.
2. Under **Network Accounts**, click **Add Login Method › Active Directory**.
3. Configure the settings.
   - **Domain**—Type the realm or domain name of the Active Directory server.
   - **Username**—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. In the Embedded Web Server, click **Settings › Security › Login Methods**.
2. Under **Network Accounts**, 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**.
- **User ID 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' email 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 email address:

- **Displayed Name**—Select the LDAP attribute that you want to show on the address book.

- **Max Search Results**—Type the maximum search results shown on the address book.
- **Use user credentials**—Use the logged-in user credentials to connect to the LDAP server.
- **Search Attributes**—Select LDAP attributes used as search filters.
- **Custom Attributes**—Type LDAP custom attributes used as search filters.

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

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

1. In the Embedded Web Server, click **Settings › Security › Login Methods**.
2. Under **Network Account**, click the LDAP, LDAP+GSSAPI, Kerberos, or Active Directory 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 username.
     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. Type a unique group name.
6. Select the group, and then under **Access Controls**, select the functions, menus, and applications that the group can access.
7. 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 64.

EDITING OR DELETING DIRECTORY GROUPS (LDAP, LDAP+GSSAPI, KERBEROS, OR ACTIVE DIRECTORY)

1. In the Embedded Web Server, click **Settings › Security › Login Methods**.
2. Under **Network Account**, click the LDAP, LDAP+GSSAPI, Kerberos, or Active Directory login method.
3. Click **Manage Groups**.

4. 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 64.

UNDERSTANDING ACCESS CONTROLS

Access controls let you limit users' access to functions, applications, and printer management.

Note: Certain settings may not be available on all 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.
- **Modify Address Book**—Enable the **Search Address Book** option available in the Email, Fax, and FTP functions when accessed from the printer home screen.
- **Manage Shortcuts**—Access the **Manage Shortcuts** menu, and enable the **Save as Shortcut** option available in the **Copy**, **Email**, **Fax**, and **FTP** functions.
- **Create Profiles**—Create profiles for printing, copying, scanning, emailing, or faxing.
- **Manage Bookmarks**—Configure bookmarks settings.
- **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.
- **Email Function**—Use the email 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.

- **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.
- **Device Menu**—Configure the printer firmware settings.
- **Supplies Plan Menu**—Manage printer supplies plan.

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.
- **Embedded Web Server Access**—Control access to the Embedded Web Server. If this control is restricted, then access to the EWS requires login.
- **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 storage drive.
- **Cloud Connector Management**—Manage cloud connector settings.

- **Cloud Services Enrollment**—Control access to the enrollment of the Lexmark® cloud services.
- **Cloud Print Release**—Configure cloud print release settings.

Apps

- **New Apps**—Use applications 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.
- **Scan Center**—Use Scan Center from the printer home screen.
- **Scan Center Custom**—Use Scan Center custom settings from the printer home screen.

Managing certificates

CONFIGURING PRINTER CERTIFICATE DEFAULTS

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.

1. In the Embedded Web Server, click **Settings › Security › Certificate Management**.
2. Click **Configure Certificate Defaults**.
3. Configure the settings.
   - **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.

   - **Key Type**—Set the key type.
   - **RSA Key Size**—Set the key size of the RSA.

- **Validity Period**—Set the number of days the certificate will be valid for. The range is **365** to **3650** days.

4. Click **Save**.

CREATING PRINTER CERTIFICATES

1. In the Embedded Web Server, click **Settings › Security › Certificate Management**.
2. Under **Device Certificates**, click **Generate**.
3. Configure the settings. For more information, see Configuring printer certificate defaults on page 66.
4. Click **Generate** or **Generate and Download**.

INSTALLING CERTIFICATES MANUALLY

Note: To download the CA certificate automatically, see Installing certificates automatically on page 67.

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. In the Embedded Web Server, click **Settings › Security › Certificate Management**.
2. Under **Manage CA Certificates**, click **Upload CA**, and then browse to the PEM (.cer) file.

   Sample certificate:

   ```
   -----BEGIN CERTIFICATE-----
   MIIE1jCCA76gAwIBAgIQY6sV0KL3tIhBtlr4gHG85zANBgkqhkiG9w0BAQUFA
   DBs
   …
   l3DTbPe0mnIbTq0iWqKEaVne1vvaDt52iSpEQyevwgUcHD16rFy+sOnCaQ==
   -----END CERTIFICATE-----
   ```

3. Click **Save**.

INSTALLING CERTIFICATES AUTOMATICALLY

1. In 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 CERTIFICATES

1. In 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 additional access controls

UNIVERSAL PRINT

Universal Print

Universal Print is a cloud-based print solution for Microsoft 365 users that enables secure printer management without on-premises print servers or printer drivers. It allows users to access cloud printers from supported devices.

Use the Universal Print page to enable and register your Xerox® printer with Universal Print.

