Version 1.0
July 2021
702P08632

Xerox® EC8036/EC8056 Color Multifunction Printer System Administrator Guide

xerox™

Table of Contents

1

Introduction

This chapter contains:

Overview

This guide is designed for a system administrator with network administrator rights who understands networking concepts and has experience creating and managing network user accounts.

Use this guide to help you install, configure, and manage your printer on a network.

Note:

- Network features are not available when the printer is connected using USB.
- Embedded fax features are not available for all printer models.

Configuration Steps

When you configure the device for the first time, complete the following tasks.

1. Ensure that your device is connected physically to your network, and to the fax line, as needed.
2. Confirm that your device is recognized on your network. By default, the device is configured to receive an IP address from a DHCP server over a TCP/IP network. If you have another type of network, or want to assign a static IP address, refer to IP.
3. Complete the installation wizards. These wizards help you configure basic device settings such as your location, time zone, and date and time preferences.
4. Print a configuration report listing the current device configuration. Review the report and locate the device IPv4 address. For details, refer to Configuration Report.
5. Open a Web browser and type the IP address of your device to access the Embedded Web Server. The Embedded Web Server is the administration and configuration software installed on the device. For details, refer to Accessing the Embedded Web Server.

   Note: You can access most configuration settings on the Properties tab in the Embedded Web Server.
6. Print the Configuration Checklist. The Configuration Checklist provides space for you to write down important information as you go through the configuration process. Use it to record information about your network settings, including passwords, network paths, and server addresses. To access the checklist, in the Embedded Web Server, click **Properties > Configuration Overview**, then click **View Checklist**.
7. Create a host name for the device. For details, refer to DNS.
8. Configure Authentication. For details, refer to Setting Access Rights.
9. Configure Security. For details, refer to Security.
10. Enable services in the Embedded Web Server. For details, refer to Selecting Apps to Appear on the Touch Screen.
11. Configure Print, Scan, and Fax features. For details, refer to Printing, Scanning, and Faxing.
12. Configure Accounting. For details, refer to Accounting.

    Note: Not all options listed are supported on all devices. Some options apply only to a specific device model, configuration, operating system, or driver type.

More Information

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

Resource	Location
Installation Guide	Packaged with the printer.
Other documentation for your printer	www.support.xerox.com
Recommended Media List	United States: https://www.xerox.com/downloads/usa/en/supplies/rml/AltaLink_C8030_C8035_C8045_C8055_RML.pdf European Union: https://www.xerox.com/downloads/europe/r/2017_05_AltaLinkC8030-C8055_Media_List_Antalis_Xerox_May_2017.pdf
Technical support information for your printer, including online technical support, Online Support Assistant, and print driver downloads.	www.support.xerox.com
Information Pages	To print from the control panel, touch **Device > Information Pages**. To print from the Embedded Web Server, click **Home > Information Pages**.
Embedded Web Server information	In the Embedded Web Server, click **Help**.
Order supplies for your printer	www.xerox.com/printer-supplies
A resource for tools and information, including interactive tutorials, printing templates, helpful tips, and customized features to meet your individual needs.	www.xerox.com/office/businessresourcecenter
Local sales and Technical Customer Support	www.xerox.com/worldcontacts
Printer registration	www.xerox.com/RegisterMyXerox
Xerox® Direct online store	www.direct.xerox.com/

2

Initial Setup

This chapter contains:

Physically Connecting the Printer

1. Connect the power cord to the printer, and plug it into an electrical outlet.
2. Connect one end of a Category 5 or better Ethernet cable to the Ethernet port on the back of the printer. Connect the other end of the cable to a correctly configured network port.
3. If your printer has fax installed, connect it to a correctly configured telephone line.
4. Power on the printer.

Assigning a Network Address

The printer automatically acquires a network address from a DHCP server by default.

To assign a static IP address, configure DNS server settings, or configure other TCP/IP settings, refer to IP.

If the printer does not detect a DHCP server, the printer uses an IPv4 self-assigned address. Address information is listed on the configuration report. For details, refer to Configuration Report.

Connecting the Device to a Wireless Network

If you have purchased the Wireless Network Adapter, you can connect the device to a wireless network using the Wireless Wizard. The Wireless Wizard provides the easiest method of connecting the device to a wireless network. If the device is connected to a wired network, you can configure wireless settings in the Embedded Web Server. You can connect a computer directly to a wireless network. For details, refer to Connecting to a Wireless Network.

Note: You cannot connect to a wired network and a wireless network at the same time.

Accessing Administration and Configuration Settings

You can access the administration and configuration settings from the Tools menu on the control panel or from the Properties tab in the Embedded Web Server. The control panel is the interface from which you can control the functions available on the device. The control panel consists of the following components:

- Touch screen: Use the touch screen to access and control the functions available on the device.
- Power button: Use the power button to power the device on or off and to wake the device from sleep mode.
- Home button: Use the Home button to return to the Home screen directly from any other screen.

The Embedded Web Server is the administration and configuration software installed on the printer. It allows you to configure and administer the printer from a Web browser.

The administrator password is required when accessing locked settings in the Embedded Web Server or at the control panel. Most printer models have a default configuration that restricts access to some settings. Access is restricted for settings on the Properties tab in the Embedded Web Server, and settings on the device touch screen Tools menu on the device touch screen.

Accessing the Control Panel as a System Administrator

1. At the device control panel touch screen, touch **Log In**.
2. Type **admin**, then touch **Next**.
3. Type the administrator password, then touch **Done**.

   Note: The default password is **1111**.

Accessing the Embedded Web Server as a System Administrator

Before you begin:

- Locate your device IP address using the Configuration Report.

  Note: The device prints a Configuration Report at power-up. For details, refer to Printing the Configuration Report.

- Ensure that TCP/IP and HTTP are enabled. If you disabled either of the protocols, at the control panel, re-enable the protocols. For details, refer to IP and HTTP.

To log in to the Embedded Web Server as the administrator:

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

   Note: To ensure that untrusted-certificate Web browser errors do not appear, install the Device Root Certificate Authority for the device. For details refer to Security Certificates.

2. In the top right area of the page, click **Login**.
3. For User ID, type **admin**.
4. For Password, type the administrator password. The default password is **1111**.
5. Click **Login**.

Note: When you attempt to log in with the default password, the system prompts you with this message: `The default password for the admin account is still being used. For greater security, changing the default password is recommended.` Select an option:

- **Prompt at Next Login**: Select this button to leave the password at the default setting.
- **Change Password / Policy**: Select this button to change the password. For details, refer to Changing the System Administrator Password.

Using the Search Function in the Embedded Web Server

The Search feature in the Embedded Web Server returns one or more links to configuration pages for features related to your search term. The Search field is at the top of the navigation pane.

Note: A general search term, such as *print*, can yield multiple results. A specific search term, such as *secure print*, yields more specific results.

To use the Search function:

1. Log in to the Embedded Web Server as an administrator.
2. Click **Properties**.
3. In the Search field, type a search term for the administrator function you want to locate.

Printing the Configuration Report

The Configuration Report lists all current settings of the printer. A configuration report prints at startup by default.

Printing the Configuration Report from the Control Panel

To print the Configuration Report from the device control panel:

1. At the control panel touch screen, log in as an administrator. For details, refer to Accessing the Control Panel as a System Administrator.
2. Touch **Device**, then touch **Information Pages**.
3. Touch **Configuration Report**, then touch **Print**.

Printing the Configuration Report from the Embedded Web Server

To print the Configuration Report from the Embedded Web Server:

1. In the Embedded Web Server, click **Home > Configuration Report**.

2. To print the report, click **Print Configuration Page**.

Disabling the Configuration Report at Startup

1. In the Embedded Web Server, click **Properties > Apps**.
2. Click **Printing > General**.
3. For Configuration Report, clear **Print at Power on**.
4. To save the new settings, click **Save**.

Initial Setup at the Control Panel

Installation Wizard

The Installation Wizard starts the first time that you power on the printer. The wizard prompts you with a series of questions to help you configure basic printer settings. You can complete the initial configuration using the Installation Wizard or a clone file.

Note: A clone file contains configuration settings from one printer that you can use to configure a similar printer.

- To assign a static IP address or change the default dynamic addressing settings, use the IP Address Settings wizard.

  Note:

  - It is recommended that you use DHCP to obtain the IP address automatically.
  - If DHCP is enabled, your DHCP server can provide the Host Name and Domain Name. For details, refer to IP.
  - To ensure that the IP address does not change, use a DHCP reserved address. You can create a DHCP reservation for a permanent IP address on your DHCP server.
- To add phone numbers for support or supplies contacts, use the Contact Numbers wizard.
- To configure basic embedded fax settings, use the Fax Setup wizard.

Note: After the initial setup, to change any printer configuration settings, or to configure other printer settings, log in to the Embedded Web Server. For details, refer to Accessing the Embedded Web Server as a System Administrator.

Using the Installation Wizard

To use the initial Installation Wizard:

1. To select a language, the Date & Time settings, and any applicable options, follow the wizard prompts.

   Note: If a network connection is not detected, an alert notifies you. Ensure that your network cable is plugged in securely.
2. Complete the Additional Install Options:
   - To add phone numbers for support or supplies contacts, touch **Contact Numbers**.
   - To assign a static IP Address, or to change the default dynamic addressing settings, touch **IP Address Settings**.
   - To configure basic embedded fax settings, touch **Fax Setup**.

   Note: You can complete the Additional Install Options later.
3. To complete the configuration using a clone file:

   a. At the prompt, insert a USB Flash drive into a USB port.

   b. Select the clone file, then click **Install**.

   c. At the confirmation prompt, click **Install**, then wait a few seconds.

4. To complete the installation without a clone file:
   a. Set the Paper Size Preference.
   b. Select a Device Information setting.
   c. Change the password for the administrator account. To leave the password at the default setting, click **Skip**. You can change the password later.

      Note: When you attempt to log in to the Embedded Web Server with the default administrator password, the system prompts you to change the password.
5. At the Device Setup Complete screen, follow the onscreen instructions, then click **Restart**.

Configuring the Additional Install Options

You can change the printer configuration settings at any time using the Additional Install Options.

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **Device Settings > Additional Install Options**.
3. To start a wizard, touch **IP Address Settings**, **Contact Numbers**, or **Fax Setup**.
4. Follow the onscreen instructions.

Setting the Measurement Units

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **Device Settings > General > Measurements**.
3. To show dimensions in metric or imperial units, for Units, select an option.
4. To specify the decimal mark symbol that the printer uses, for Numeric Separator, select **Comma** or **Period**.
5. Click **OK**.

Installing Optional Software Features

When you purchase an optional software feature, to enable it, provide a feature installation key. Some features come with an activation code that you use to request a feature installation key. Go to the Xerox® Software Activation Portal website at www.xeroxlicensing.xerox.com/fik to enter the activation code. The website generates a feature installation key that you can use to enable the feature.

You can also install optional software features by sending a print file. You can install features on multiple printers by sending a formatted **.csv** file as a print job to the printers. A Xerox representative creates this file and provides installation instructions.

Installing a Software Feature at the Control Panel

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **Device Settings > General > Feature Installation**.
3. Touch **Enter Feature Installation Key**, then type the key.

4. Touch **OK**.

Initial Setup in the Embedded Web Server

Restricting Access to the Printer

You can lock or unlock the printer by selecting preset services and tools permissions for non-logged-in users. For details about roles and user permissions, refer to Setting Access Rights.

1. In the Embedded Web Server, click **Properties > Login/Permissions/Accounting**.
2. Click **User Permissions**.
3. For User Permission Roles, click **Edit**.
4. For Permission Role, for Non-Logged-User, click **Edit**.
5. For Print Feature, select the desired option, then click **Edit**.

Setting Permissions for When Users Can Print

1. For Allow Printing, select **When Users Can Print**, then select an option.
   - **Always**: This option allows printing at any time. There are no time restrictions.
   - **Monday – Friday from**: This option allows printing on weekdays. To set the printing times, use the From Time and To Time menus.
   - **Time of Day (Advanced)**: This option allows printing on specific days, during a specific time range. To set the printing days, use the From Time and To Time menus. To select the printing times, click **Add Time Range**. To delete, click the Trash icon.
   - **Never**: This option restricts all printing.
2. To specify permissions for Color and Black and White printing independently, select **Make color printing more restrictive than black & white** printing.
3. Click **Save**.

   Note: Not all options listed are supported on all devices. Some options apply only to a specific device model, configuration, operating system, or driver type.

Setting 1-Sided Print Permissions

1. On the 1-Sided Printing page, under Role State, select **Not Allowed** to require users to print 2-sided.
2. Click **Save**.

Setting Job Type Print Permissions

1. Under Presets, select an option:
   - **Allow all Job Types** allows users to print any job type.
   - **Only Allow Secure Print** ensures that users only send Secure Print jobs.
   - **Custom** allows you to select the job types that users are allowed to send.

   If you selected Custom, under Role State, next to each job type, to restrict users from using the job type, select **Not Allowed**.
2. To lock all job types, click the **Lock** icon. To unlock all job types, click the **Unlock** icon.

3. Click **Save**.

Setting Paper Tray Print Permissions

1. To restrict users from using a paper tray, under Role State, next to the paper tray, select **Not Allowed**.
2. To lock all job types, click the **Lock** icon. To unlock all job types, click the **Unlock** icon.
3. Click **Apply**.

Setting Application Print Permissions

1. For Applications, click **Edit**.
2. Select an application.

   Note: To add an application to the list, click **Add New Application**, or submit a print job from that application to the printer.

3. To restrict users from using a printing method, for the printing method, select **Not Allowed**.
4. Click **Apply**.

Using the Configuration Overview Page

The Configuration Overview page contains links to the commonly accessed pages on the Properties tab. Use the Configuration Overview page to help you install your printer successfully.

1. In the Embedded Web Server, click **Properties > Configuration Overview**.
2. Select an option:
   - To open the Configuration Checklist page, click **View Checklist**.
   - To open the settings page for an app or feature, for the desired app or feature, click **Settings** or **Setup**.
   - To create a clone file, for Cloning, click **View**. Cloning allows you to save your current printer settings to a file to use as a backup and restore file for your printer. You can also use a clone file to copy your printer settings to other printers.

Assigning a Name and Location to the Printer

The Description page displays the printer model information and product code or serial number. It also provides a place to assign a name and location to the printer. Asset tags let you enter unique identifiers for inventory management.

1. In the Embedded Web Server, click **Properties > Description**.
2. For Device Name, type a name for the device.
3. For Location, type the location of the device.

   Note: This location appears in the list of devices on your network. Use a meaningful location name, such as a building name or number, floor, and quadrant. A meaningful location name helps users know where the device is located within your organization.

4. For Customer Asset Tag and Xerox® Asset Tag, type unique identifiers as needed.

5. For Organization Information, type the Name and Unit for your organization, as needed.
6. For Geographic Location, type the latitude and longitude coordinates for the geographical location of the device.
7. Click **Apply**.

Selecting Services to Appear on the Touch Screen

A standard app is installed on the device by default. Optionally, you can install EIP and weblet apps, which provide extra functionality. For details, refer to Weblet Management.

Specify the Apps to Display on the Touch Screen

To specify the apps to display on the touch screen:

1. In the Embedded Web Server, click **Properties > Apps > Display**.
2. Click **Show/Hide**.
   - To select all apps in the list to appear on the touch screen, click **Show All**.
   - To hide all apps in the list so that no apps appear on the touch screen, click **Hide All**.
   - To select individual apps to appear on the touch screen, for Displayed, select the apps that you want to appear.
3. Click **Apply**.

   Note: You cannot hide apps that are required for basic device operation.

Arranging the Order that Apps Appear on the Touch Screen

To arrange the order that apps appear on the touch screen:

1. In the Embedded Web Server, click **Properties > Apps > Display**.
2. Click **Order**.
3. To arrange the order that apps appear on the control panel, click, drag, then drop the buttons in the preferred order.
4. Click **Apply**.

Installing Optional Software Features

When you purchase an optional software feature, to enable it, provide a feature installation key. Some features come with an activation code that you use to request a feature installation key. Go to the Xerox® Software Activation Portal website at www.xeroxlicensing.xerox.com/fik/ to enter the activation code. The website generates a feature installation key that you can use to enable the feature.

You can also install optional software features by sending a print file. You can install features on multiple printers by sending a formatted **.csv** file as a print job to the printers. A Xerox representative creates this file and provides installation instructions.

Installing a Software Feature in the Embedded Web Server

1. In the Embedded Web Server, click **Properties > General Setup**.
2. Click **Feature Installation**.
3. For Feature Installation Key Entry, click **Enter Installation Key**, or for the feature you want to install, click **Install**.
4. Type the key.
5. Click **Apply**.

Supplies Plan Activation Code

Your Xerox® equipment supplier offers supplies and service plans such as PagePack® and eClick®.

PagePack® and eClick® are cost-per-page-based programs that include all service and supplies for your device in one contract. If you have enrolled in a supplies program, you must activate the supplies plan at regular intervals. To enable your device for your purchased plan, or to get a Supplies Activation Code, contact your Xerox® equipment supplier with the device serial number.

1. In the Embedded Web Server, click **Properties > General Setup**.
2. Click **Supplies Plan Activation Code**.
3. Type the code, then click **Apply**.

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

Physical Connection Settings

You can specify Ethernet and USB settings, such as Ethernet Rated Speed, USB Connection Mode, and Print Timeout for USB printing.

Setting Ethernet Options

The Ethernet interface on the printer automatically detects the speed of your network. Any auto-sensing devices connected to the network, such as a hub, do not always detect the correct speed. Refer to the Configuration Report to ensure that the printer detects the correct network speed.

1. In the Embedded Web Server, click **Properties > Connectivity > Setup**.
2. For Wired Connection, click **Edit**.
3. To configure Ethernet settings, for Ethernet, click **Edit**.
4. For Rated Speed, select a connection speed.
5. Click **Save**.

   Note: For the new settings to take effect, restart your printer.

Configuring USB Connection Mode

1. In the Embedded Web Server, click **Properties > Connectivity > Setup**.
2. For USB Connection Mode, select **Edit**.

3. For USB Connection, select an option:
   - **Software Tools**: This option disables Direct Printing via Driver. If you use Xerox® Copier Assistant, select this option. Xerox representatives also use this feature to connect directly to the printer and use diagnostic software and other utilities.
   - **Direct Printing via Driver**: This option allows your computer to connect to the printer using a USB cable.
4. For Print Timeout, type the amount of time in seconds that the printer waits inactive before it disconnects from a device that is connected to the port. Type **0** to disable the timeout.
5. Click **Save**.

Changing the System Administrator Password

After you configure the printer, it is recommended that you change the default system administrator password. The user name is **admin**. The default password is **1111**.

Note:

- Ensure that you store the administrator password in a secure location.
- To avoid using the default administrator account, you can create a number of user accounts with administrator access.

1. In the Embedded Web Server, click **Properties > Security**.
2. Click **Password Policies > Admin Password**.
3. Type the old password.
4. Type the new password, then retype the new password.
5. The check box for Do not prompt to change admin password when set to factory default is clear by default. The clear check box ensures that when an administrator logs in or logs out, a reminder prompt appears to change the administrator password. To disable the reminder prompt, select the check box.
6. Click **Apply**.

Changing the System Administrator Password at the Control Panel

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **Security Settings > Change Admin Password**.
3. To change the password, type the old password.
4. Type the new password, then retype the new password.
5. Touch **OK**.

Setting the Date and Time

Setting the Date and Time in the Embedded Web Server

1. In the Embedded Web Server, click **Properties > General Setup**.
2. Click **Date and Time**.
3. For Date and Time Setup, select an option:
   - **Automatic using NTP**: This option allows the NTP service to set the time automatically.
   - **Manual (NTP Disabled)**: This option allows you to set the date and time manually.
4. If you are using an NTP server, select the address type. Options are **IPv4 Address** or **Host Name**. Type the appropriately formatted address, alternate address, and port numbers. The default port number is 123.

   Note: Changes to these settings cause the printer to restart.
5. Select the date and time format, then type the date and time in the appropriate fields. To show the time in 24-hour format, select the **Display 24 hour clock** check box.
6. For Time Zone, select your time zone from the menu.
7. To test connectivity to the NTP server, click **NTP Destination Test**.

   If the test succeeds, a confirmation message appears.

   If the test fails, an error message appears. Verify the NTP server settings, then repeat the test. For details, refer to NTP.
8. Click **Apply**.

Setting the Date and Time at the Control Panel

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **Device Settings > General > Date and Time**.

   Note: If this feature does not appear, log in as a system administrator. For details, refer to Logging In as the System Administrator at the Control Panel.
3. To set the time zone, touch **Time Zone**, touch the **Geographic Region** list, then touch your region. Use the **Up** or **Down** arrows to navigate and select your Time Zone.

   Note: The date and time are set automatically through Network Time Protocol (NTP). To modify these settings, access the Embedded Web Server, then select the Properties tab. Change the Date and Time Setup to **Manual (NTP Disabled)**.
4. To set the date:
   a. Touch **Date**.
   b. Touch the **Year** field. To select a number, use the arrows.
   c. Touch the **Month** field. To select a number, use the arrows.
   d. Touch the **Day** field. To select a number, use the arrows.

   e. Touch **Format**, then touch the date format that you want to use.

5. To set the time:

   a. Touch **Time**

   b. To specify the 12-hour or 24-hour format, touch **Display 24 hour Clock**.

   c. Touch the **Hours** field. To select a number, use the arrows.

   d. Touch the **Minutes** field. To select a number, use the arrows.

   e. If your printer is set to display the 12-hour clock, touch **AM** or **PM**.

6. Touch **OK**.

3

Network Connectivity

This chapter contains:

Connecting to a Wireless Network

If you have purchased the Wireless Network Adapter, you can use the Wireless Wizard to connect to a wireless network. If the device is connected to a wired network, you can configure wireless settings in the Embedded Web Server.

Before you begin, purchase the Xerox® Wireless Network Adapter.

Note:

- For more information, refer to the Xerox® Wireless Network Adapter Kit Hardware Install and Setup instructions that are included with the kit.
- The device uses either the wireless or the wired network connection. Activating one network connection deactivates the other network connection.
- When you switch from a wired connection to a wireless connection, the IP address of the printer changes. The connection to the Embedded Web Server through your Web browser closes. To reconnect to the Embedded Web Server, in the Web browser address field, type the new IP address or host name of your printer. For details, refer to Verifying the Wireless Status and Viewing the Wireless IP Address.

Connecting to a Wireless Network Using the Wireless Wizard

You can use the Wireless Wizard to simplify the process of connecting your device to an available wireless network. You can use the Wireless Wizard to select a different wireless network or to connect to a wireless network manually.

Note:

- Advanced enterprise networks require certificates. For details, refer to Security Certificates.
- When you plug in the Wireless Network Adapter, Wi-Fi Direct is available immediately. For details, refer to Wi-Fi Direct.

To connect to a wireless network using the Wireless Wizard:

1. Plug the wireless network adapter directly into an active USB port on the device.
2. Select an option.
   - If you are connecting the device to a wireless network for the first time, touch **Continue Wireless Install**.
   - If you have connected the device to a wireless network previously, that network appears on the screen. Select an option:
     - To connect to the last network used, which is shown on the screen, touch **Activate Wireless**.
     - To connect to another network, touch **Pick New Network**.
3. Log in as an administrator. For details, refer to Accessing Administration and Configuration Settings.

4. Select a wireless network from the list.
   - If you are joining a secure network, the secure settings appear.
     - If the security settings require a user name, touch **User Name**, type the user name, then touch **Done**.
     - Touch **Password**, type the password, then touch **Done**.
     - Touch **Join**.
   - If you are joining an unsecured network, to confirm joining the network, touch **Join this Network**.

   Note: If your network does not appear, select an option.

   - To refresh the wireless networks list, touch **Check for Networks**.
   - To join the network manually, touch **Manual Setup**. For details on manual setup, refer to Configuring Wireless Settings Manually.
5. Touch **Done**.

   Note: If the connection fails, select **Edit Connection**, **Pick New Network**, or **Use Wired Connection**.

Connecting to a Wireless Network in the Embedded Web Server

1. In the Embedded Web Server, click **Properties > Connectivity > Setup**.
2. For Xerox® Wireless Network Interface, click **Edit**.

   Note: After you install the Wireless Network Adapter, the Edit button appears.
3. To configure IPv4, IPv6, and DNS settings, on the Wireless Profile page, for IP, click **Edit**. Configure settings as needed, then click **Apply**. The device uses separate IP settings for wired and wireless network connections. For details, refer to IP.
4. On the Wireless Profile page, for Wireless Settings, click **Edit**.
5. If your device is connected to a wireless network, on the Wireless Settings page, click **Select Different Network**.
6. On the Wireless Settings page, click **Scan for Available Networks**. A list of detected networks appears.
7. For the SSID name of the network that you want to join, click **Select & Configure**.

8. The device detects the security mode that your network uses. Configure the following security mode settings, as needed.
   - For WEP Settings and Key String Type, select the bit strength and key.
   - For Encryption Algorithm, select an encryption method. Auto detects the algorithm that your wireless network uses automatically.
   - For Authentication Method, select the authentication method that your wireless network uses.
   - To require the device to validate certificates, for Server Validation - Validate server using, select the certificate that you want to use.
     - Install the validation server root certificate on the Security Certificates page.
     - To access the Security Certificates page, click **Properties > Security > Security Certificates**.

     For details, refer to Security Certificates.
   - For Device Certificate (TLS) - Authentication Certificate, select the device certificate that you want to use.

     Install the device certificate on the Security Certificates page at **Properties > Security > Security Certificates**.

     For details, refer to Security Certificates.
   - For Outer Identity, configure the external User ID.
   - For User Name, type the user name that the device uses to access the wireless network.
   - For Password, type and confirm a password. Click **Select to save new password**, as needed.
9. Click **Save**.
10. Navigate back to the Setup page, then click **Properties > Connectivity > Setup**.
11. For Xerox® Wireless Network Interface, click **Make Active**.

Verifying the Wireless Status and Viewing the Wireless IP Address

To verify the wireless status and view the wireless IP address, print a Configuration Report. For details, refer to Configuration Report. Note the Connectivity Physical Connections, Connectivity Protocols, and TCP/IPv4 sections of the report.

Configuring Wireless Settings Manually

If the device does not detect your wireless network, configure wireless settings manually and provide information about your wireless network.

Configuring Wireless Settings Manually at the Control Panel

To configure wireless settings manually at the control panel:

1. Ensure that the Wireless Network Adapter is installed in an active USB port.
2. At the device control panel touch screen, log in as an administrator. For details, refer to Accessing the Control Panel as a System Administrator.

3. Touch **Device > Tools > Network Settings > Network Connectivity > Wireless**.

   The Wireless Wizard opens. For details on using the Wireless Wizard, refer to Connecting to a Wireless Network Using the Wireless Wizard.

4. Select an option.
   - If you are connecting the device to a wireless network for the first time, touch **Continue Wireless Install**.
   - If you have connected the device to a wireless network previously, touch **Pick New Network**.

5. At the bottom of the list of available networks, touch **Manual Setup**.

6. On the SSID screen, type the network name, then touch **Done**.

7. Touch **Security**, then select the security method that your wireless network uses.

8. Configure the following security mode settings as needed.
   - For Encryption Algorithm, select an encryption method. Auto automatically detects the algorithm that your wireless network uses.
   - For Authentication Mode, select the authentication method that your wireless network uses.
   - For User Name, type the user name that the device uses to access the wireless network.
   - For Password, type a password, then touch **Done**.

9. Touch **Join**.

10. Touch **Done**.

    Note: For detailed IP settings and security settings, use the Embedded Web Server.

Configuring Wireless Settings Manually in the Embedded Web Server

To configure wireless settings manually in the Embedded Web Server:

1. In the Embedded Web Server, click **Properties > Connectivity > Setup**.

2. For Xerox® Wireless Network Interface, click **Edit**.

3. To configure IPv4, IPv6, and DNS settings, on the Wireless Profile page, for IP, click **Edit**. The printer uses separate IP settings for wired and wireless network connections. For details, refer to IP.

4. On the Wireless Profile page, for Wireless Settings, click **Edit**.

5. If your device is connected to a wireless network, on the Wireless Settings page, click **Select Different Network**.

6. On the Wireless Settings page, click **Join Other Network**.

7. For Network Name, type the name of your network.

8. For Security Mode, select the security method that your wireless network uses.

9. Configure the following security mode settings, as needed.
   - For WEP Settings and Key String Type, select the bit strength and key.
   - For Encryption Algorithm, select an encryption method. Auto detects the algorithm that your wireless network uses automatically.
   - For Authentication Method, select the authentication method that your wireless network uses.
   - To require the printer to validate certificates, for Server Validation - Validate server using, select the certificate that you want to use.

     Install the validation server root certificate on the Security Certificates page at **Properties > Security > Certificates > Security Certificates**.

     For details, refer to Security Certificates.
   - For Device Certificate (TLS) - Authentication Certificate, select the device certificate that you want to use.

     Install the device certificate on the Security Certificates page at **Properties > Security > Certificates > Security Certificates**.

     For details, refer to Security Certificates.
   - For Outer Identity, configure the external User ID.
   - For User Name, type the user name that the device uses to access the wireless network.
   - For Password, type and confirm a password.
   - Click **Select to save new password**, as needed.
10. Click **Save**.
11. Navigate back to the Setup page, then click **Properties > Connectivity > Setup**.
12. For Xerox® Wireless Network Interface, click **Make Active**.

Connecting Directly to a Wireless Network

Before you begin, purchase and install the Xerox® Wireless Network Adapter.

1. Ensure that the printer is not connected to a wired Ethernet network.
2. Restart the printer.
3. Refer to the Configuration Report to find the self-assigned IP address of the printer, in the 169.254.x.x range. For details, refer to Printing the Configuration Report.
4. Using an Ethernet cable, connect a computer to the printer.

   Note:

   - Depending on your computer hardware, use a crossover cable or adapter as needed.
   - Ensure that wireless connectivity is disabled on your computer.
5. Find the IP address of the computer.
6. Ensure that the computer obtains an automatic private IP address, in the 169.254.x.x range, and is therefore on the same subnet as the printer.
7. On the computer, access the Embedded Web Server. Type the IP address of the printer in the address field of a Web browser, then press **Enter** or **Return**.

8. Configure wireless settings in the Embedded Web Server. For details, refer to Connecting to a Wireless Network.

   Note: When you switch from a wired connection to a wireless connection, the IP address of the device changes. The connection to the Embedded Web Server through your Web browser closes. To reconnect to the Embedded Web Server, in the Web browser address field, type the new IP address or host name of your device.

Wi-Fi Direct

Wi-Fi Direct enables devices to connect with each other without requiring a wireless access point. The printer acts as a Software Access Point (SoftAP), and manages the Wi-Fi Direct connections and security.

Wi-Fi Direct does not require manual configuration. The Wi-Fi Direct Protected Setup (WPS) Name and subnet address prefix generate automatically. Wi-Fi Direct uses WPS and WPA2 encryption to create a secure wireless network. The printer supports AirPrint and Mopria using Wi-Fi Direct connections.

Before you set up Wi-Fi Direct, ensure that you have the wireless network interface enabled on your device. For information, refer to Connecting to a Wireless Network. To use the Wi-Fi Direct connection to the printer, users have to enable Wi-Fi Direct on their mobile devices.

Configuring Wi-Fi Direct

If you configured your device to use default settings, no further Wi-Fi Direct feature configuration is required.

1. In the Embedded Web Server, click **Properties > Connectivity > Setup**.
2. In the Profile area, for Wi-Fi Direct, click **Edit**.
3. To enable Wi-Fi Direct, in the Settings area, for Wi-Fi Direct, select **Enabled**.
4. To create a password, for Wi-Fi Direct Access Point — SSID Password, type a password.
5. To configure the password to appear on the printer control panel, select **Show password on the device touch screen in Device App**.
6. To modify the Wi-Fi Protected Setup (WPS) Name, in the Convenience Link area, for Device Name, select **Edit**.
   If the Device Name field is blank, the Wi-Fi Protected Setup (WPS) Name field displays a default value. If you change the Device Name, the Wi-Fi Protected Setup (WPS) Name field displays the Device Name information.
7. To modify the Subnet Address Prefix, type the Subnet Address Prefix.

   Note: You do not have to modify the Subnet Address Prefix unless your network environment already uses the default address.
8. Click **Apply**.

Verifying HTTP Settings for Wi-Fi Direct

After you configure the Wi-Fi Direct feature, verify that the HTTP settings are correct:

1. In the Embedded Web Server, click **Properties > Connectivity > Setup**.
2. Confirm that the Wi-Fi Direct feature is enabled.
3. For Force Traffic over Secure Connection (HTTPS), select **No (Requests can be made over HTTP and HTTPS)**.
4. Click **Save**.

Disabling Wi-Fi Direct

1. In the Embedded Web Server, click **Properties > Connectivity > Setup**.
2. In the Profile area, for Wi-Fi Direct, click **Edit**.
3. To disable Wi-Fi Direct, in the Settings area, for Wi-Fi Direct, clear the check box for **Enabled**.
4. Click **Apply**.