Prerequisites

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

Universal Print status

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

- Device is not currently registered with Universal Print—Appears when the printer is not registered.
- Waiting for user to authenticate—Appears when registration is in process and the printer is waiting for user authentication at Microsoft.com.
- Waiting to finish registration—Appears when the user has authenticated and registration is completing.
- Device is online and registered with Universal Print—Appears when registration is successful.
- Successfully deregistered printer from Universal Print—Appears when printer deregistration is successful.

Registering a printer for Universal Print

1. In the Embedded Web Server, click **Settings › Network/Ports › Universal Print**.
2. If you want to change the default printer name, in the **Printer Name** field, enter a new name.

3. Click **Register**.

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

4. When the registration code appears, click **Copy**, and then click the displayed link: https://login.microsoft.com/device.

   Notes

   - Complete the registration before the code expires.
   - The registration code expires after 15 minutes.

5. A Microsoft-managed web page opens. Do the following:
   a. In the **Enter code** window, paste the registration code into the **Code** field, and then click **Next**.
   b. At the **Pick an account** window, select the appropriate Microsoft account.

      Note: The selected Microsoft account is used only to establish a trusted connection between the printer and the Universal Print service. Universal Print does not use the account after registration.

   c. The Xerox Universal Print window appears. Click **Continue**, and then close the window.

   If the registration expires or registration fails, the status changes to **`Device is not currently registered with Universal Print`** in the Universal Print area. Repeat the registration process.

   If registration is successful, the status changes to **`Device is online and registered with Universal Print`** in the Universal Print area. The printer is then available as a cloud printer in the Universal Print service.

To allow users to access the printer, the Azure administrator must share the printer in the Microsoft Azure portal. Do the following:

1. In a web browser, go to https://portal.azure.com/#home, and then log in using the account that was used to register the printer.
2. Under Azure services, click **Universal Print**.
3. Click **Manage › Printers**.
4. Select your printer, and then click **Share**.
5. Do any of the following:

   - To change the default printer name, update the **Share name** field for the cloud printer. A unique share name helps users identify the cloud printer.
   - To allow access to the cloud printer for everyone in the organization, turn on the toggle.
   - To share the printer with specific users, under **Select member(s)**, select the usernames. Use the search option to locate users by name.

6. Click **Share Printer**. When printer sharing is complete, a confirmation message appears.

   After the printer is shared, an authorized user can discover the printer using the **Add Printer** feature in Windows 10 or Windows 11. The printer appears as a cloud printer in the list discovered printers.

To add a cloud printer in Windows 10 or Windows 11, do the following:

1. Click **Settings › Printers & Scanners › Add device**.
2. Select the cloud printer from the list of discovered printers, and then click **Add device**.

Administrator functions for Universal Print

To unregister your local device from Universal Print, do the following:

1. In the Embedded Web Server, click **Settings › Network/Ports › Universal Print**.
2. Under **Registration**, click **Deregister**.
3. At the prompt, click **OK**.
4. Wait a few minutes until the displayed status changes to **`Successfully deregistered printer from Universal Print`**.
5. Click **Continue**.
6. To remove the printer from the Universal Print server, in a web browser, go to the Azure portal https://portal. azure.com/#home, then log in with your credentials.
7. In the Azure portal, click **Manage › Printers**, and then select your printer.
8. Click **Delete Printer Share**, then click **OK**.
9. Click **Unregister**, then at the prompt, click **Unregister Printer**.

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.

Note: Certain features may not be available on all printer models.

1. In 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.

CONFIGURING 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. In 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 HELD JOBS SETUP

1. In the Embedded Web Server, click **Settings › Security › Held Jobs Setup**.
2. Configure the following:
   - **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.

   Confidential Jobs
   - **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.
     - To turn off this setting, enter **0**.

   - **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 storage drive.
     - If the printer is turned off, then all confidential jobs held in the printer memory are deleted.

   - **Keep Held Jobs**—Keep confidential held jobs.

   Repeat Jobs
   - **Job Expiration**—Set the expiration time for a repeat print job.

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

   - **Keep Held Jobs**—Keep repeat print jobs.

   Reserve Jobs
   - **Job Expiration**—Set the expiration time that the printer stores print jobs.

     Note: Reserve held jobs are automatically deleted after printing.

   - **Keep Held Jobs**—Keep reserve print jobs.

Verify Jobs

- **Job Expiration**—Set the expiration time that the printer stores print jobs.

  Note: Reserve held jobs are automatically deleted after printing.

- **Keep Held Jobs**—Keep verify print jobs.

3. Click **Save**.

ENABLING SOLUTIONS LDAP SETTINGS

1. In 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**—Enable verification of LDAP certificates.

     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, secured applications or functions are hidden on the printer home screen.

Note: Certain settings may not be available on all printer models.