AirPrint

AirPrint is a software feature that allows you to print documents from Apple iOS-based mobile devices and Mac OS-based devices without a print driver. AirPrint-enabled printers allow you to print or fax directly from a Mac or from an iPhone, iPad, or iPod touch. You can use AirPrint to print from a wired or wireless device directly without using a print driver. You can also use AirPrint to scan from a printer to supported Apple devices.

Note:

- Not all applications support AirPrint.
- When AirPrint is enabled, HTTP, IPP, and Multicast DNS are enabled automatically.
- IPP enablement requires a Web server reset.
- The device that submits the AirPrint job must be on the same subnet as the printer. To allow devices to print from different subnets, configure your network to pass multicast DNS traffic across subnets.
- Supported mobile devices: all models of iPad, iPhone 3GS or later, and iPod touch third generation or later, running the latest version of iOS.
- If AirPrint is not available on your device, contact your Xerox representative.

Configuring AirPrint

1. In the Embedded Web Server, click **Properties > Connectivity > Setup**.
2. For Mobile Workflows, for AirPrint, click **Edit**.
3. Configure HTTP, IPP, and Multicast DNS Registration as required. To configure a protocol, click **Edit**.
4. To enable AirPrint, for Enablement, select one or both options:
   - **Allow Printing/Faxing to be initiated From AirPrint Supported Devices**
   - **Allow Scanning to be initiated From AirPrint (or Mopria) Supported Devices**

   Note:

   - AirPrint Faxing is supported only on devices that have embedded fax enabled and are configured to allow sending.
   - AirPrint Printing/Faxing is enabled by default.
   - To require authentication for AirPrint Printing and Faxing, configure IPP authentication. For details, refer to IPP.
   - Enabling scanning for AirPrint, also enables scanning for Mopria.

5. For Require Authentication for Scanning, select an option:
   - **Off**: This option allows the device to scan without requiring authentication.
   - **HTTP Basic**: This option authenticates with user accounts that are configured in the device user database or in the network database.

     Note: HTTP Basic sends user login credentials as plain, unencrypted text over HTTP. To send encrypted login credentials, use HTTPS.

   - **HTTP Digest**: This option authenticates with user accounts that are configured in the device user database. HTTP Digest uses encrypted user login credentials over HTTP or HTTPS. HTTP Digest is always encrypted. It is the most secure option. HTTP Digest is available when Scanning is enabled and when FIPS 140-2 is configured as follows:
     - FIPS 140-2 is disabled.
     - FIPS 140-2 is enabled with HTTP Digest indicated as an exception. For details, refer to FIPS 140-2.
6. If you selected HTTP Basic authentication, for Validation Location, select an option:
   - **Validation on the Device**: This option enables IPP authentication of user accounts that are configured in the device user database. For details, refer to Device User Database.
   - **Validation on the Network**: This option enables IPP authentication of user accounts that are configured on the network authentication server for the device.

   Note: The same network authentication configuration is used on the printer for each login method that is configured for Network Authentication.
7. To edit the device name or location, for Device Name, Device Location, or Geographic Location, click **Edit**.

   Note: Providing a device name can help users identify the device.
8. Click **Save**.

   Note: To use AirPrint with accounting, you can create IPP accounting exceptions. For more information, refer to Configuring Validation Policies and Print Job Exceptions.

Mopria

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

Configuring Mopria

1. In the Embedded Web Server, click **Properties > Connectivity > Setup**.
2. For Mobile Workflows, for Mopria Discovery, click **Edit**.
3. To configure HTTP, HTTPS, IPP, Multicast DNS Registration, or NFC as needed, for each protocol, click **Edit**.
4. For Mopria Discovery, select **On**.
5. For Enablement, select one or both options.
   - **Allow Printing to be initiated From Mopria Supported Devices**
   - **Allow Scanning to be initiated From Mopria Supported Devices**

     Note: Enabling scanning for Mopria also enables scanning for AirPrint.
6. For Require Authentication for Scanning, select an option.
   - **Off**: This option allows the device to scan without requiring authentication.
   - **HTTP Basic**: This option authenticates with user accounts that are configured in the device user database or on the network.

     Note: HTTP Basic sends user login credentials as plain, unencrypted text over HTTP. For sending encrypted login credentials, use HTTPS.
   - **HTTP Digest**: This option authenticates with user accounts that are configured in the device user database. HTTP Digest uses encrypted user login credentials over HTTP or HTTPS.

     Note:

     - HTTP Digest is always encrypted. It is the most secure option.
     - HTTP Digest is available when Scanning is enabled and FIPS 140-2 is disabled. HTTP Digest is also available when FIPS 140-2 is enabled with HTTP Digest indicated as an exception. For details, refer to FIPS 140-2.
7. If you selected HTTP Basic authentication, for Validation Location, select an option.
   - **Validation on the Device:** This option enables IPP authentication of user accounts that are configured in the device user database. Refer to User Database.
   - **Validation on the Network**: This option enables IPP authentication of user accounts that are configured on the network authentication server for the device.

   Note: The same network authentication configuration is used on the printer for each login method that is configured for Network Authentication.
8. To edit the device name, for Device Name, click **Edit**.

   Note: Providing a device name can help users identify this device.
9. Click **Save**.

USB Settings

You can use USB Settings to configure the following:

- USB Connection Mode and the print timeout value
- USB Port State in Sleep Mode

Configuring USB Connection Mode

1. In the Embedded Web Server, click **Properties > Connectivity > Setup**.
2. For USB Connection Mode, select **Edit**.
3. For USB Connection, select an option:
   - **Software Tools**: This option disables Direct Printing via Driver. If you use Xerox® Copier Assistant, select this option. Xerox representatives also use this feature to connect directly to the printer and use diagnostic software and other utilities.
   - **Direct Printing via Driver**: This option allows your computer to connect to the printer using a USB cable.
4. For Print Timeout, type the amount of time in seconds that the printer waits inactive before it disconnects from a device that is connected to the port. Type **0** to disable the timeout.
5. Click **Save**.

Configuring USB Port State in Sleep Mode

The USB Port State in Sleep Mode feature controls power supply to USB (Type A) accessories when the device is in Sleep Mode. To remain active, accessories, such as Xerox® Wireless Network Adapter and USB card readers, require that power is maintained to the USB port in sleep mode.

To configure USB Port State Sleep Mode in the Embedded Web Server:

1. In the Embedded Web Server, click **Properties > Connectivity > Setup**.
2. For USB Port State in Sleep Mode, select **Edit**.
   - To permit USB accessories to operate during Sleep Mode, select **Powered**.

     Note: The Powered option can cause an increase in power consumption during Sleep Mode.
   - To disconnect power from USB accessories during Sleep Mode, select **Not Powered**.

     Note: When wireless networking is active on the device, you cannot disconnect power from USB accessories. The Not Powered option is not available.
3. Click **Save**.

Enabling USB Port State Sleep Mode at the Control Panel

To enable USB Port State Sleep Mode at the control panel:

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **Network Settings > USB Settings**.
3. Touch **USB Port State in Sleep Mode**.

4. For Power USB Port in Sleep Mode, select the toggle button.

   Note: A check mark on the toggle button indicates Enabled.

5. Touch **OK**.

USB Port Security

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

Enabling or Disabling USB Ports

1. In the Embedded Web Server, click **Properties > Security**.
2. Click **USB Port Security**.
3. To enable a USB port, for the port, select **Enabled**. To disable the port, clear the check box.
4. Click **Save**.

   Note:

   - If USB ports are disabled, you cannot use a USB card reader for authentication, update the software, or print from a USB Flash drive.
   - If your device model has a cover for the USB port on the control panel, you can install or remove the cover. You can find the installation instructions and the USB cover in the compartment inside Tray 1.
   - Only Type A ports can be enabled or disabled. These settings do not affect Type B ports.

Enabling or Disabling all USB Ports at the Control Panel

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **Security Settings > USB Port Security**.
3. To enable or disable the USB ports, touch **Enabled** or **Disabled**.
4. Touch **OK**.

FTP/SFTP Filing

File Transport Protocol (FTP) is a standard network protocol used to pass and manipulate files over a TCP/IP network. Several services running on your printer, including Network Scanning, Saved Jobs Backup, and Software upgrade can use FTP as a filing service.

Secure FTP (SFTP) is a standard network protocol that is used with SSH to ensure that data is encrypted and transferred securely.

Configuring FTP and SFTP Filing Settings

1. In the Embedded Web Server, click **Properties > Connectivity > Setup**.
2. For Protocol, for FTP/SFTP Filing, click **Edit**.
3. To configure FTP or SFTP filing settings for each app listed under Within Apps, click the link.
4. For Mode, select an option:
   - **Passive**: This option transfers data over a random port specified by the FTP server from a connection made from the printer.
   - **Active**: This option transfers data over a fixed, known port from a connection made from the server.
5. Click **Save**.

HTTP

Hypertext Transfer Protocol (HTTP) is a request-response standard protocol between clients and servers. Clients that make HTTP requests are called User Agents (UAs). Servers that respond to these requests for resources, such as HTML pages, are called Origin Servers. There can be any number of intermediaries, such as tunnels, proxies, or gateways between User Agents and Origin Servers.

Enabling HTTP at the Control Panel

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **Network Settings > Advanced Settings**.
3. Touch **HTTP Settings**.
4. Touch **Enabled**, then touch **OK**.
5. To apply the settings, touch **Finish**.

   Note: HTTP is enabled by default.

Configuring HTTP Settings in the Embedded Web Server

1. In the Embedded Web Server, click **Properties > Connectivity > Setup**.
2. In the Protocol area, for HTTP, click **Edit**.
3. For Connection, select **Enabled**.

   Note: HTTP is enabled by default. If you disable HTTP, then the Embedded Web Server is no longer available.

4. Type a connection port number as needed. The default is 80.
5. To encrypt HTTP communication, for Force Traffic over Secure Connection (HTTPS), select **Yes**. When Force Traffic over Secure Connection (HTTPS) is enabled, all Web pages contain https:// in the URL.

   Note: By default, the device accepts jobs submitted over both HTTP and HTTPS. Force Traffic over Secure Connection (HTTPS) is disabled.

6. Change the HTTPS Port Number as needed. The default is 443.
7. For Keep Alive Timeout, type a time up to 60 seconds. The printer waits the specified amount of time before it terminates the connection.

   Note: Increasing the Keep Alive Timeout can cause slower connections.

8. For Choose Device Certificate, select a certificate.

   Note: To install more device certificates, refer to Security Certificates.

9. To view the selected certificate details, or save the certificate to your computer, click **View/Save**.

   Note: If you are using the Xerox® Default Device Certificate, you can install the Device Root Certificate Authority in your Web browser. Installing the Device Root Certificate Authority ensures that your browser trusts the printer.

10. To download the certificate authority, click **Download the Device Root Certificate Authority**.
11. Click **Save**.

Accessing HTTP Web Services

To access the HTTP Web Services page, from the HTTP page, click **Web Services**.

HTTP Web Services

You can enable or disable Web Services on the Web Services page. This page provides a list of all available Web services on your printer, and displays the configuration status of each service.

- To disable a Web service, clear the check box next to the Web service name.
- To view Web service port numbers or to remove login restrictions, click **Advanced Settings**.

For more information about Xerox Extensible Interface Platform® and Web services, see the documentation included in the Xerox Extensible Interface Platform® Software Development Kit (SDK). For information on how to download the SDK, go to www.xerox.com/en-us/office/eip.

Accessing HTTP Advanced Settings

To access the HTTP Web Services Advanced Settings page, from the HTTP page, click **Web Services > Advanced Settings**.

HTTP Advanced Settings

The Advanced Web Services page displays all services currently enabled on the printer and their port numbers.

To remove all login restrictions for web services on the printer, under Web Services IP Lockout, click **Clear Lockout**.

IP

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

Enabling TCP/IP

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **Network Settings > TCP/IP Settings**.
3. Touch **TCP/IP Enablement**.
4. For IPv4 or IPv6, touch **Enabled**, then touch **OK**.
5. To apply the settings, touch **Finish**.

   Note: By default, IPv4 is enabled. If you disable IPv4, before you can access the Embedded Web Server, enable IPv4 or IPv6 at the printer control panel. For details, refer to IP and HTTP.

Configuring the Network Address Manually at the Control Panel

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **Network Settings > TCP/IP Settings**.
3. Touch **Dynamic Addressing**.
4. Touch **Disabled**, then touch **OK**.
5. Touch **IPv4**, then type the IPv4 Address, IP Gateway Address, and Network Mask Address. After each address, touch **OK**.
6. When you are finished, touch **OK**.
7. To apply the settings, touch **Finish**.

Configuring DNS Settings at the Control Panel

Domain Name System (DNS) is a system that maps host names to IP addresses.

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **Network Settings > TCP/IP Settings**.
3. Touch **DNS Configuration**.
   a. Touch **Host Name**.
   b. Type a host name.
   c. Touch **OK**.
   d. Touch **Close**.

      Note: If DHCP is enabled, your DHCP server can provide the Domain Name and the Requested Domain Name.

   e. Touch **Domain Name**.
   f. For Requested Domain Name, type the domain name.
   g. Touch **OK**.
   h. Touch **Close**.

4. Touch **DNS Servers**.
   a. Touch **Primary DNS Server**, type the server address, then touch **OK**.
   b. Touch **Alternate DNS Server #1**, type the server address, then touch **OK**.
   c. Touch **Alternate DNS Server #2**, type the server address, then touch **OK**.
   d. Touch **Close**.

   Note: If DHCP is enabled, you can configure the DHCP server to provide the DNS server IP addresses.

5. Touch **Close** again.
6. To apply the settings, touch **Finish**.

Configuring IP Settings in the Embedded Web Server

If your printer has a valid network address, you can configure TCP/IP settings in the Embedded Web Server. For details, refer to Assigning a Network Address.

Configuring IPv4

You can use IPv4 or IPv6 in addition to or in place of the other.

1. In the Embedded Web Server, click **Properties > Connectivity > Setup**.
2. For Network, next to a connection type, click **Edit**.

   Note: The device uses separate IPv4, IPv6, and DNS settings for wired and wireless network connections. Before you configure wireless IP settings, install the Xerox® Wireless Network Interface, then connect to a wireless network. For details, refer to Connecting to a Wireless Network.

3. For Configuration Settings, next to IP, click **Edit**.
4. To configure IPv4, click **Show IPv4 Settings**.
5. For Protocol, select **Enabled**.
6. For IP Address Resolution, select an option.
   - **BOOTP**: This option permits the device to obtain an IP address from a BOOTP server that does not respond to DHCP requests.
   - **DHCP**: This option permits the device to obtain an IP address from a DHCP server. This option permits the printer to obtain an IP address from a BOOTP server that is configured to accept DHCP requests. The printer requests that the server register the IP address and hostname of the printer with the DNS server.
   - **STATIC**: This option disables dynamic addressing and allows you to type a static IP address. Type a Machine IP Address, Subnet Mask, and Gateway Address.

7. For Broadcast, select **Enabled** as needed.

   Note: If the device does not obtain an IP address from a DHCP/BOOTP server, enable broadcast. Enable broadcast when your DHCP/BOOTP server is on a different subnet than the device and communicates through a relay agent router.

8. For Zero-Configuration Networking, for Self Assigned Address, select **Enabled** as needed. This option instructs the device to assign itself an address when a DHCP server does not provide one.
9. Click **Apply**.

   Note: If you select Default All, the device sets the IPv4, IPv6, and DNS values as the default settings.

Configuring IPv6

IPv6 hosts can configure themselves automatically when connected to a routed IPv6 network using the Internet Control Message Protocol Version 6 (ICMPv6). ICMPv6 performs error reporting for IP along with other diagnostic functions. When first connected to a network, a host sends a link-local multicast router solicitation request for configuration parameters. If suitably configured, routers respond to this request with a router advertisement packet containing network-layer configuration parameters.

1. In the Embedded Web Server, click **Properties > Connectivity > Setup**.
2. For Network, for a connection type, click **Edit**.

   Note: The device uses separate IPv4, IPv6, and DNS settings for wired and wireless network connections. Before you configure wireless IP settings, install the Xerox® Wireless Network Interface, then connect to a wireless network. For details, refer to Connecting to a Wireless Network.

3. For Configuration Settings, for IP, click **Edit**.
4. To configure IPv6, click **Show IPv6 Settings**.

   Note: If both IPv4 and IPv6 are disabled, you cannot access the Embedded Web Server. To access IPv4 and IPv6 settings in the Embedded Web Server, at the device control panel, enable IPv4, IPv6, or both. If you disable IPv4 and IPv6 or change the IP addresses, any dependent protocols are disabled.

5. For Protocol, select **Enabled**.
6. To allow the router to assign address prefixes, for Stateless Addresses, select **Use Router Supplied Prefixes**.
7. To select how DHCP operates for IPv6, for Default Dynamic Host Configuration Protocol (DHCP) Settings, select an option.
8. To enter the address manually, for Manual Address Options, select **Enable Manual Address**.
9. From the menu, select a router prefix, or type a new router prefix, then click **Add**.
10. To save the new settings, click **Apply**.