1. In the Embedded Web Server, click **Settings › Security › Miscellaneous**.
2. Under **Protected Features**, select **Show**.
3. Click **Save**.

CONFIGURING PRINT PERMISSION

Use this feature to control printing costs. User access to color or black-and-white printing depends on the configured print permissions. For more information, see the **Managing login methods** section.

1. In the Embedded Web Server, click **Settings › Security › Miscellaneous**.
2. Enable **Print Permission**.
3. Click **Save**.

Securing printer data

CONFIGURING PRINTER SETTINGS

Note: Certain settings may not be available on all printer models.

1. In the Embedded Web Server, click **Settings › Device › Maintenance**.
2. Depending on the printer model, click **Config Menu** or **Configuration Menu**.
3. Configure the settings.

   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**—Set the printer to link the trays that have the same paper type and paper size settings.
- **Show Tray Insert Message**—Display a message to select paper size and type after inserting the tray.
- **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**—Set the tray to support multiple universal paper sizes.

  Note: This menu item is available only in certain printer models.

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 usage history to the factory shipped level.
- **Fuser Reset**—Reset the fuser counter after installing a new supply item or maintenance kit.
- **ITM Reset**—Reset the ITM counter after installing a new supply item or maintenance kit.
- Tiered Coverage Ranges
  - **Tiered Coverage Metrics**—Show the **Tiered Coverage Billing** section on the Device Statistics report.

Printer Emulations
- **PPDS Emulation**—Set the printer to recognize and use the PPDS emulation data stream.
- **PS Emulation**—Set the printer to recognize and use the PostScript emulation data stream.
- **Enable Prescribe**—Activate the PRESCRIBE printer language.
- Emulator Security
  - **Page Timeout**—Set the page timeout during emulation.
  - **Reset Emulator After Job**—Reset the emulator after a print job.
  - **Disable Printer Message Access**—Disable access to the printer message during emulation.

Fax Configuration
- **Fax Low Power Support**—Set fax to enter Sleep mode whenever the printer determines that it should.

Print Configuration
- **Black Only Mode**—Print color content in grayscale.

- **Color Trapping**—Enhance the printed output to compensate for misregistration in the printer.
- **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.

Device Operations
- **Quiet Mode**—Set the printer to operate in Quiet Mode.

  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 operate in a special mode, in which it attempts to continue offering as much functionality as possible, despite known issues.
- **Minimum Copy Memory**—Set the minimum memory allocation for storing copy jobs.
- **Clear Custom Status**—Erase user-defined strings for the Default or Alternate custom messages.
- **Clear All Remotely-Installed Messages**—Erase messages that were remotely installed.
- **Automatically Display Error Screens**—Show existing error messages on the display after the printer remains inactive on the home screen for a length of time equal to the **Screen Timeout** setting.
- **Honor Orientation on Fast Path Copy**—Enable the printer to use the orientation setting under the **Copy** menu when sending quick copy jobs.
- **Service Nonvolatile Memory**
  - **Encryption Status**—Show the encryption status of the storage drive.

Toner Patch Sensor Setup
- **Calibration Frequency Preference**—Set the default calibration frequency.
- **Full Calibration**—Run the full color calibration.
- **TPS Information Page**
  - **Print TPS Information Page**—Print a diagnostic page that contains toner patch sensor calibration.

App Configuration
- **LES Applications**—Enable Lexmark Embedded Solutions (LES) applications.

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 ADF 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
  - **Flatbed Edge Erase**—Set the size, in millimeters, of the no-print area around a flatbed scan job.
  - **ADF Edge Erase**—Set the size, in millimeters, of the no-print area around an ADF scan job.
- **Disable Scanner**—Disable the scanner when 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**—Set the number of scans before the user receives a prompt to clean the scanner glass.

  Note: The range of the number of scans is from **1000** to **30000**.

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. In the Embedded Web Server, click **Settings › Device › Maintenance**.
2. Under **Erase Printer Memory**, select **Sanitize all information on nonvolatile memory**.
3. If necessary, under **After erasing all nonvolatile memory**, select either of the following:
   - **Start initial setup wizard**
   - **Leave printer offline**
4. Click **Start**.

ERASING THE PRINTER STORAGE DRIVE

1. In 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**
   - For intelligent storage drive (ISD), select **Cryptographically erase all user data on ISD**.
3. To further configure **Erase Printer Memory** settings, select any of the following:
   - **Erase all printer and network settings**
   - **Erase all apps and app settings**
   - **Erase all shortcuts and shortcut settings**

Note: By default, selecting **Sanitize all information on nonvolatile memory** automatically selects the three erase options listed above.

4. Click **Start**.

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

CONFIGURING THE INTELLIGENT STORAGE DRIVE

Note: This menu item appears only when an intelligent storage drive is installed.