Configuring DNS

Domain Name System (DNS) is a system that maps host names to IP addresses.

1. In the Embedded Web Server, click **Properties > Connectivity > Setup**.
2. For Network, for a connection type, click **Edit**.

   Note: The printer uses separate IPv4, IPv6, and DNS settings for wired and wireless network connections. Before you configure wireless IP settings, install the Xerox® Wireless Network Interface, then connect to a wireless network. For details, refer to Connecting to a Wireless Network.

3. For Configuration Settings, for IP, click **Edit**.
4. To configure DNS, click **Show DNS Settings**.
5. For Requested Host Name, type a unique name for your printer. If the host name registers to the DNS server successfully, the host name appears as a Verified Host Name. The default host name is XRXxxx, where xxx is the MAC address of the printer.

   Note: If no host name appears for Verified Host Name, the host name did not register to the DNS server successfully. Configure your DHCP server to perform updates on behalf of the DHCP clients or enter DNS records manually.

6. For Requested Domain Name, type the name of the domain to which the printer is connected. If the domain name registers to the DNS server successfully, the domain name appears as a Verified Domain Name.

   Note: If no domain name appears for Verified Domain Name, the domain name did not register successfully to the DNS server. Configure your DHCP server to perform updates on behalf of the DHCP clients or enter DNS records manually.

7. To allow users to see and connect to the printer using Bonjour, for Multicast DNS Registration, select **Enabled**.
8. For Release this connection's DHCP leases and DNS registrations, select **Enabled** as needed. This option allows the printer to send a release request to the DHCP and DNS servers. If the servers grant the request, the servers release the current IP address and dynamic DNS names. The IP addresses and DNS names renew immediately and when the printer is turned off.
9. For Additional DNS Server Addresses, type addresses as needed. If you have a DHCP server, recognized addresses can appear in the DNS Server Addresses list if they were provided by the server.
10. For DNS Connection Timeout, type the time in seconds that the printer waits to connect to a DNS server. After the timeout period, the printer attempts to connect to any additional DNS servers.
11. To add the printer domain to the Domain Name Search List, for Append Device Domain, select **Enabled**.
12. To add the parent domains of the printer to the Domain Name Search List, for Append Parent Domains, select **Enabled**.
13. If you have a DHCP server, recognized search domain names can appear in the Domain Name Search List if they were provided by the server. The list of domain names allows the DNS server to recognize unqualified host names. If you want the printer to search for other domain names, for Additional Search Domains, enter the names.
14. To set the printer to use an IPv6 address before it uses an IPv4 address, select **Prefer IPv6 Address over IPv4**.
15. Click **Apply**.

IPP

Internet Printing Protocol (IPP) is a standard network protocol that allows you to print and manage jobs remotely. When IPP is configured, IPP authentication gives users the option to authenticate their identities using IPP through HTTP authentication methods. An IPP client can pass user credentials to the printer to use for authentication.

Configuring IPP

1. In the Embedded Web Server, click **Properties > Connectivity > Setup**.
2. In the Protocol area, for IPP, click **Edit**.
3. For IPP Enablement, select **On**.

   Note:

   - IPP enablement requires a Web server reset.
   - Enabling IPP authentication impacts AirPrint job submissions because AirPrint uses IPP.
4. To enable IPP authentication, for Authentication, select **HTTP Basic with Secure IPP (IPPS)**. This option authenticates to user accounts that are configured in the device user database or in the network database.

   Note: HTTP Basic is unencrypted, unless authentication credentials are sent using HTTPS.
5. If HTTP Basic with Secure IPP (IPPS) authentication is enabled, for Validation Location, select an option.
   - **Validation on the Device**: This option enables IPP authentication of user accounts that are configured in the device user database. For details, refer to User Database
   - **Validation on the Network**: This option enables IPP authentication of user accounts that are configured on the network authentication server for the device.
6. To configure Secure IPP Mode, select an option:
   - **IPP and Secure IPP (IPPS)**: This option allows the device to accept insecure IPP jobs and secure IPPS jobs. This option is the default setting.
   - **Secure IPP (IPPS) only**: This option allows the device to accept secure IPPS jobs only. If you select this option, IPPS is shown to users as an available option for jobs submitted using AirPrint. IPP is not shown as an available option.
7. You can edit configuration settings for HTTP, and the Device User Database or Authentication Server.
   - To edit HTTP settings, in the Configuration Settings area, for HTTP, click **Edit**.
   - To edit Device User Database settings, in the Configuration Settings area, for Device User Database, click **Edit**.

     Note: The Device User Database option is available only when HTTP Basic with Secure IPP (IPPS) is selected, and, for Validation Location, Validate on the Device is selected.
   - To edit Authentication Server settings, in the Configuration Settings area, for Authentication Server, click **Edit**.

     Note: The Authentication Server option is available only when HTTP Basic with Secure IPP (IPPS) is selected, and, for Validation Location, Validate on the Network is selected.

8. To configure the IPP identify printer functionality, for Identify Printer, select an option.
   - **On**: This option enables an IPP client to request the printer to identify itself through a graphic or sound.
   - **Off**: This option revokes the ability of an IPP client to request the printer to identify itself through a graphic or sound.

   Note: When the IPP client requests sound, the Identify Printer feature uses the Fault tone. You can configure the Fault tone on the printer control panel. For details, refer to the *System Administrator Guide*.

9. If Fax is supported and configured, you can configure Remote IPP FaxOut Log Display. To configure the Remote IPP FaxOut Log Display, select an option.
   - **On**: This option allows a remote user to view the IPP FaxOut Log.
   - **Off**: This option does not permit remote users to view the IPP FaxOut Log.
10. Click **Save**.

LDAP

Lightweight Directory Access Protocol (LDAP) is a protocol used to process queries and updates to an LDAP information directory, on an external server. LDAP can also be used for network authentication and authorization. LDAP directories are heavily optimized for read performance. Use this page to define how the printer retrieves user information from an LDAP directory.

Adding LDAP Server Information

The LDAP Server page displays the current LDAP servers configured for your printer. You can configure a maximum of nine LDAP servers for your printer.

To add an LDAP server:

1. In the Embedded Web Server, click **Properties > Connectivity > Setup**.
2. In the Protocol area, for LDAP, click **Edit**.
3. Click **Add New**.
4. For Server Information, select the preferred address type.
5. For Friendly Name, type a name for the LDAP server.
6. Type the appropriately formatted address or host name of your server, then change the default port number as needed.
7. Type the appropriately formatted address or host name of your backup server, then change the default port number as needed.
8. For LDAP Server, select an LDAP server type.
    - **Exchange**: This option is for use with Microsoft® Exchange.
    - **Domino**: This option is for use with Lotus Domino.
    - **ADS**: This option is for use with Microsoft® Active Directory Service.
9. Click **Apply**.

Managing LDAP Servers in the Embedded Web Server

1. In the Embedded Web Server, click **Properties > Connectivity > Setup**.
2. In the Protocol area, for LDAP, click **Edit**.
    - To edit an LDAP server configuration, in the Actions column of the server to edit, click **Edit**.
    - To copy an LDAP server configuration, select the server to copy, then click **Copy From**.
    - To delete all LDAP servers configured to your printer, click **Delete All**.
    - To enable SASL binds, click **LDAP Policies**.
3. Click **Close**.

Configuring LDAP Server Optional Information

1. In the Embedded Web Server, click **Properties > Connectivity > Setup**.
2. In the Protocol area, for LDAP, click **Edit**.
3. Click **Add New**.

4. For Optional Information, in the Search Directory Root field, type the root path of the search directory in Base DN format.

   Note: For details on Base DN, refer to the *RFC 2849 - LDAP Data Interchange Format Technical Specification* on the Internet Engineering Task Force website.

5. Specify the login credentials required to access the LDAP directory.
   - **None**: This option instructs the printer to access the LDAP directory.
   - **Logged-in User**: This option instructs the printer to log in to the repository and provide the credentials of the logged-in user.
   - **Device**: This option instructs the printer to use specific credentials when the printer accesses the LDAP repository. If you select Device, type the credentials in the Login Name and Password fields. To update an existing password, select **Select to save new password**.

6. To use LDAPS, for Secure LDAP Connection, select **Enable Secure Connection (LDAPS)**.

   a. To allow the printer to validate certificates, select **Validate Repository SSL Certificate (trusted, not expired, correct FQDN)**.

   b. To select a security certificate, for Trusted SSL Certificate, click the menu, then select an option.

   c. To view the selected certificate details, or save the certificate to your computer, click **View/ Save**.

7. To define the number of addresses returned in a search, for Maximum Number of Search Results, type a number from 5–100. The default number is 100. To use the maximum number of search results specified by the LDAP server, select **Use LDAP Server Maximum**.

8. To allow the printer to use the current settings for the LDAP server, for Search Timeout, select **Use LDAP Server Timeout**. To specify a time that the printer waits before it times out, select **Wait**, then type the number of seconds from 5–100. The default is 30 seconds.

   Note: If you experience trouble retrieving results from your LDAP server, use the Wait option.

9. If you connect your primary LDAP server to other servers, to include more LDAP servers in your searches, select **LDAP Referrals**.

10. For Perform Search on Mapped Fields, select an option.
    - **Name**: This option instructs the printer to query the configured name field.
    - **Surname and Given Name**: This option instructs the printer to query the configured surname and given name fields.
    - **Display Name**: This option instructs the printer to query the configured display name field.

    Note: If you want to sort your search results, for Sort Results by Mapped Field, select an option.

11. Click **Apply**.

Configuring a Secure LDAP Connection

1. In the Embedded Web Server, click **Properties > Connectivity > Setup**.
2. In the Protocol area, for LDAP, click **Edit**.
3. On the LDAP page, click **Add New**.

4. To enable a secure connection to the LDAP server, for Secure LDAP Connection, select **Enable Secure Connection (LDAPS)**.
5. To validate the SSL certificate used for HTTPS, select **Validate Server Certificate (trusted, not expired, correct FQDN)**.
6. To view a list of external root or intermediate trusted SSL certificates, click **View Root/ Intermediate Trusted Certificates**.
7. For Root/Intermediate Trusted Certificates, select a certificate.
8. To view the selected certificate details, or to save the certificate to your computer, click **View/ Save**.

   Note: If the LDAP Server has encryption enabled, ensure that a certificate issued from the LDAP server certificate authority is installed on the device.

LDAP Server Contexts

Contexts are defined starting points in an LDAP database from which the search function begins searching. Contexts are used with the Authentication feature. You can configure the printer to add an authentication context automatically to the Login Name provided by the user.

Note: Contexts are used only if you configure LDAP server settings and select NDS as the server type.

Configuring LDAP Contexts

1. In the Embedded Web Server, click **Properties > Connectivity > Setup**.
2. For Protocol, for LDAP, click **Edit**.
3. Click **Add New**.
4. Click the **Contexts** tab.
5. For Default Login Context, type details as needed.
6. Click **Apply**.

Configuring LDAP User Mappings

LDAP servers display different results depending on how they implement mappings. Use this page to map LDAP fields to fields on your printer. Editing current map settings allows you to fine-tune server search results.

Defining User Mappings

1. On the LDAP Server page, click **User Mappings**.
2. For Search, type a user name in the Enter Name field, then click **Search**.

3. For Imported Heading, for each field, make menu selections. Remap the headings as needed. The schema on the LDAP server defines the headings.

   Note:

   - If you are using Internet fax, ensure that the Internet Fax field is not set to **No Mappings Available**. This setting prevents the Network Address Book from displaying on the printer control panel Internet fax screen. If your LDAP server does not contain a unique Internet fax address field, you can set the fax address to match the heading for email address.
   - If the user mapping is incorrect, an LDAP search in the Embedded Web Server can work properly, but authentication at the printer control panel fails.

4. Click **Apply**.

LDAP Custom Filters

You can edit custom filters so that text strings typed at the control panel are changed to match the format that the LDAP server requires.

There are three types of filters that you can customize:

- **LDAP Authentication Filter** allows you to add text to the beginning or end of a User ID, or the Login Name configured as the System Login Name for the server. Typical filters are domain_name/USERID or USERID@domain_name.
- **Email Address Book Filter** allows you to customize the standard filter that is used when a user types a name to search in the Network Address Book.
- **User ID Query Filter** allows you to customize the standard filter that the printer uses when searching for the name of the logged-in user. For example, when remote authorization is configured, and a user logs in at the control panel, the printer searches the authorization server using this filter. The standard filter looks in the field mapped as the Login Name field. If you are using an ADS LDAP server, this field is typically sAMAccountName. If you want a search for a specific person to return an exact match, do not use wildcard characters.

Configuring Custom Filters

1. In the Embedded Web Server, click **Properties > Connectivity > Setup**.
2. For Protocol, for LDAP, click **Edit**.
3. Click the **Custom Filters** tab.
4. For LDAP Authentication, select **Prepend Domain Name**. This setting prepends the base Domain Name (DN) to a user Relative Distinguished Name (RDN) when authenticating the user. Use the Common Name (CN) attribute to specify USERID in the base DN.

   Note:

   - If Authenticated User is selected for Login Credentials to Access LDAP Server, some UNIX/Linux LDAP servers can require setting the Prepend Domain Name attribute.
   - For details on Base DN formatting, refer to the *RFC 2849 - LDAP Data Interchange Format (LDIF) Technical Specification* on the IETF website.

5. For Email Address Book Filter, select **Enable Custom Filter**.

6. Type the LDAP search string or filter as needed, where LDAP represents the string provided for the query. The filter defines a series of conditions that the LDAP search must fulfill to return the desired information. For example, to find people only, type **(ObjectClass=Person)&(cn=LDAP*)**.
7. For User ID Query Filter, select **Enable Custom Filter**.
8. Type the LDAP search string or filter where LDAP represents the string provided for the query. The filter defines a series of conditions that the LDAP search must fulfill to return the desired information. For example, to ensure that only user information is returned rather than equipment or conference rooms, type **(objectClass=user) (sAMAccountName=LDAP)**.
9. Click **Apply**.

LPR/LPD

The Line Printer Daemon (LPD) and Line Printer Remote (LPR) protocols provide printer spooling and network print server functionality for UNIX-based systems, such as HP-UX, Linux, and Macintosh.

1. In the Embedded Web Server, click **Properties > Connectivity > Setup**.
2. For LPR/LPD Protocol, click **Edit**.
3. For Protocol, select **Enabled**.
4. For Port Number, type a value.
5. To allow multiple printer languages in a single job, for PDL Switching, select **Enabled**. This option allows the printer to process a single print job that contains two or more printer languages. An example is a PostScript print job with a PCL header.
6. For PDL banner page attributes to override LPR control file attributes for job name and owner, select **Enabled**. This feature allows you to replace the standard information displayed on a banner page with the user name and job name from the print job.
7. For Place temporary hold on which jobs, select an option:
   - **None (Use printer's default banner sheet job name if data file 1st)**: This option omits a printer wait time to receive the job control information. This selection can cause banner page information to print incorrectly.
   - **Only those with data file received 1st**: This option holds the job when the data file for the job is received first. This option ensures that the printer waits to receive the control file information to print banner page details correctly.
   - **All (consistent with older implementations)**: This option puts all jobs on hold. The job prints when the printer receives all job data. This setting can cause jobs to print slowly but results in accurate banner page information.
8. Click **Save**.

NFC

Near Field Communication (NFC), is a technology that enables devices to communicate when they are nearby. NFC allows you to add a printer to your Android mobile device easily. After you add the printer, there is no need to use NFC on that printer. You can use NFC to obtain the network interface to establish a TCP/IP connection between your device and the printer.

Devices can communicate using NFC when the devices are within the following ranges:

- Device with case: 17–20 mm
- Device without case: 20–25 mm

Note: The actual range can vary depending on device manufacturer.

To configure NFC:

1. In the Embedded Web Server, click **Properties > Connectivity > Setup**.
2. For NFC, click **Edit**.
3. For NFC Services, select **Enabled**.
4. Click **Save**.

   Note: For details about mobile device setup and operation, refer to the Xerox printer User Guide.

NTP

The Network Time Protocol (NTP) feature synchronizes the internal clock of the device over a network connection. The device checks the NTP server when you enable NTP, when you change the NTP settings, and every 24-hour period during device cleanup. You can specify the maximum amount of time for the difference between the device internal clock and the NTP server clock. If the device internal clock exceeds this threshold, the device synchronizes with the NTP server automatically.

If your device uses DHCP, valid addresses and offsets are accepted when the DHCP server provides one or both of the following:

- The addresses of NTP servers in the network, specified by DHCP option 42
- The Greenwich Mean Time (GMT) offset

If the addresses or offset received from the DHCP server are invalid, the values are ignored and the manually set values are applied.

1. In the Embedded Web Server, click **Properties > Connectivity > Setup**.
2. For Protocol, for NTP, click **Edit**.
3. For NTP Enabled, select **Enabled**.
4. Select **IPv4 Address** or **Host Name**.
   - **IPv4 Address**: For IP Address: Port and Alternate IP Address: Port, type the IP addresses and port numbers.
   - **Host Name**: For Host Name: Port, and Alternate Host Name: Port, type the host names and port numbers.
5. For IP Address: Port and Alternate IP Address: Port, type the address and port numbers.
6. To test connectivity to the NTP server, click **Destination Test**.

   If the test succeeds, a confirmation message appears.

   If the test fails, an error message appears. Verify the NTP server settings, then repeat the test.
7. Click **Save**.
8. For the new settings to take effect, restart your device.

POP3

Post Office Protocol, version 3 (POP3) is a protocol that allows email clients to retrieve email from remote servers over TCP/IP on network port 110. This printer uses POP3 for the Internet fax and email features to retrieve fax jobs over email.

1. In the Embedded Web Server, click **Properties > Connectivity > Setup**.
2. For Under Protocol, for POP3 Setup, click **Edit**.
3. For Under Server Information, select **IPv4** or **Host Name**.
4. Type the address or server name.
5. For Login Name, type the name assigned to the printer for logging in to the POP3 server.
6. For Password, type a password. For Retype password, retype the password to verify.
7. To save the new password, click **Select to save new password**.
8. For the POP3 Settings pane, select **Enable receipt of Email via POP3**.
9. For Polling Interval, type a value from 1 through 60.
10. Click **Save**.

Proxy Server

A proxy server acts as a go-between for clients seeking services and servers that provide them. The proxy server filters client requests and if the requests meet the proxy server filtering rules, it grants the request and allows the connection.

A proxy server has two main purposes:

- To keep any devices behind it anonymous for security purposes.
- To cache content from resources, such as Web pages from a Web server, to increase resource access time.

Proxy server settings apply to features that use HTTP or HTTPS. Examples include Remote Services, Xerox Online Support, Workflow Scanning destinations, workflow pool repositories, and Extensible Service Setup.

Configuring the Proxy Server

1. In the Embedded Web Server, click **Properties > Connectivity > Setup**.
2. For Protocol, for Proxy Server, click **Edit**.
3. For HTTP Proxy Server, select **Enabled**.
4. Select the HTTP Proxy Server address type. Options are **IPv4 Address**, **IPv6 Address**, or **Host Name**.
5. Type the appropriately formatted Proxy Server address and port number.
6. Click **Save**.

   Note: Not all printer models support all features that use the proxy server.

Raw TCP/IP Printing

Raw TCP/IP is used to open a TCP socket-level connection over Port 9100, and stream a print-ready file to the printer input buffer. It then closes the connection either after sensing an End Of Job character in the PDL or after expiration of a preset timeout value. Port 9100 does not require an LPR request from the computer or the use of an LPD running on the printer. Raw TCP/IP printing is selected in Windows as the Standard TCP/IP port.

Note: Enable TCP/IP before enabling Raw TCP/IP printing.

Configuring Raw TCP/IP Settings

1. In the Embedded Web Server, click **Properties > Connectivity > Setup**.
2. For Protocol, for Raw TCP/IP Printing, click **Edit**.
3. On the Raw TCP/IP Printing tab, for Protocol, select **Enabled**.
4. For TCP Port Number, ensure that Port 1 is set to **9100**.

   Note: To emulate HP JetDirect EX Plus 3, set Port 2 to **9101** and Port 3 to **9102**.
5. For Bidirectional, for each active port, select **Enabled**.
6. For Maximum Connections per Port, for each active port, type a number from 1 through 32.
7. For End of Job Timeout, for each active port, type a time in seconds from 0 through 1800.
8. For PDL Switching, for each active port, select **Enabled** as needed.

   Note: PDL Switching allows the printer to switch automatically between multiple supported PDLs within a single job.
9. To save the new settings, click **Apply**.
10. To return all settings to the default status, click **Default All**.

Configuring Raw TCP/IP Advanced Settings

1. On the Raw TCP/IP Printing page, click the **Advanced** tab.
2. Under Connections, set the following:
   - Set the Maximum Connections per port between **1–32**. The default port value is 32.
   - To allow concurrent jobs to process for each port connection, type a number between **0–500** jobs in each port. Type **0** to allow unlimited concurrent jobs.
   - To limit the number of jobs that are active for each port connection, type a number between **0–32768**. Type **0** to allow unlimited number of active jobs.
3. Under Job Boundary Determination:

   Type the End of Job Timeout between **0–1800** seconds to specify the amount of time to pass before a job processes with an End of Job character. The default time is 300 seconds.Type **0** to disable end of job detection by timeout.

4. Under Backchannel Data:

   Enable **Backchannel Data Transmission to Client**, then, enable **Out of Order Backchannel Data** to allow data from several jobs to be interspersed.

   > **Note:** Out of Order Backchannel Data is only available when Backchannel Data Transmission to Client is enabled.

5. Under Banner Page Printing:
   - To restrict banner pages to print for specific jobs only, select the job types from the Banner Page Enabled drop-down menu. Options are **First Job Only**, **No Jobs**, or **All Jobs**.
   - To enable banner pages to print before each PDL document within a single job, select **Enabled** for Banner Page for Each Document of Job.
   - To restrict banner pages to print for jobs that specifically request them through PJL, select **Enabled** for Banner Page for Job Containing only PJL Commands.

6. Miscellaneous
   - To allow the printer to switch between multiple PDLs within a single job, select **Enabled** for Language (PDL) Switching within PJL Job.
   - To force parsing of job data, select **Enabled** for Job Data Parsing Override.

   > **Note:** Job data is not parsed when bidirectional communication and PDL switching are disabled.

7. Click **Apply** to save the new settings or **Undo** to retain the previous settings.

   Click **Default All** to reset settings to default values.

SLP

Printers use Service Location Protocol (SLP) to announce and look up services on a local network without prior configuration. When SLP is enabled, the printer becomes a Service Agent (SA) and announces its services to User Agents (UA) on the network using SLP.

Directory Agents (DA) are components that cache services. They are used in larger networks to reduce the amount of traffic. DAs are optional. If a DA is present, then User Agents (UAs) and System Agents (SAs) are required to use it instead of communicating directly with the printer.

Configuring SLP

1. In the Embedded Web Server, click **Properties > Connectivity > Setup**.
2. In the Protocol area, for SLP, click **Edit**.
3. For Protocol, select **Enabled**.
4. For Directory Agent, type the IP address for the Directory Agent (DA), as needed.
5. To group services, for Scope 1, 2, and 3, type a name as needed. Printers cannot recognize services that are in different scopes.
6. For Message Type, select an option.
   - **Multicast**: This option routes multicast packets between subnets.
   - **Broadcast**: This option does not route packets between subnets.
7. Under Multicast Radius, type a value from 0 through 255.

   Multicast Radius defines how many routers the multicast packet can cross.
8. For Maximum Transmission Unit (MTU), type a value from 484 through 32768.

   Note: The maximum MTU for IP over Ethernet is 1500 bytes.
9. Click **Save**.

SMB Filing

You can specify Kerberos authentication options for features that file images to an SMB-shared network location.

Configuring Kerberos Authentication Options for SMB

1. In the Embedded Web Server, click **Properties > Connectivity > Setup**.
2. In the Protocol area, for SMB Filing, click **Edit**.
3. In the With Kerberos Tickets area, for the Workflow Scanning, Server Fax, and Scan to Home features, select an option:
   - **Always File with Kerberos Ticket**: This option instructs the printer to attempt to use Kerberos authentication to the SMB shared network location. Configure network authentication or Smart Card authentication using a Kerberos server.
   - **Prefer Filing with Kerberos Ticket**: This option instructs the printer to authenticate to the SMB shared network location with a Kerberos ticket if available. If a Kerberos ticket is not available, or Kerberos authentication fails, the printer attempts to authenticate using other methods, such as NT, or NTLM.
   - **Do Not File with Kerberos Ticket**: This option instructs the printer to attempt to authenticate to the SMB shared network location using other methods, such as NT, or NTLM. Do not select this option when Smart Card authentication is enabled. If you select this option when Smart Card authentication is enabled, SMB file transmission fails, and an error message appears on the touch screen.
4. The Without Kerberos Tickets area lists features that can use SMB, but cannot use Kerberos authentication. For FIPS 140 compliance, disable these features or configure the features to use a protocol other than SMB. To navigate to the configuration page for a listed feature, click the appropriate link.
5. In the SMB Protocol Version area, select at least one SMB protocol version.
   - **SMBv3**: This option instructs the device to use the SMBv3 protocol. **SMBv3** is enabled by default. From the list, select the highest version of SMBv3 that the device supports.
   - **SMBv2**: This option instructs the device to use the SMBv2 protocol. **SMBv2** is enabled by default.
   - **SMBv1**: This option instructs the device to use the SMBv1 protocol. **SMBv1** is disabled by default.

   Note: If both **SMBv3** and **SMBv1** are enabled, **SMBv2** is enabled also.
6. Click **Save**.

SMTP Server

Simple Mail Transfer Protocol (SMTP) is an Internet standard used to transmit email across IP networks. Your printer uses SMTP to transmit scanned images, Internet fax jobs, and alerts through email.

Configuring SMTP Server Settings

1. In the Embedded Web Server, click **Properties > Connectivity > Setup**.
2. For Protocol, for SMTP, click **Edit**.
3. To allow the printer to use DNS to identify an SMTP server on your network automatically, for Server, select **Use DNS**.
4. To specify an SMTP server manually, select **Specify SMTP Server manually**.
   1. For address type, select an option. Options are **IPv4 Address**, **IPv6 Address**, or **Host Name**.
   2. Type the appropriately formatted address and port number.
5. For Device Email Address, type the email address of the printer.
6. Click **Apply**.

Configuring SMTP Authentication Settings

1. In the Embedded Web Server, click **Properties > Connectivity > Setup**.
2. For Protocol, for SMTP (Email), click **Edit**.
3. On the SMTP (Email) page, click the **SMTP Authentication** tab.
4. For Login credentials that are used for user-initiated email jobs, select an option:
   - **None**: This option does not require the device to provide a user name or password to the server.
   - **Device**: This option uses the information that is provided in the Login Name and Password Fields to access the server.

     To update the password for an existing Login Name, enable **Select to save new password**.
   - **Logged-in User**: This option uses the credentials of the authenticated user to access the server.

     Note: If network authentication is configured to use a Kerberos server, and you want to use Kerberos tickets, for Kerberos tickets, select **Always**.
   - **Prompt at device control panel**: This option requires users to type a login name and password at the control panel.
5. For Login credentials that are used for device-initiated email messages, select an option:
   - **None**: This option does not require the device to provide a user name or password to the server.
   - **Device**: This option uses the information that is provided in the Login Name and Password Fields to access the server.

     To update the password for an existing Login Name, enable **Select to save new password**.
6. Click **Apply**.

Configuring SMTP Connection Encryption Settings

1. In the Embedded Web Server, click **Properties > Connectivity > Setup**.
2. For Protocol, for SMTP (Email), click **Edit**.
3. On the SMTP (Email) page, click the **Connection Encryption** tab.
4. To encrypt SMTP communication, for Encryption Mechanism used by devices when communicating with the SMTP Server, select an option.

   Note: If you do not know the encryption method that your server supports, select **STARTTLS (if available)**. If you select **STARTTLS (if available)**, the printer attempts to use STARTTLS. If your server does not support STARTTLS, SMTP communication is not encrypted.

5. Click **Apply**.

Configuring SMTP File Size Management

1. On the SMTP (Email) page, click the **File Size Management** tab.
2. To define a maximum message size for messages with attachments, type a value between **512–20480** KB in the Maximum Message Size field.
3. To improve transmission speed, set messages to fragment between **1–500** times.
4. To set a maximum job size, type a value between **512–2000000** KB in the Total Job Size field.
5. If you selected more than 1 fragment in Number of Fragments, under Email Job Splitting Boundary, select an option:
   - **Page Boundary** instructs the mail client not to reassemble the job on receipt.
   - **Automatic Boundary** instructs the mail client to reassemble the job on receipt.
6. Click **Apply**.

Testing SMTP Configuration Settings

1. On the SMTP (Email) page, click the **Test Configuration** tab.
2. Under To Address, type an email address.
3. To send a test email to the address, click **Send Email**.

   If the email transmission succeeds, a confirmation message appears. If the transmission fails, an error message appears.

SNMP

Simple Network Management Protocol (SNMP) is a set of network protocols designed to allow you to manage and monitor devices on your network.

You can use the SNMP configuration pages in the Embedded Web Server to:

- Enable or disable Authentication Failure Generic Traps.
- Enable SNMPv3 to create an encrypted channel for secure printer management.
- Assign privacy, authentication protocols, and keys to Administrative and key user accounts.
- Assign read and write access to User accounts.
- Limit SNMP access to the printer using hosts.

Enabling SNMP

1. In the Embedded Web Server, click **Properties > Connectivity > Setup**.
2. For Protocol, for SNMP, click **Edit**.
3. Select an option:
   - To enable SNMP v1/v2c, select **Enable SNMP v1/v2c Protocols**.
   - To enable SNMP v3, select **Enable SNMP v3 Protocol**.
4. To prompt the printer to generate a trap for every SNMP request processed with an invalid community name, for Authentication Failure Generic Traps, select **Enabled**.
5. Click **Save**.

Configuring SNMPv1/v2c

SNMP version 1 (SNMPv1) is the initial implementation of the SNMP protocol. SNMPv1 operates over protocols such as User Datagram Protocol (UDP) and IP.

SNMPv2c includes improvements in performance, confidentiality, and manager-to-manager communications over SNMPv1, however it uses the simple-community based security scheme of SNMPv1.

1. In the Embedded Web Server, click **Properties > Connectivity > Setup**.
2. For Protocol, for SNMP, click **Edit**.
3. Click **Edit SNMPv1/v2c Properties**.
4. For GET Community Name, type a name.
5. For SET Community Name, type a name.
6. For Confirm SET Community Name, reenter the SET Community Name.

   Caution: Changes made to the GET or SET community names for this printer require corresponding changes to the GET or SET community names for applications that use SNMP.

7. To save the SET Community Name, select the Select to save new 'SET Community Name' check box.

8. For TRAP Community Name, type a name.

   Note: Use the Default TRAP Community Name to specify the default community name for all traps the printer generates. Individual Trap Community Names specified for each trap destination address can override the community name. Each Trap Community Name must be unique.

9. Click **Save**.

Configuring SNMPv3

SNMPv3 is the current standard version of SNMP defined by the Internet Engineering Task Force (IETF). It provides three important security features:

- Message integrity to ensure that a packet has not been tampered with in transit
- Authentication to verify that the message is from a valid source
- Encryption of packets to prevent unauthorized access

Editing SNMPv3 Security Settings

1. In the Embedded Web Server, click **Properties > Connectivity > Setup**.
2. For Protocol, for SNMP, click **Edit**.
3. Click **Edit SNMPv3 Properties**.
4. For Security, select an Authentication/Encryption protocol pair for SNMPv3.
5. To use factory-default administrator account values, for Administrator Account, select **Account Enabled**.
6. To use factory-default print driver and remote client account values, for Print Drivers/Remote Clients Account, select **Account Enabled**.
7. Click **Save**.

Configuring the SNMPv3 Administrator Account

1. In the Embedded Web Server, click **Properties > Connectivity > Setup**.
2. For Protocol, for SNMP, click **Edit**.
3. Click **Edit SNMPv3 Properties**.
4. To enable the administrator account, for Administrator Account, select **Account Enabled**.
5. Type the User Name for the Administrator Account.
6. Type, then confirm the **Authentication Password**.
7. Type, then confirm the **Privacy Password**.

   Note:

   - The passwords must be at least eight characters in length.
   - To set the account credentials to factory-default values, select **Default All**.

8. Click **Save**.

Configuring the SNMPv3 Print Drivers/Remote Clients Account

1. In the Embedded Web Server, click **Properties > Connectivity > Setup**.
2. For Protocol, for SNMP, click **Edit**.
3. Click **Edit SNMPv3 Properties**.
4. For Print Drivers/Remote Clients Account, click **Account Enabled**. This account allows Xerox® clients and print drivers limited access to objects on the device.
5. Type the User Name for the Print Drivers/Remote Clients Account.
6. Type, then confirm the **Authentication Password**.
7. Type, then confirm the **Privacy Password**.

   Note:

   - The passwords must be at least eight characters in length.
   - To set the account credentials to factory-default values, select **Default All**.
8. Click **Save**.