1. In the Embedded Web Server, click **Settings › Security › Miscellaneous**.
2. Select **Use Intelligent Storage Drive for User Data**.
3. Click **Save**.

RESTORING FACTORY DEFAULT SETTINGS

Note: Certain settings may not be available on all printer models.

1. In the Embedded Web Server, click **Settings › Device › Restore Factory Defaults**.
2. Select the settings that you want to restore.
   - **Restore all settings**—Restore all printer factory default settings.
   - **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

This chapter contains

9. Troubleshooting

Application error

Try one or more of the following:

- Check the diagnostic log.

  Note: This solution applies only to certain printer models.

  1. Open a web browser, and then type `IP/se`, where `IP` is the printer IP address.
  2. Click **Embedded Solutions**.
  3. Click **Clear Log File › Yes › Submit**, and then go back to the main menu.
  4. Click **Set Logging Level › Yes › Submit**, and then go back to the main menu.
  5. Click **Log File**.
  6. Analyze the log and resolve the problem.

     Note: After resolving the problem, make sure **Set Logging Level** is set to **No**.

- Contact customer support.

Login troubleshooting

CANNOT DETECT THE CARD READER OR THE SMART CARD

Try one or more of the following:

- Make sure the card reader is connected properly to the printer.
- Make sure the card reader and the smart card are compatible.

  For a list of supported card readers, see the printer *User's Guide*.
- Make sure the card reader driver is installed on the printer.
- Check whether the type of smart card you are using can be reset. If the card cannot be reset, replace the card.

  Note: This solution applies only to certain printer models.
- Turn off the printer, wait for about 30 seconds, and then turn on the printer.
- Contact customer support.

USER ACCOUNT IS LOCKED

Try one or more of the following:

- Update the allowed number of login failures and lockout time. The user may have reached the maximum allowed number of login failures.

  Note: This solution applies only to certain printer models.

  1. In the Embedded Web Server, click **Settings › Security › Login Restrictions**.

2. Update **Login failures** and **Lockout time**.
3. Click **Save**.

- Check whether the type of smart card you are using can be reset. If the card cannot be reset, replace it.

  Note: This solution applies only to certain printer models.

USER IS AUTOMATICALLY LOGGED OUT

1. In 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 the user is assigned to a group with access to the required applications and functions. For more information, see the **Managing login methods** section.

KDC AND PRINTER CLOCKS ARE OUT OF SYNC

Make sure the printer date and time settings are correct. For more information, see Configuring date and time for Kerberos authentication on page 60.

DOMAIN CONTROLLER CERTIFICATE IS NOT INSTALLED

Make sure the correct certificate is installed on the printer. For more information, see the **Managing certificates** section.

KDC IS NOT RESPONDING WITHIN THE REQUIRED TIME

Try one or more of the following:

- Make sure the IP address or host name of the KDC is correct.
- Make sure the KDC is available in the configuration file.
- Make sure the server and firewall settings allow communication between the printer and the KDC server on port 88.

Authentication issues

KERBEROS AUTHENTICATION FAILED

Try one or more of the following:

- Check the **Security Log** file.

  1. Open a web browser, and then type `IP/se`, where `IP` is the printer IP address.
  2. Click **Security Log**, and then click **Turn Debugging ON**.

     Note: Keep the **Security Log** page open.

  3. Log in to the printer using the Kerberos login method to execute a Kerberos authentication workflow.
  4. After completing the workflow, go back to the **Security Log** page and click **View Log File**.

5. Copy or download the **Log File** contents.
6. Analyze the log and resolve the problem.

- Make sure the configuration file is installed on the printer.
  - If you are using simple Kerberos setup to create the Kerberos configuration file, do the following:
    1. In the Embedded Web Server, click **Apps › Smart Card Authentication Client › Configure**.
    2. Under **Simple Kerberos Setup**, make sure the **Realm**, **Domain Controller**, **Domain**, and **Timeout Values** are correct.
  - If you are using the device Kerberos setup file, see Creating Kerberos login methods on page 59 for more information.
- Make sure the configuration file content and format are correct.
  - If you are using simple Kerberos setup, modify the simple Kerberos setup settings.
  - If you are using the device Kerberos setup file, modify and reinstall the file.
- Make sure the Kerberos realm is in uppercase.
  - If you are using simple Kerberos setup, do the following:
    1. In the Embedded Web Server, click **Apps › Smart Card Authentication Client › Configure**.
    2. Under **Simple Kerberos Setup**, make sure the **Realm** value is correct and typed in uppercase.
    3. Click **Apply**.
  - If you are using the device Kerberos setup file, see Creating Kerberos login methods on page 59 for more information.
- Specify the Microsoft Windows operating system domain.
  - If you are using simple Kerberos setup, do the following:
    1. In the Embedded Web Server, click **Apps › Smart Card Authentication Client › Configure**.
    2. Under **Simple Kerberos Setup**, in the **Domain** field, add the Windows domain.