Configuring SNMP Advanced Settings

You can add, edit, or delete IP addresses for Network Management workstations that receive traps from the printer.

Configuring SNMP Advanced Settings

1. In the Embedded Web Server, click **Properties > Connectivity > Setup**.
2. For Protocol, for SNMP, click **Edit**.
3. Click **Advanced Settings**.
   - To add an IP trap destination address, for Trap Destination Addresses, click **Add IP Address**.
   - To edit an address, click **Edit**.
   - To delete an address, select the check box for the address, then click **Delete**.

Adding or Editing an IP Trap Destination Address

1. On the Advanced Settings page, click **Add IP Address**, or select an existing address and click **Edit**.
2. Type the IP address of the host running the SNMP manager that receives traps.
3. Type the UDP Port Number. The default is 162 for traps.
4. Select the SNMP version based on what the system receiving traps supports.
5. Select the type of traps that the SNMP manager receives under Traps to be Received.
6. Click **Save** to apply the new settings or **Undo** to retain the previous settings.
7. Click **Cancel** to return to the previous page.

WSD

Web Services for Devices (WSD) is technology from Microsoft that provides a standard method for discovering and using network connected devices. It is supported in Windows Vista, Windows Server 2008, and newer operating systems. WSD is one of several supported communication protocols.

Enabling WSD

1. In the Embedded Web Server, click **Properties > Connectivity > Setup**.
2. For Protocol, for WSD, click **Edit**.
3. For WSD Services, select **Enabled**.
4. Click **Save**.

4

Security

This chapter contains:

For reference:

www.xerox.com/security

Setting Access Rights

You can control access to apps and features by setting up authentication and authorization. Personalization allows the printer to retrieve user information to customize features.

Authentication

Authentication is the process of confirming your identity. When the system administrator enables authentication, the printer compares the information that you provide to another source of information, such as an LDAP directory. The information can be a user name and password, or the information stored on a magnetic, proximity, or smart card. If the information is valid, you are considered an authenticated user.

There are several ways to authenticate a user:

- **User Name/Password - Validate on the Device**: This option enables local authentication. Users prove their identity by typing a user name and password at the control panel or in the Embedded Web Server. The printer compares the user credentials to the information stored in the user database. If you have a limited number of users, or do not have access to an authentication server, use this authentication method.
- **User Name/Password - Validate on the Network**: This option enables network authentication. Users prove their identity by typing a user name and password at the control panel or in the Embedded Web Server. The printer compares the user credentials to the information stored on an authentication server.

  Note: The printer can use one of the following authentication server types: Kerberos (Solaris or Windows), SMB (Windows 2000/2003), or LDAP.
- **Convenience Authentication**: This option enables authentication for a Proximity Card Reader. Users swipe a pre-programmed identification card at the control panel. To use this method, purchase and install a USB card reader and an authentication server that supports the Xerox®Convenience Authentication API.
- **Xerox Secure Access - Unified ID System**: This option enables authentication for the Xerox Secure Access Unified ID System. Users present a pre-programmed identification card to a card reader at the control panel. The printer compares the user credentials to the information stored on the Xerox®Secure Access server. To use this method, purchase and install the Xerox Secure Access Unified ID System.
- **Smart Cards**: This option enables authentication for a Smartcard Reader. Users insert a pre-programmed identification card in a carder reader at the control panel. To use this method, purchase and install a Smartcard Reader system.

Setting the Login Method for the Embedded Web Server

1. In the Embedded Web Server, click **Properties > Login/Permissions/Accounting**.
2. Click **Login Methods**.
3. For Control Panel & Website Login Methods, click **Edit**.

4. For Website Login, select an option.

   Note: Website Login is only available when one of the following authentication methods is enabled for the control panel:

   - Convenience Authentication
   - Xerox Secure Access - Unified ID System
   - Smart Cards

5. Click **Save**.

Setting the Login Method for the Control Panel

1. In the Embedded Web Server, click **Properties > Login/Permissions/Accounting**.
2. Click **Login Methods**.
3. For Control Panel & Website Login Methods, click **Edit**.
4. For Control Panel Login, select an option.
5. If you selected Convenience Authentication or Smart Cards as the authentication method, you can also allow users to log in at the control panel. This option is useful if a user loses a smart card, but must access the device. For Alternate Control Panel Login, select **User Name / Password - Validate on the Network**.
6. Click **Save**.

   Note: The first time you select Smart Cards as the authentication method, you are prompted for a Feature Enablement Key. The Feature Enablement Key is included in the Common Access Card Enablement Kit.

Configuring Authentication Settings

Configuring Local Authentication Settings

When you configure local authentication, users prove their identity by typing a user name and password at the control panel or in the Embedded Web Server. The device compares the user credentials to the information stored in the user database. If you have a limited number of users, or do not have access to an authentication server, use this authentication method.

To configure access rights using local authentication:

- Set the login method to **User Name / Password - Validate on the Device**. For details, refer to Setting the Login Method for the Embedded Web Server.
- Add user information to the user information database.
- If you enabled Personalization, configure LDAP server settings. For details, refer to Configuring LDAP Server Optional Information.
- Configure authorization settings. For details, refer to Authorization.

The Login Methods page in the Embedded Web Server provides links to authentication and personalization configuration settings.

1. In the Embedded Web Server, click **Properties > Login/Permissions/Accounting**.

2. Click **Login Methods**.

User Database

The user database stores user credential information. The printer uses this information for local authentication and authorization, and for Xerox® Standard Accounting. When you configure local authentication, the printer checks the credentials that a user provides against the information in the user database. When you configure local authorization, the printer checks the user database to determine which features the user is allowed to access.

Adding or Editing User Information in the Device Database

1. In the Embedded Web Server, click **Properties > Login/Permissions/Accounting > Device User Database**.
   - To add a user, click **Add New User**.
   - To edit an existing user, for the user, click **Edit**.
2. Type a User Name and Friendly Name for the user.

   Note: After you add a User Name and Friendly Name, you can edit the Friendly Name, but you cannot edit the User Name.
3. Type a Password for the user, then retype it to verify.

   Note: The Password field only appears if the selected authentication method is local authentication.
4. To add the user to a role, for the role, select the check box:
   - **Accounting Administrator**: This role allows the user to access accounting settings, apps, and locked settings.
   - **System Administrator**: This role allows the user to access all apps and settings.
   - **Copying Only**: This role allows the user to access only the device copying functions.

   If you have created any user roles, they also appear in the list.
5. To edit a custom user role, for the role, click **Edit**.
6. Click **Save**.

Specifying User Password and Account Requirements

Basic rules for local user account names and passwords are standard on the Xerox device. You can customize these rules for your particular policies.

1. In the Embedded Web Server, click **Properties > Login/Permissions/Accounting > Device User Database**.
2. Click **Device Account Requirements**.
3. To use a preset, for Requirement Preset, select an option.
   For information, refer to Requirement Preset Options.
   - **Level 1: Basic**: This setting is the default.
   - **Level 2: Elevated**
   - **Level 3: High**
   - **Custom**: This level allows you to customize the password requirements.
4. To customize the password requirements, select or change options as needed:

a. To change the minimum number of characters required, for Minimum Password Length, type a value. The default value is 4.

Note: To change the value, use the **Plus** (**+**) and **Minus** (**-**) icons.

b. To require specific character types, for each character type needed, select the check box. Options include:

- Require Uppercase Character
- Require Lowercase Character
- Require Numeric Character
- Require Special Character

c. To change the interval before a user can reuse a previously used password, for Interval Before Password Can Be Reused (Generations), type a value. The maximum value is 7.

Note: A value of 1 allows a user to reuse a password immediately.

d. To change the user lock out period, for User Lock Out Period (Minutes), type a value. The default value is 30 minutes.

Note: The system sets the values for Lock Out User After Invalid Login Attempts and Browser Session Lock Out Period (Minutes).

5. To enable an account inactivity timer:

a. For Enable Account Inactivity Timer, select the check box. This setting specifies the amount of time an account is allowed inactivity before the account is disabled.

b. For Disable Account After Period of Inactivity (Days), type a value. The default value is 180 days.

Note:

- The administrator account is not disabled after the specified inactivity period.
- When the administrator reactivates an individual account, the password remains unchanged.

6. Click **Update**.

Note:

- New password rules do not affect existing passwords.
- New password rules are enforced the next time a user logs in.

Requirement Preset Options

Requirement Preset options include:

Level 1

This level requires:

1. A minimum password length of four characters.
2. A minimum of one generation of a password before the user can reuse a password.

Level 2

This level requires:

1. A minimum password length of eight characters, including a minimum of one uppercase character and one numeric character.
2. A minimum of three generations of a password before the user can reuse a password.

Level 3

This level requires:

1. A minimum password length of 15 characters, including a minimum of one of each character type:
   - Uppercase
   - Lowercase
   - Numeric
   - Special
2. A minimum of seven generations of a password before the user can reuse a password.

Restricting System Account Access

You can prevent the following non-system administrator accounts from logging in to the device:

- Diagnostics
- Customer Service Engineer
- Force OnBox Login

When you enable this feature, only these accounts are restricted. This feature does not impact other authentication and accounting accounts.

To restrict non-system administrator accounts:

1. In the Embedded Web Server, click **Properties > Login/Permissions/Accounting > Device User Accounts**.
2. From the Management Actions menu, select **Restrict System Account Access**.
3. For Prevent Log In From Non-Admin System Accounts, select the check box.
4. Click **Save**.

Configuring Network Authentication Settings

When you configure network authentication, to prove their identity, users type their name and password in at the control panel or in the Embedded Web Server. The device compares the user credentials to the information stored on an authentication server.

Note: If two or more authentication servers are configured, then the IPP Authentication Policy window appears. The IPP Authentication Policy is used to determine which server to use for IPP Authentication.

To configure access rights using network authentication:

- Set the login method to **User Name / Password - Validate on the Network**. For details, refer to Setting the Login Method for the Embedded Web Server.
- Provide information about your authentication server and configure authentication server settings.
- If you enabled Personalization, configure LDAP server settings.
- Configure authorization settings. For details, refer to Authorization.

The Login Methods page in the Embedded Web Server provides links to authentication and personalization configuration settings.

1. In the Embedded Web Server, click **Properties > Login/Permissions/Accounting**.
2. Click **Login Methods**.

Configuring Authentication Server Settings for Kerberos

1. On the Login Methods page, for Authentication Servers, click **Edit**.
2. For Authentication Type, select **Kerberos**.
3. Click **Add New**.
4. For Server Information, in the Domain or Realm field, type the domain or realm for your authentication server.
5. Select the desired address type.
6. Type the appropriately formatted address and port numbers for both the primary and backup addresses.

   Note: A backup address is optional.
7. To use an LDAP server for network authorization or personalization:
   a. Click **Add LDAP Mapping**.
   b. Select the LDAP server from the list and click **Add Mapping**, or click **Add New** to add an LDAP server.
8. Click **Save**.
9. To specify server settings for an alternate authentication server, click **Add New**.
10. To copy the settings from another server, select a server from the list, then click **Copy From**.
11. To update the settings, click **Edit**.

Configuring Authentication Server Settings for SMB

1. On the Login Methods page, next to Authentication Servers, click **Edit**.
2. Under Authentication Type, select **SMB (Windows NT 4)** or **SMB (Windows 2000/2003)**.
3. Click **Add New**.
4. Under Domain, type the domain name of your authentication server.
5. Select the address type.
6. Type the appropriately formatted address and port number.
7. Click **Save**.
8. To specify server settings for an alternate authentication server, click **Add New**.
9. To copy the settings from another server, select a server from the list and click **Copy From**.
10. Click **Edit** to update the settings.

Configuring Authentication Server Settings for LDAP

The device uses the primary LDAP server for authentication, authorization, and personalization. The primary LDAP server appears in the Embedded Web Server on the LDAP Server page. If you have configured LDAP server settings, when you select LDAP as the network authentication or authorization method, the device uses this server automatically. The device only uses alternate LDAP servers for authorization and personalization when primary LDAP server communication fails.

1. On the Login Methods page, for Authentication Servers, click **Edit**.
2. For Authentication Type, select **LDAP**.
3. Click **Add New**.
4. Configure LDAP server settings, then click **Apply**.

Configuring Xerox Secure Access Unified ID System Authentication Settings

When Xerox® Secure Access authentication is configured, users swipe a pre-programmed identification card at the control panel. The printer compares the user credentials to the information stored on the Xerox® Secure Access server. To use Xerox® Secure Access, purchase and install the Xerox Secure Access Unified ID System.

To configure access rights using Xerox Secure Access Unified ID System authentication:

- Install the Xerox® Secure Access authentication server software and configure it with user accounts. For details, refer to the Xerox Secure Access Unified ID System documentation.
- Enable the Authentication and Accounting Configuration Web service. For details, refer to HTTP.
- Format and configure identification cards.
- Connect your card reader to the USB Port.

  Note: Ensure that USB ports are enabled. For details, refer to USB Port Security.

- Set the login method to **Xerox Secure Access - Unified ID System**. For details, refer to Setting the Login Method for the Control Panel.
- Configure Xerox® Secure Access Setup settings.
- Enable the Xerox® Secure Access Web service. For details, refer to HTTP.
- If you enabled Personalization, configure LDAP server settings. For details, refer to LDAP server settings.
- Configure authorization settings. For details, refer to Authorization.

The Login Methods page in the Embedded Web Server provides links to authentication and personalization configuration settings.

1. In the Embedded Web Server, click **Properties > Login/ Permissions/ Accounting**.
2. Click **Login Methods**.

Configuring Xerox Secure Access

1. On the Login Methods page, next to Xerox® Secure Access Setup, click **Edit**.
2. Configure the remote server. For details, see the instructions provided with your server hardware. Once the server is configured, it communicates with the printer and automatically completes the configuration process.
3. To configure communication manually, personalize instructional windows, and review accounting options, click **Manually Configure**.
4. To return to the Login Methods page, click **Pending Remote Server Setup**.
5. To configure any settings that are marked in red text as **Required; Not Configured**, in the table at the bottom of the page, click **Edit**.

Manually Configuring Xerox Secure Access Settings

If you are using Xerox® Secure Access for authentication, you can manually configure remote server communication, personalize instructional windows, or review accounting options.

Before you begin:

Configure the Xerox® Secure Access authentication server.

1. On the Login Methods page, next to Xerox® Secure Access Setup, click **Edit**.
2. Click **Manually Configure**.
3. Under Server Communication, select the address type and port number.
4. Type the appropriately formatted address and port number.
5. In the Path field, type the following HTTP path: **public/dce/xeroxvalidation/convauth**.
6. Under Embedded, select **Enabled**.
7. Under Device Log-In Methods, select an option:
   - **Xerox Secure Access Device Only** allows users to access the printer only using the card reader.
   - **Xerox Secure Access Device + alternate onscreen authentication method** allows users to access the printer by logging in at the control panel.
8. When Network Accounting is configured, the printer can obtain user accounting information from the authentication server. To reduce the number of screens that appear when a user logs in at the control panel, select **Automatically apply Accounting Codes from the server**.
   If you want users to provide an accounting code at the control panel, select **User must manually enter accounting codes at the device**.
9. To create login instructions for users, under Device Instructional Blocking Window, type text in the fields.
   a. In the Window Title field, type text to appear as a title at the top of the touch screen.
   b. In the Instructional Text field, type instructions that appear below the title.

      Note: If the Title and Prompt are configured on the Xerox Partner authentication server, then any instructional text that you type is ignored.
10. Click **Save**.

Configuring Convenience Authentication Settings

When Convenience Authentication is enabled, users swipe a pre-programmed identification card through a Proximity Card Reader at the control panel. To use this method, purchase and install a USB card reader and an authentication server that supports the Xerox® Convenience Authentication API.

The Login Methods page in the Embedded Web Server provides links to authentication and personalization configuration settings.

1. In the Embedded Web Server, click **Properties > Login/ Permissions/ Accounting**.
2. Click **Login Methods**.

Configuring Access Rights Using Convenience Authentication

To configure access rights using Convenience Authentication:

- Format and configure identification cards.
- Connect your card reader to the USB Port.

  Note: Ensure that USB ports are enabled. For details, refer to USB Port Security.
- Enable the Xerox® Secure Access Web service. For details, refer to Configuring Xerox Secure Access Unified ID System Authentication Settings.

- Set the login method to **Convenience Authentication**. For details, refer to Setting the Login Method for the Control Panel.
- To provide information about your authentication server, for Convenience Authentication Setup, click **Edit**.
- To enable the Xerox® Secure Access Web service, for Web Service Enablement, click **Edit**.
- To configure card reader policies, for Card Reader Setup, click **Edit**.
- To customize the title and instruction text that appears on the blocking screen, for Customized Blocking Screen, click **Edit**.
- If you selected an alternate login method that requires a network authentication server, provide information about your server. For Authentication Servers, click **Edit**.
- To provide information about your LDAP server for personalization, for LDAP Servers, click **Edit**.
- Configure authorization settings. For details, refer to Authorization.