       For example, if the **Domain** field value is `DomainName,.DomainName,` and the Windows domain is `x.y.z`, then change the **Domain** field value to `DomainName,.DomainName,x.y.z`.

       Note: The domain is case sensitive.
    3. Click **Apply**.
  - If you are using the device Kerberos setup file, add an entry to the `domain_realm` section of the file. Type the Windows domain realm in uppercase, then reinstall the file on the printer.
- Contact customer support.

CANNOT GENERATE OR READ CERTIFICATION INFORMATION FROM THE SMART CARD

Try one or more of the following:

- Make sure the certificate information on the smart card is correct.

- Contact customer support.

CANNOT VALIDATE THE DOMAIN CONTROLLER

Try one or more of the following:

- Make sure the realm, domain controller, and domain in the Kerberos configuration file are correct.
  - If you are using simple Kerberos setup to create the Kerberos configuration file, do the following:
    1. In the Embedded Web Server, click **Apps › Smart Card Authentication Client › Configure**.
    2. Under **Simple Kerberos Setup**, make sure the **Realm**, **Domain Controller**, **Domain**, and **Timeout** values are correct.
  - If you are using the device Kerberos setup file, see Creating Kerberos login methods on page 59 for more information.
- Increase the domain controller timeout value.
  - If you are using simple Kerberos setup to create the Kerberos configuration file, do the following:
    1. In the Embedded Web Server, click **Apps › Smart Card Authentication Client › Configure**.
    2. Under **Simple Kerberos Setup**, in the **Timeout** field, enter a value from **3** to **30** seconds.
    3. Click **Apply**.
  - If you are using the device Kerberos setup file, enter a value from **3** to **30** seconds. When finished, reinstall the file on the printer. For more information on configuring the smart card settings, see Configuring the smart card settings on page 92.
- Make sure the domain controller is available.

  Note: Use commas to separate multiple values. The domain controllers are validated in the order listed.
- Make sure port 88 is not blocked between the printer and the domain controller.

CANNOT VALIDATE THE DOMAIN CONTROLLER CERTIFICATE

Try one or more of the following:

- Make sure the certificates installed on the printer are correct. For more information, see Installing certificates manually on page 67.
- Make sure the domain controller validation method is configured properly.
  1. In the Embedded Web Server, click **Apps › Smart Card Authentication Client › Configure**.
  2. Under **Smart Card Setup**, select the appropriate validation method under **Domain Controller Validation**.
  3. Click **Apply**.

CANNOT FIND REALM IN THE KERBEROS CONFIGURATION FILE

Try one or more of the following:

- If you are using simple Kerberos setup, do the following:
  1. In the Embedded Web Server, click **Apps › Smart Card Authentication Client › Configure**.

2. Under **Simple Kerberos Setup**, in the **Realm** field, add or change the realm. The realm must be typed in uppercase.

   Note: The simple Kerberos setup does not support multiple Kerberos realm entries. If multiple realms are needed, install a Kerberos configuration file containing the necessary realms.

3. **Apply**.

- If you are using the device Kerberos setup file, add or change the realm in the file. The realm must be typed in uppercase. When finished, reinstall the file on the printer.

DOMAIN CONTROLLER AND DEVICE CLOCKS ARE OUT OF SYNC

Make sure the time difference between the printer and the domain controller does not exceed five minutes. For more information, see Configuring date and time for Kerberos authentication on page 60.

CANNOT VALIDATE THE DOMAIN CONTROLLER CERTIFICATE CHAIN

Try one or more of the following:

- Make sure the certificates installed on the printer are correct. For more information, see Installing certificates manually on page 67.
- Make sure the certificate chain is from the domain controller to the root CA.
- Make sure all certificates are not expired.

  1. In the Embedded Web Server, click **Settings › Security › Certificate Management**.
  2. Make sure the **Valid From** and **Valid To** dates have not expired.

- Allow users to log in even if the status of one or more certificates is unknown.
  1. In the Embedded Web Server, click **Apps › Smart Card Authentication Client › Configure**.
  2. Under **Online Certificate Status Protocol (OCSP)**, select **Allow Unknown Status**.
  3. Click **Apply**.

- Contact customer support.

CANNOT CONNECT TO THE OCSP RESPONDER

Try one or more of the following:

- Ensure that the OCSP responder URL is correct.

  1. In the Embedded Web Server, click **Apps › Smart Card Authentication Client › Configure**.
  2. Under **Online Certificate Status Protocol (OCSP)**, ensure that the responder URL is correct.
  3. Click **Apply**.

- Increase the responder timeout value.

  1. In the Embedded Web Server, click **Apps › Smart Card Authentication Client › Configure**.
  2. Under **Online Certificate Status Protocol (OCSP)**, in the **Responder Timeout** field, enter a value from **5** to **30**.
  3. Click **Apply**.