Configuring an Authentication Server for Convenience Authentication

1. On the Login Methods page, for Convenience Authentication Setup, click **Edit**.
2. For Server Communication, select an address type. Type the appropriately formatted address or host name of your server and change the default port number as needed.
3. For Path, type the path of the authentication Web service on your server.
4. When Network Accounting is configured, the device can obtain user accounting information from the authentication server. To reduce the number of screens that appear when a user logs in at the control panel, select **Automatically apply Accounting Codes from the server**.
   If you want users to provide an accounting code at the control panel, select **User must manually enter accounting codes at the device**.
5. Click **Save**.

Configuring Smart Card Authentication Settings

When Smart Card authentication is configured, users swipe a pre-programmed identification card at the control panel. Purchase and install a Smart Card reading system before configuring Smart Card authentication.

The Login Methods page in the Embedded Web Server provides links to authentication and personalization configuration settings.

1. In the Embedded Web Server, click **Properties > Login/Permissions/Accounting**.
2. Click **Login Methods**.
3. In the Control Panel & Website Login Methods area, for Control Panel, select **Smart Cards**.

4. For Smart Card Type, select an option:
   - **All Supported Smart Cards**: This option allows the user to log in with all smart cards that are listed on the default smart card list.
   - **CAC & PIV Cards**: If you are using the CAC and PIV smart card types only, you can select this option. This option can allow your CAC or PIV smart card to function even if the smart card is not added to the default smart card list.
   - **IDPrime MD Cards**: If you are using the IDPrime MD smart card type only, you can select this option. This option can allow your IDPrime MD smart card to function even if the smart card has not been added to the default smart card list.

   Note: The **CAC & PIV** and **IDPrime MD** smart card type options instruct the device to bypass the smart card white list and use the driver for the selected smart card type. This option can allow you to use smart cards of the selected type without the need for Xerox to add the card to the default smart card list.

5. To allow users to log in without a Smart Card, for Alternate Control Panel Login, select **User Name / Password — Validate on the Network**.

   Note: This option is useful in when a user loses a smart card, but needs to access the device.

6. Click **Save**.

7. On the Login Methods page, in the Configuration Settings area, configure the options for Smart Card Authentication:
   - Provide information about your domain controller servers and configure Domain Controller and NTP settings. For details, refer to Domain Controller.
   - If you want to validate certificates, configure Certificate Validation options and provide information about your OCSP server. For details, refer to Configuring OCSP Validation Server Settings.
   - If needed, configure Smart Card Inactivity Timer settings. For details, refer to Setting the Inactive Time Limit.
   - If needed, specify the method the printer uses to acquire the email address of a user by configuring email Smart Card Policies. For details, refer to Specifying the Method the Printer Uses to Acquire Email Address of Users.
   - If you want a custom image to appear at the control panel, import your image. In the Configuration Settings area, for Customize Blocking Screen, click **Edit**.
   - Configure authorization settings. For details, refer to Authorization.
   - If you enabled Personalization, configure LDAP server settings. In the Configuration Settings area, for LDAP Servers, click **Edit**. For details, refer to Adding LDAP Server Information.

Setting Up Authentication for a Smart Card System

Domain Controller

1. On the Login Methods page, for Domain Controllers, click **Edit**. Users cannot access the device until the domain controller validates the smart card domain certificate.

2. Click **Add Domain Controller**.

3. If you are using a Windows-based domain controller, for Domain Controller Type, select **Windows-Based Domain Controller**.

4. Type the domain controller server address information.

5. To apply the new settings, click **Save**. To return to the previous page, click **Cancel**.

   Note: Before you access the device, ensure that the domain controller server has validated the domain certificate on the smart card. Install domain controller certificates on the Security Certificates.

6. To change the search priority of the domain controller, click **Change Domain Priority**.
   a. To change the priority of the server, select a server in the list. To move the selected server up or down in the priority list, click the arrows.
   b. Click **Close**.
7. To ensure that the printer and the domain controller are synchronized, enable and configure NTP settings:
   a. For NTP, click **Edit**.
   b. Synchronize the domain controller time with the time set on the device.

   Note: Xerox recommends that you enable NTP to ensure time synchronization.

8. To return to the Login Methods page, click **Close**.

To associate an LDAP server with your Domain Controller for authorization or personalization, for LDAP Server Mapping, click **Add LDAP Mapping**.

Configuring OCSP Validation Server Settings

If you have an OCSP server, or an OCSP certificate validation service, you can configure the printer to validate certificates installed on the domain controller.

Before you begin, add a domain controller. Refer to Domain Controller.

1. On the Login Methods page, for Certificate Validation, click **Edit**.
2. Select a validation method, then click **Next**.
3. On the Required Settings page, type the URL of the OCSP server.
4. To ensure that the printer can communicate with the OCSP server and the domain controller, configure your proxy server settings as needed.
5. For each domain controller listed, for Domain Controller Certificate, select the corresponding domain controller certificate from the menu. If there are no certificates installed, click **Install Missing Certificate**.
6. Click **Save**.

Setting the Inactive Time Limit

1. On the Login Methods page, for Smart Card Inactivity Timer, click **Edit**.
2. Specify the maximum amount of time before a user is logged out automatically. Type the time in minutes.
3. Click **Save**.

Disabling the Logout Confirmation Prompt

1. On the Login Methods page, for Log Out Confirmation, click **Edit**.
2. To disable the log out confirmation prompt on the device control panel, select **Yes**.

3. Click **Save**.

Specifying the Method the Printer Uses to Acquire Email Address of Users

1. On the Login Methods page, for Acquired Logged-in User's Email Address, click **Edit**.
2. For Acquire logged-in user's email address from, select an option:
   - **Auto** instructs the printer to attempt to acquire the email address of the user from the Smart Card. If an email address is not associated with the Smart Card, the printer searches the Network Address Book. If an email address is not found, the printer uses the email address specified in the From field. Edit From field settings on the Required Settings tab of the Email Setup page.
   - **Only Smart Card** instructs the printer to acquire the email address of the user from the Smart Card.
   - **Only Network Address Book (LDAP)** instructs the printer to search the Network Address Book to acquire the email address of the user.
3. To configure LDAP server settings, under Server Configuration, for Network Address Book (LDAP), click **Edit**.
4. To enable or disable Personalization, under Feature Enablement, for Acquire Email from Network Address Book, click **Enable Personalization** or **Disable Personalization**.
5. Click **Save**.

Customizing the Supported Smart Card List

You can customize the list of supported smart cards.

⚠ Caution: Xerox recommends that you use this feature only with the assistance or direction of qualified Xerox personnel.

To access the Customize Supported Smart Card List feature:

1. In the Embedded Web Server, click **Properties > Login/ Permissions/ Accounting**.
2. Click **Login Methods**.
3. For Control Panel & Website Login Methods, click **Edit**.
4. Click **Customize Supported Smart Card List**.
5. Follow the instructions provided to you by your Xerox representative.
6. To return to the Edit Login Methods page, click **Close**.

Restoring the Default Supported Smart Cards List

You can restore the supported smart card list to the default list provided by Xerox.

1. In the Embedded Web Server, click **Properties > Login/ Permissions/ Accounting**.
2. Click **Login Methods**.
3. For Control Panel & Website Login Methods, click **Edit**.
4. Click **Customize Supported Smart Card List**.
5. To restore the default smart card list, in the Restore Xerox Default Supported Smart Cards List area, click **Restore**.
6. To return to the Edit Login Methods page, click **Close**.

Configuring Single Sign-On

The Single Sign-On feature requires that the Xerox® Connect for Microsoft® OneDrive subscription-based app is installed and accessible on the device. For details on creating a Xerox® App Gallery account and installing Xerox® App Gallery apps, refer to the *Xerox® EC8036/EC8056 Color Multifunction Printer User Guide*.

The Single Sign-On feature allows the logged-in user to scan to and print from Microsoft® OneDrive without a separate login to Microsoft® OneDrive. The Single Sign-On feature uses an identity provider that facilitates the communication of authentication information between your device and Microsoft® OneDrive. As a result of this communication, Microsoft® Azure Active Directory grants the logged-in user access to Microsoft® OneDrive without requiring a second login.

Note: You can use Single Sign-On with the following login methods:

- **User Name / Password Validate on the Network**: This feature works with network authentication when network authentication is configured with a Kerberos authentication server.
- **Smart Cards**: This feature works with CAC and PIV smart card types.

To configure the Single Sign-On feature:

1. In the Embedded Web Server, click **Properties > Login/ Permissions/ Accounting**.
2. Click **Login Methods**.
3. In the Configuration Settings area, for Single Sign On Identity Provider, click **Edit**.
4. On the Single Sign On Identity Provider screen, for Setup, select **Enable**.
5. For AD FS Endpoint Path, type the path to your Active Directory Federation Services (AD FS) server.

   Note: Xerox supports only the `trust/13/windowstransport` endpoint.
6. If required, to validate the AD FS certificate, select **Validate the AD FS Server Certificate**. To view installed certificates, click **View Xerox Device Certificates**.
7. For SAML Token Access Code, type a code with 14–64 characters.

   Note: If a SAML Token Access Code was not entered previously, a red asterisk (*) appears. If a SAML Token Access Code was entered previously, the red asterisk does not appear, but the text field remains blank. You can type a new code, but a new code is not required.
8. Click **Save**.

Authorization

Authorization is the function of specifying the features that users are allowed to access, and the process of approving or disapproving access. You can configure the printer to allow users to access the printer, but restrict access to certain features, tools, and apps. For example, you can allow users to access copying but restrict access to scanning. You can also control access to features at specific times of the day. For example, you can restrict a group of users from printing during peak business hours.

There are two types of authorization:

- **Local Authorization** verifies user information on the printer to approve access.
- **Network Authorization** verifies user information stored externally in a network database, such as an LDAP directory, to approve access.

Configuring Authorization Settings

Setting the Authorization Method

1. In the Embedded Web Server, click **Properties > Login/Permissions/Accounting**.
2. Click **User Permissions**.
3. To change the User Permissions Method, for Control Panel & Website Login Methods, click **Edit**.
4. For User Permissions Method, select an option.
5. Click **Save**.

Configuring Local Authorization Settings

When you configure local authorization, the printer references the user database for authorization information for the authenticated user.

To configure local authorization:

- Add user information to the user information database.
- Configure User Permissions.

The User Permissions page in the Embedded Web Server provides links to authorization configuration settings.

1. In the Embedded Web Server, click **Properties > Login/Permissions/Accounting**.
2. Click **User Permissions**.

Configuring Network Authorization Settings

When you configure network authorization, the printer references an authorization server for authorization information for the authenticated user.

To configure network authorization:

- Provide information about your authorization server and configure authorization server settings.
- Configure User Permissions.

The User Permissions page in the Embedded Web Server provides links to authorization configuration settings.

1. In the Embedded Web Server, click **Properties > Login/Permissions/Accounting**.
2. Click **User Permissions**.

Configuring Network Authorization Server Settings

1. On the User Permissions page, for LDAP Server or SMB Server, click **Edit**.

2. If you are using an LDAP server for authorization, configure LDAP server settings as needed. For details, refer to LDAP.

   Note: The device uses the primary LDAP server for authentication, authorization, and personalization. The primary LDAP server appears in the Embedded Web Server on the LDAP Server page. If you have configured LDAP server settings, when you select LDAP as the network authentication or authorization method, the device uses this server automatically. The device only uses alternate LDAP servers for authorization and personalization when primary LDAP server communication fails.

3. If you are using an SMB server for authorization:

   a. For Configuration, type the Default Domain.

   b. Select the address type.

   c. Type the appropriately formatted IP address.

   d. For Login Credentials to Access SMB Server, select an option

      - **None**: This option does not require the device to provide the server a user name or password.
      - **Logged in User**: This option instructs the device to log in to the repository using the credentials of the logged-in user.
      - **Device**: This option uses the information provided in the Login Name and Password Fields to access the server.

   e. If you select Device, type the Login Name and Password used to access the server. Type the password, then type the password again to verify.

   f. To update the password for an existing Login Name, select **Select to save new password**.

   g. Click **Save**.

User Permissions

You can control access to apps, tools, printing times, and methods for a group of users.

Print permissions are rules that allow you to control printing times and methods for a group of users. You can:

- Restrict color printing, requiring users to print in black and white.
- Restrict 1-sided printing, requiring users to print 2-sided.
- Restrict a Job Type, such as Secure Print.
- Restrict access to specific paper trays.
- Specify the software applications from which users are allowed to print.
- Restrict printing, color printing, and 1-sided printing from specific software applications.

Apps and Tools permissions are rules that allow you to control access to features or configuration settings for a group of users. You can configure Apps and Tools to:

- Restrict access to specific apps, such as Copy, Email, or Fax.
- Restrict access to settings managed at the control panel, on the Tools menu.
- Restrict access to settings managed in the Embedded Web Server, on the Properties tab.

Note: Not all options listed are supported on all devices. Some options apply only to a specific device model, configuration, operating system, or driver type.

User Roles

A role is a set of permissions associated with a group of users. To edit permissions for a group of users, you edit permissions for a role.

There are three types of roles:

- The **Non-Logged-In Users Role** applies to any user who accesses the printer, but is not authenticated. This role also applies to anyone who sends a job that is not associated with a user name or job owner. Examples are a job sent using LPR, or a job sent from a mainframe application.
- **Logged-In Users Roles** are roles that you create. These roles apply to authenticated users only. You can assign specific users or user groups to the role, or you can create a role that applies to all authenticated users.
- **Device System Roles** give administrator privileges to logged-in users. These roles apply to authenticated users only. You can assign specific users or user groups to the role, restrict access to specific features, and restrict access to specific days and times. There are two predefined roles that you can modify as needed. You can create roles with access permissions that you define. The predefined roles are as follows:
  - **Device Administrator**: This role allows unrestricted access to all features, including Tools.
  - **Accounting Administrator**: This role allows unrestricted access to all features, including accounting management features.

Non-Logged-In Users

Editing Print Permissions for the Non-Logged-In Users Role

1. In the Embedded Web Server, click **Properties > Login/Permissions/Accounting**.
2. Click **User Permissions**.
3. For User Permission Roles, click **Edit**.
4. Click the **Non-Logged-In Users** tab.
5. For the Non-Logged-In User Permission Role, for Actions, click **Edit**.
6. Click the **Print** tab.
7. To restrict print permissions, for the print setting that you want to restrict, click **Edit**.

Setting Printing Time Restrictions

1. On the When Users can Print (Non-Logged-In User) page, for Allow Printing, select when users can print:
   - To allow printing at all times, select **Always**.
   - To allow printing on weekdays only, select **Monday – Friday from**, then select when users are allowed to print from the From Time and To Time menus.
   - To allow printing on specific days during a specific time range, select **Time of Day (Advanced)**. To set the time range for a day, for the day, click **Add Time Range**. Select when users are allowed to print from the From Time and To Time menus. To delete a time range, for the range, click the red X icon.
   - To restrict printing at all times, select **Never**.
2. Click **Save**.

Setting Black and White and Color Print Permissions

1. For When Users can Print, click **Edit**.
2. On the When Users can Print (Non-Logged-In User) page, for Color and Black and White printing independently, select **Make color printing more restrictive than black & white printing**.
3. Click **Save**.

   Note: Not all options listed are supported on all devices. Some options apply only to a specific device model, configuration, operating system, or driver type.

Setting 1-Sided Print Permissions

1. On the 1-Sided Printing page, for Role State, select an option:
   - To require users to print 2-sided, select **Not Allowed**.
   - To allow users to print 1-sided, select **Allowed**.
2. Click **Save**.

Setting Job Type Print Permissions

1. On the Job Types page, in the Presets area, select an option:
   - To allow users to print any job type, select **Allow all Job Types**.
   - To require that users only send secure print jobs, select **Only Allow Secure Print**.
   - To allow only the job types that you specify, select **Custom**.
2. If you selected Custom, under Role State, for each job type, select an option:
   - To allow users to use the job type, select **Allowed**.
   - To restrict users from using the job type, select **Not Allowed**.
3. To allow or restrict all job types, select an option:
   - To lock all job types, click the **Lock All** icon.
   - To unlock all job types, click the **Unlock All** icon.
4. Click **Save**.

Setting Paper Tray Print Permissions

1. To restrict users from using a paper tray, for the paper tray, select **Not Allowed**.
2. To allow or restrict printing from all paper trays, select an option:
   - To lock all paper trays, click the **Lock All** icon.
   - To unlock all paper trays, click the **Unlock All** icon.
3. Click **Apply**.