CANNOT VALIDATE THE DOMAIN CONTROLLER CERTIFICATE AGAINST THE OCSP RESPONDER

Try one or more of the following:

- Make sure the OCSP responder URL and the responder certificate are configured correctly.

  1. In the Embedded Web Server, click **Apps › Smart Card Authentication Client › Configure**.
  2. Under **Online Certificate Status Protocol (OCSP)**, in the **Responder URL** field, specify the following:
     - IP address or host name of the OCSP responder or repeater
     - Port number used

     For example, `https://192.198.10.1:80`, where `192.198.10.1` is the OSCP responder IP address and `80` is the port number.
  3. In the **Responder Certificate** field, browse to the appropriate certificate.
  4. Click **Apply**.

- Make sure the domain controller returns the correct certificate.
- Make sure the OCSP responder validates the correct domain controller certificate.

CANNOT ACCESS INDIVIDUAL APPLICATIONS AND FUNCTIONS ON THE PRINTER

Try one or more of the following:

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

LDAP troubleshooting

LDAP LOOKUPS FAIL

Try one or more of the following:

- Make sure the server and firewall settings are configured to allow communication between the printer and the LDAP server on ports **389** and **636**.

  Note: The default ports are **389** and **636**.

- If reverse DNS lookup is not used in your network, disable it in the Kerberos settings:

  1. In the Embedded Web Server, click **Settings › Security › Login Methods**.
  2. Under **Network Accounts**, click **Add Login Method**, and then click **Kerberos**.
  3. Under **Miscellaneous Settings**, select **Disable Reverse IP Lookups**.
  4. Click **Save and Verify**.

- If the LDAP server requires SSL, enable SSL for LDAP lookups.

  Note: Some authentication solutions require SSL to be enabled 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 required users.
- Make sure all LDAP attributes being searched are correct.

Scanning problems

CANNOT SCAN TO THE SELECTED DESTINATION

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

Try one or more of the following:

- Make sure the destination is valid.

  In 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, make sure the domain information is specified.

  In the Embedded Web Server, open the application configuration page, and then enter the appropriate domain information.
- Make sure the printer is connected to the network.
- Make sure the username and password are correct.
- Make sure the user has permission to save scans to the destination.
  1. In the Embedded Web Server, open the application configuration page.
  2. In the **Scan Destination** section, select the destination to configure.
  3. In the **Authentication Options** section, select the correct authentication type, and type the correct authentication credentials if needed.
  4. Click **Apply**.
- Make sure that a file with the default file name does not exist at the destination.

  Remove the existing file, or configure the application to do one of the following:
  - 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

Try one or more of the following:

- Make sure the printer date and time settings are correct.
  1. In the Embedded Web Server, click **Settings › Device › Preferences › Date and Time**.

2. Do one of the following:

   - **Configuring manually**

     Note: Configuring the date and time manually disables NTP.

     a. Under **Configure**, 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**

     Note: Configuring the NTP settings helps the printer keep the current date and time even after it is turned off.

     a. Under **Network Time Protocol**, select **Enable NTP**, and then type the IP address or host name of the NTP server.

     Note: Most NTP servers are publicly available online. You can use any IP address from these servers.

     b. If the NTP server requires authentication, then in the **Enable Authentication** menu, select **MD5 key**.

     c. Enter the key ID and password.

- Contact customer support.

AN ERROR OCCURS WHEN OPENING A SECURE PDF FILE

Make sure **PDF Version** is not set to **A-1a**.

1. In the Embedded Web Server, do either of the following:
   - Click **Settings › Email › Email Defaults**.
   - Click **Settings › FTP**.
2. Under **PDF Settings**, select any 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 the sender used the correct fax number.
- Check whether the fax has no caller ID or station name.

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

- Check whether the sender fax number is not blocked.

  1. In the Embedded Web Server, click **Settings › Fax › Fax Setup**.
  2. Under **Fax Receive Settings**, click **Admin Controls**. If the sender fax number is listed in **Banned Fax List**, remove it.
  3. Click **Save**.

- Generate fax logs and identify the status message.

  In the Embedded Web Server, click **Reports › Fax › Fax Job Log**.

CANNOT RECEIVE FAX FROM ALL SENDERS

Note: Fax receiving issues may occur if the line uses VoIP instead of analog. VoIP can affect fax functionality. Contact your service provider to verify that the line supports both sending and receiving faxes.

Try one or more of the following:

- Make sure the printer is configured to receive faxes.

  1. In the Embedded Web Server, click **Settings › Fax › Fax Setup**.
  2. Under **Fax Receive Settings**, click **Admin Controls**, and then select **Enable Fax Receive**.
  3. Click **Save**.

- If using a distinctive ring service, make sure the printer is configured to answer the correct ring pattern.

  1. In the Embedded Web Server, click **Settings › Fax › Fax Setup**.
  2. Under **Fax Receive Settings**, click **Admin Controls**, and then select the correct ring pattern under **Answer On**.
  3. Click **Save**.

- Reduce the maximum receive speed.

  1. In the Embedded Web Server, click **Settings › Fax › Fax Setup**.
  2. Under **Fax Receive Settings**, click **Admin Controls**, and then reduce the **Max Speed** setting.
  3. Click **Save**.

- Check the fax forwarding setting.

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

  1. In the Embedded Web Server, click **Settings › Fax › Fax Setup**.
  2. Under **Fax Receive Settings**, click **Admin Controls**, and then select any setting in **Fax Forwarding** except **Forward**.
  3. Click **Save**.

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

  1. In the Embedded Web Server, click **Settings › Fax › Fax Setup**.
  2. Under **Fax Receive Settings**, change the **Rings to Answer** value.
  3. Click **Save**.

- Generate fax logs and identify the status message.

  In 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 you entered the correct fax number.
- Reduce the maximum send speed.

  1. In the Embedded Web Server, click **Settings › Fax › Fax Setup**.
  2. Under **Fax Send Settings**, click **Admin Controls**, and then reduce the **Max Speed** setting.
  3. Click **Save**.

- Generate fax logs and identify the status message.

  In 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 **Fax Mode** is set to **Fax**.

  Note: This feature is supported only in certain printer models.

  1. In the Embedded Web Server, click **Settings › Fax**.
  2. Under **Fax Mode**, make sure **Fax** is selected.

- Make sure the printer is configured to send faxes.

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

- Check whether 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, do the following:

  1. In the Embedded Web Server, click **Settings › Fax › Fax Setup**.
  2. Under **Fax Send Settings**, select **Behind a PABX**.
  3. Click **Save**.

- Check whether you have entered the correct dialing prefix.

  1. In the Embedded Web Server, click **Settings › Fax › Fax Setup**.
  2. Under **Fax Send Settings**, click **Admin Controls**, and then check the value in **Dial Prefix**.

     Add the dialing prefix that you want to use, and then click **Save** if needed.

- Reduce the maximum send speed.

  1. In the Embedded Web Server, click **Settings › Fax › Fax Setup**.
  2. Under **Fax Send Settings**, click **Admin Controls**, and then reduce the **Max Speed** setting.
  3. Click **Save**.

- Make sure you entered a station ID and station number.

  1. In the Embedded Web Server, click **Settings › Fax › Fax Setup**.
  2. Under **General Fax Settings**, make sure **Fax Name** and **Fax Number** are not blank.
  3. Click **Save**.

- Generate fax logs and identify the status message.

  In 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. In the Embedded Web Server, click **Reports › Network › Network Setup Page**.
  2. Under **Ethernet** and/or **Wireless**, check whether **Card Status** is connected.
  3. If the printer is disconnected, do either of the following:

     - For wired connection, make sure 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 46.

- Check the printer port access.

  1. In the Embedded Web Server, click **Settings › Network/Ports › TCP/IP › TCP/IP Port Access**.
  2. If necessary, enable the required ports. For more information, see Configuring TCP/IP port access settings on page 48.
  3. Click **Save**.

- Check the **Restricted Server List** setting.

  1. In the Embedded Web Server, click **Settings › Network/Ports › TCP/IP**.
  2. Under **Restricted Server List**, check whether required destination server IP addresses are listed.

     - If the list is populated and the required server IP addresses are not listed, add them.
     - If the setting is not required, clear the **Restricted Server List**.

  3. Click **Save**.

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

Contacting customer support

To accurately diagnose your issue, our support agents must perform diagnostic troubleshooting with you during your call. Make sure you are near your device so you can follow the on-screen or spoken instructions.

If you are not near your device, you can call us back when you are ready.

Have the following information ready when you contact support:

- Printer model and serial number
- A brief description of the issue
- Any error messages (if applicable)

Note:

- For instructions on locating the printer serial number or the , see Finding the printer serial number or XSN (Xerox serial number) on page 12.
- Depending on your printer model, the serial number is 9, 10, or 13 digits. Look for **SN** or **XSN–Xerox Serial Number** on the label.

Technical support is also available by phone:

- For Xerox, go to https://support.xerox.com, and then click **Contact Support**.
- For Lexmark (U.S. or Canada), call **1-800-539-6257**. For other countries or regions, go to www.lexmark.com/supportdirectory.

Configuring smart card authentication

This chapter contains

10. Configuring smart card authentication

Configuring the login screen settings

Note: Certain settings may not be available on all printer models.

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

Configuring the manual login settings

Note: Certain settings may not be available on all printer models.

For manual login, the printer uses the default domain specified in the Kerberos configuration file. If users log in with a different domain, specify the domain name in the manual login settings.

1. In the Embedded Web Server, click **Apps › Smart Card Authentication Client › Configure**.
2. Under **Manual Login Setup**, in the **Manual Login Domains** field, enter one or more domain names.
3. Click **Apply**.

Configuring the smart card settings

Notes

- Certain settings may not be available on all printer models.
- Ensure that the network connection between the printer and the authenticating server is configured properly. For more information, contact the system administrator.

1. In the Embedded Web Server, click **Apps › Smart Card Authentication Client › Configure**.
2. Under **Smart Card Setup**, in the **Kerberos Information** menu, select one of the following:
   - **Use device Kerberos setup file**—A Kerberos configuration file must be manually installed on the printer.
     a. In the Embedded Web Server, click **Settings › Security › Login Methods**.
     b. Under **Network Accounts**, click **Add Login Method › Kerberos**.

c. Under **Import Kerberos File**, browse to the appropriate `krb5.conf` file.

d. If your network does not use reverse DNS lookup, then under **Miscellaneous Settings**, select **Disable Reverse IP Lookups**.

e. Click **Save** and **Verify**.

- **Use simple Kerberos setup**—A Kerberos configuration file is created automatically on the printer. Configure the following settings:
  - **Realm**—Enter the realm in uppercase.
  - **Domain Controller**—Enter one or more domain controllers, separated by commas. The printer validates the domain controllers in the order listed.
  - **Domain**—Enter the domain that maps to the Kerberos realm specified in the **Realm** field. Use commas to separate multiple domains.

    Note: The domain is case sensitive.

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

3. Under **Domain Controller Validation**, select the method for validating the domain controller certificate.

   Note: Before configuring this setting, make sure the appropriate certificates are installed on the printer. For more information, see Installing certificates manually on page 67.

   - **Use device certificate validation**—Uses the CA certificate installed on the printer.
   - **Use device chain validation**—Uses the entire certificate chain installed on the printer.
   - **Use OCSP validation**—Uses an OCSP server. Ensure that the entire certificate chain is installed on the printer. Under **Online Certificate Status Protocol (OCSP)**, configure the following:
     - **Responder URL**—Enter the IP address or host name of the OCSP responder or repeater and the port number.

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

     - **Responder Certificate**—Uses the X.509 certificate.
     - **Responder Timeout**—Enter a value from **5** to **30** seconds.
     - **Allow Unknown Status**—Allows users to log in even if the status of one or more certificates is unknown.

4. Click **Apply**.

Configuring advanced settings

Note: Certain settings may not be available on all printer models.

1. In the Embedded Web Server, click **Apps › Smart Card Authentication Client › Configure**.
2. Under **Advanced Settings**, select a session user ID.

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

3. Under **Email From Address**, select where the printer retrieves the user email address.

4. If required, select **Wait for user information** to retrieve all user information before allowing access to the home screen or secure applications.

   If the following settings are set to **LDAP Lookup**, then select this option:
   - **Session User ID**
   - **Email From Address**

   If the following settings are not empty, then select this option:
   - **Other User Attributes**
   - **Group Authorization List**

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

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

   Note: The groups must exist in the LDAP server.

8. If DNS is not enabled in your network, then upload a hosts file.

   Enter mappings in the format `xy`, where `x` is the IP address and `y` is the host name.

   Multiple host names can be assigned to a single IP address.

   For example: `255.255.255.255 HostName1 HostName2 HostName3`

   You cannot assign multiple IP addresses to a single host name. To assign multiple IP addresses, enter each IP address and its associated host names on a separate line.

   ```
   123.123.123.123 HostName1 HostName2
   ```

   ```
   102.102.102.102 HostName3
   ```

9. Click **Apply**.

Notices

This chapter contains

Notices

Edition notices

June 2026

The following paragraph does not apply to any country where such provisions are inconsistent with local law: XEROX CORPORATION 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 Xerox technical support, go to https://www.support.xerox.com/.

For information on Xerox's privacy policy governing the use of this product, go to https://www.xerox.com/en-us/about/privacy-policy.

For information on supplies and downloads, go to https://www.xerox.com.

GOVERNMENT END USERS

The Software and accompanying documentation are "commercial" as defined in FAR 2.101. For civilian agencies, consistent with FAR 12.212, commercial computer software or commercial computer software documentation are licensed to the U.S. Government under the vendor's standard commercial license(s) customarily provided to the public, and the Government shall have only those rights specified in such license(s), to the extent consistent with Federal law and otherwise meeting Government needs. For Department of Defense (DoD) agencies, consistent with DFARS 227.7202-1 and 227.7202-3, commercial computer software or commercial computer software documentation are licensed to DoD under the vendor's standard commercial license(s) customarily provided to the public, and the Government shall have only the rights specified in such license(s), unless additional rights are expressly negotiated and expressly stated in the contract or an addendum.

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.