Setting Application Print Permissions

1. On the Applications page, click **Add New Application**.
2. From the Application List, select an application.

   Note: To add an application to the list, you can also submit a print job from that application to the printer.
3. To restrict users from using the printing method, for a permission type, select **Not Allowed**.
4. Click **Apply**.

   Note: Not all options listed are supported on all devices. Some options apply only to a specific device model, configuration, operating system, or driver type.

Managing the List of Applications

Application Manager allows you to associate Application IDs with an Application Group. Application Group Names for common application types appear in the table at the bottom of the Application Manager page. The associated Application IDs appear next to each of the Application Group Names. An Application ID identifies the application from which the job was sent. To control print permissions for an application, the Application ID of the application must be associated with an Application Group Name. If you send a job from an application that is not in the default list, a new Application ID appears in the Custom Application ID list.

1. On the Applications page, click **Application Manager**.
2. To associate a custom Application ID with an existing Application Group, for the custom application ID, click **Merge With**.
   - For Merge With the Application Group, select an application from the list.
   - Click **Save**.
3. To create an Application Group from a custom Application ID, for the custom application ID, click **Make This A Group**.
   - For Application Group Name, type a name for the group.
   - Click **Save**.
4. To rename an Application Group, for the custom application ID, click **Rename**.
5. To delete a custom Application ID, for the custom application ID, click **Delete**.

6. To delete or disassociate a custom Application ID from an Application Group Name, for the Application Group, click **Manage**.
   - To remove the Application ID, click **Un-merge**. To delete the Application ID, click **Delete**.
   - Click **Close**.
7. To create a custom Application ID, click **Add Manually**.
   - For Application ID, type an Application ID.
   - Click **Save**.
8. To return to the Applications page, click **Close**.

Editing Apps and Tools Permissions for the Non-Logged-In Users Role

1. In the Embedded Web Server, click **Properties > Login/Permissions/Accounting**.
2. Click **User Permissions**.
3. For User Permission Roles, click **Edit**.
4. Click the **Non-Logged-In Users** tab.
5. For Actions, click **Edit**.
6. Click the **Apps and Tools** tab.
7. For Presets, select an option.
8. If you selected Custom, for each app, select a Role State:
   - To allow users to use the app, select **Allowed**.
   - To restrict users from using the app, select **Not Allowed**.

   Note: Selecting **Not Allowed** hides the app icon on the device control panel touch screen.
9. To allow or restrict all apps, select an option:
   - To lock all apps, click the **Lock All** icon.
   - To unlock all apps, click the **Unlock All** icon.
10. Click **Apply**.

    Note: You cannot restrict access for logged-in users and allow access for non-logged in users. To restrict access for non-logged-in users, click **Auto Correct**.

Logged-In Users

Adding a New Role for Logged-In Users

To edit permissions for a specific group of users, first create a role.

1. In the Embedded Web Server, click **Properties > Login/Permissions/Accounting**.
2. Click **User Permissions**.
3. For User Permission Roles, click **Edit**.
4. Click the **Logged-In Users** tab.
5. To create a role, click **Make Your Own Permission Roles** or **Add New Role**.
6. For New Permission Profile, type a name and description for the role.

7. To configure access for users to apps, click **View Quick Setup Options**, then for Allow users, select an option.

   Note: If you do not select an option, print permissions are set to Allowed. The default permissions for a new role are the same as the permissions for the Non-Logged-In user role.

8. Click **Create**.
9. To assign users to the role, or to configure permissions for the role, click the **Print** link or the **Apps and Tools** link.
10. To save, click **Apply**.

Assigning Users to a Role for Local Authorization

After you configure local authorization, add user information to the user database, and create a user-defined permission role, you can assign users to the role.

1. In the Embedded Web Server, click **Properties > Login/Permissions/Accounting**.
2. Click **User Permissions**.
3. For User Permission Roles, click **Edit**.
4. Click the **Logged-In Users** tab.
5. To add users to a user-defined permission role, for the desired role, click **Edit User Mappings**.
6. For Methods, select an option.
   - To assign specific users to the role, select **Select Individual Users**, then from the list of user names, select a user.
   - To assign all users to the role, select **All Logged-in Users**. To exclude individual users from this list, select **Exceptions**, then from the list of user names, select users.
7. To create a user entry and add it to the role, click **Add New User**.
8. Click **Apply**.

Assigning User Groups to a Role for Network Authorization

After you configure network authorization, you can assign LDAP or SMB groups of users to roles.

1. In the Embedded Web Server, click **Properties > Login/Permissions/Accounting**.
2. Click **User Permissions**.
3. For User Permission Roles, click **Edit**.
4. Click the **Logged-In Users** tab.
5. For a role, click **Edit User Mappings**.
6. Under Methods, select an option:
   - **Assign Groups**: This option allows you to select the user groups that you want to assign to the role.
   - **All Logged-in Users**: This option assigns all user groups to the role.

   To select specific user groups to remove from the role, select **All Logged-in Users** then select **Exceptions**. All other user groups are assigned to the role.
7. If you chose Select Individual Users, or Exceptions, select user groups from the list.

a. If you know the name of the group you want to add, for Assign Groups, type the group name, then click **Search for Groups**.

> **Note:** If LDAP or SMB server settings are not configured, you cannot search for and add groups.

b. To add a group to the role, select the group from the list, then click **Add**.
Groups assigned to the role appear in the Users in Assigned Groups list.

c. To remove a group, select the group in the Users in Assigned Groups list, then click **Remove**.
To remove all groups from the list, click **Remove All**.

8. Click **Apply**

Editing a Logged-In User Role

1. In the Embedded Web Server, click **Properties > Login/Permissions/Accounting**.
2. Click **User Permissions**.
3. For User Permission Roles, click **Edit**.
4. Click the **Logged-In Users** tab.
5. For the role that you want to edit, click **Edit User Mappings**.

   > **Note:** You cannot edit permissions for the System Administrator or Accounting Administrator roles. Users assigned to the System Administrator role can access all features of the device. Users assigned to the Accounting Administrator role can access accounting features only.

6. To assign users to the role, or to configure permissions for the role, click either the **Print** tab or the **Apps and Tools** tab.
7. To save, click **Apply**.
   For details, refer to Editing Print Permissions for the Non-Logged-In Users Role and Editing Apps and Tools Permissions for the Non-Logged-In Users Role.

   > **Note:** For each user permission type, you cannot restrict access for logged-in users and allow access for non-logged-in users. To restrict access for non-logged-in users, for a permission setting, click the **Auto Correct** link.

Device Management

Adding a New Device System Role

To edit permissions for a specific group of users, first create a role.

1. In the Embedded Web Server, click **Properties > Login/Permissions/Accounting**.
2. Click **User Permissions**.
3. For User Permission Roles, click **Edit**.
4. Click the **Device Managements** tab.
5. To create a role, click **Add New Role**.
6. For Enter Role Name & Description, type a name and description for the role.
7. Click **Create**.

8. To assign users to the role, click the **Assign Users to Role** tab, then select an option.
   - **Select Individual Users**: This option allows you to add specific members from a list of users.
   - **All Logged-In Users**: This option allows you to add all users that are logged in to the device.

   Note: To exclude a user from the role, select **Exceptions**, then clear the check box for the user name.

9. To save, click **Apply**.

Specifying Job Override Policies

Use Job Override Policies to specify what happens when a user without appropriate print permissions sends a color or 1-sided print job to the printer.

1. In the Embedded Web Server, click **Properties > Login/Permissions/Accounting**.
2. Click **User Permissions**.
3. For Job Override Policies, click **Edit**.
4. For Color Printing, select **Print Job in Black & White**, or **Delete Job**. If an unauthorized user sends a color job, the job prints in black and white or is deleted.
5. For 1-Sided Printing, select **Print Job 2-Sided**, or **Delete Job**. If an unauthorized user sends a 1-sided job, the job prints 2-sided or is deleted.
6. Click **Save**.

   Note: Not all options listed are supported on all devices. Some options apply only to a specific device model, configuration, operating system, or driver type.

Troubleshooting Conflicting Permissions

1. In the Embedded Web Server, click **Properties > Login/Permissions/Accounting**.
2. Click **User Permissions**.
3. For Action, for User Permission Roles, click **Edit**.
4. Click **Troubleshooting**.
5. To see a summary of permissions for a user, on the Permission Role Summaries tab, click **Permissions Summary**.

Temporarily Disabling Print Permissions for all Users

1. On the Troubleshooting page, click the **Permission Enablement** tab.
2. To disable print restrictions for all users, next to Print, under Actions, select **Disable**.
3. Click **Apply**.

Personalization

Personalization is the process of customizing apps for a specific user. When a user selects the Scan to Home or Email Scanning feature, the device searches an LDAP directory for the home directory and email address of that user.

HTTPS (TLS)

To establish an HTTP Secure (HTTPS) connection to the printer, you can use TLS to encrypt data sent over HTTP. Features that require HTTPS use TLS automatically. You can use TLS encryption for protocols such as LDAP and SMTP.

Note:

- TLS encryption is protocol-independent. You can enable TLS for protocols or scan destinations as needed.
- When the device uses HTTPS, all pages in the Embedded Web Server contain https:// in the URL.

Using TLS for all HTTP Communication (HTTPS)

1. In the Embedded Web Server, click **Properties > Connectivity > Setup**.
2. For Protocol, for HTTP, click **Edit**.
3. Click the **HTTP** tab.
4. For Force Traffic over HTTPS, select **Yes**. Change the default port number as needed.
   a. From the Choose Device Certificate menu, select the Device Certificate to use for HTTPS.
   b. To view the selected certificate details, or to save the certificate to your computer, click **View/Save**.
   c. If you are using the Xerox Default Device Certificate, you can install the Xerox Generic Root Certificate Authority in your Web browser. Installing the Xerox Generic Root Certificate Authority ensures that your browser trusts the device. To download the certificate, click **Download the Xerox Generic Root Certificate Authority**.
5. Click **Save**.

FIPS 140-2

If FIPS 140-2 encryption is required, all computers, servers, browser software, security certificates, and applications must comply with the standard or operate in FIPS-compliant mode. Transmitted and stored data must be encrypted as specified in United States Federal Information Processing Standard (FIPS) 140-2, Level 1. You can enable the printer to check that the current configuration ensures the specified encryption.

Enabling FIPS 140 Mode can prevent the printer from communicating with network devices that communicate using protocols that do not use FIPS-compliant encryption algorithms. To allow non-FIPS-compliant protocols or features when FIPS 140 mode is enabled, acknowledge the notification of non-compliance during the validation process.

When you enable non-FIPS-compliant protocols after FIPS mode is enabled, a message appears that indicates that the protocols use non-FIPS-compliant encryption algorithms. Examples of non-FIPS-compliant protocols include SMB, Digest HTTP authentication for AirPrint scanning and Mopria scanning, and wireless networking.

When you enable FIPS-140 mode, the device performs the following checks to validate the current configuration:

- The device validates all pre-installed and user-installed certificates on the device for FIPS compliance. Certificates include the default Xerox Device Certificate, CA-signed Device Certificates, Root/Intermediate Certificates, and Peer Device/Domain Controller Certificates.

  The digital certificates that are installed on the device enable various workflows, including:

  - Establishing a secure connection between the device acting as a server and a peer device acting as a client
  - Establishing a secure connection between the device acting as a client, and a peer device acting as a server
  - Verifying the identity of a peer device
  - Validating that a peer device is trusted
- The device checks features and protocols for non-compliant encryption algorithms. For example, HTTP Digest authentication for AirPrint scanning and Mopria scanning use encryption algorithms that are not FIPS-compliant.

Validation involves a series of iterative checks on the device configuration. After each check, information and links appear in a table at the bottom of the page.

- To disable a non-compliant feature, or protocol, click the appropriate link.
- To replace any non-compliant certificates, click the appropriate link.
- To acknowledge that you allow the printer to use non-compliant features and protocols, click the appropriate link.

  Note:

  - FIPS is not enabled until the system administrator receives notification that all configuration checks are complete and the device is restarted.
  - Some configuration actions require you to move from the FIPS page to other Embedded Web Server pages. After completing these actions, to continue the FIPS validation checks and enablement, restart the FIPS checks.

Enabling FIPS 140 Mode and Checking for Compliance

1. In the Embedded Web Server, click **Properties > Security > Encryption**.
2. Click **FIPS 140-2**.
3. Click **Enable**.
4. Click **Run Configuration Check and Apply**.

   Note:

   - When FIPS 140 Mode is enabled, only FIPS-compliant certificates can be installed on the device.
   - When the validation completes, the system administrator receives notification that the configuration check passed. After the system administrator restarts the device, the FIPS status details update.

5. To enable FIPS, restart the device.

FIPS Configuration Check

The FIPS Configuration Check page displays a pass or fail message as a result of the FIPS configuration check.

To complete the FIPS configuration check:

- If the configuration check passes, to save and restart the printer, click **Reboot Machine**.
- If the configuration check fails, conditions that caused the failed test appear in the section labeled Feature Needing Attention. For each reason, a link is provided in the table at the bottom of the page. To disable the protocol, replace the certificate, or allow the printer to use the non-compliant protocol, click the appropriate link.

Stored Data Encryption

You can encrypt user data on the printer hard drive to prevent unauthorized access to data stored on the drive.

Enabling Encryption of Stored Data

Caution: Before you begin, back up all jobs and folders. When you enable the data encryption feature, the device restarts and interrupts or deletes current jobs.

1. In the Embedded Web Server, click **Properties > Security > Encryption**.
2. Click **User Data Encryption**.
3. For User Data Encryption Enablement, select **Enabled**.
4. To save the new settings, click **Apply**. To retain the previous settings, click **Undo**.

IP Filtering

You can prevent unauthorized network access by creating an IP Filter to block or allow data sent from particular IP addresses.

Creating or Editing an IP Filter Rule

1. In the Embedded Web Server, click **Properties > Security**.
2. Click **IP Filtering**.
3. Click **Add IP Filter**.
4. For Define Protocol, select the protocol.
5. For Define Action, select how you want the filter to manage the incoming packet.
   - If you want the device to allow the packet access, select **Accept**.
   - If you want the device to ignore the packet, select **Drop**.
   - If you want the device to reject the packet and send an ICMP message back to the source host, select **Reject**.
6. Type the Source IP Address.
7. Type a number from 0 through 32 for the Source IP Mask that uses this IP filter rule. The range of 0–32 corresponds to the 32-bit binary number comprising IP addresses. For example:
   - The number 8 represents a Class A address with a mask of 255.0.0.0.
   - The number 16 represents a Class B address with a mask of 255.255.0.0.
   - The number 24 represents a Class C address with a mask of 255.255.255.0.
8. If you selected TCP or UDP, type the Destination Port for the rule to manage. If the incoming packet is not sent to this port, the rule is ignored.
9. If you selected ICMP, type the ICMP Message Type for the rule to manage.
10. To specify the order that actions are performed, for Precedence Order, select an option. Actions are performed in the order defined in the rule list. To arrange rule execution order, refer to IP Filtering.
11. Click **Save**.

Editing an IP Filter Rule

1. In the Embedded Web Server, click **Properties > Security**.
2. Click **IP Filtering**.
3. For the IP filter rule you want to edit, click **Edit**.
4. Make changes to the settings as needed.
5. Click **Save**.

Arranging the Execution Order of IP Filter Rules

1. In the Embedded Web Server, click **Properties > Security**.

2. Click **IP Filtering**.
3. Click an IP filter rule.
4. For Move Up/Down, click the appropriate arrow.

Logs

Audit Log

The Audit Log feature records security-related events that occur on the device. You can download the log as a tab-delimited text file to review for potential problems or security issues.

Enabling Audit Log

1. In the Embedded Web Server, click **Properties > Security**.
2. Click **Audit Log**.
3. For Device Audit Log, click **Enabled**.
4. Click **Apply**.

   Note: When McAfee antivirus software is enabled, this option cannot be disabled.

Enabling Automatic Log Transfer

The system administrator can use Secure FTP to send the device audit log file to a server. You can transfer the audit log on demand or schedule it as a daily service.

Note: Secure FTP applies to IPv4 only.

To enable automatic log transfer:

1. In the Embedded Web Server, click **Properties > Security**.
2. Click **Audit Log**.
3. For Automatic Log Transfer, click **Enabled**.
4. For Schedule Automatic Log Transfer, click **Enabled**.
5. To establish an automatic daily log transfer time, type a time, then select **AM** or **PM**.
6. For Automatic Log Transfer Server, select an option, then type the repository server IP address or host name.
7. For Path, type the complete path name.
8. For Login Name, type the login credentials.
9. For Password, type a password. For Retype password, type the password again.
10. Click **Apply**.

Enabling Secure Protocol Logs

Protocol logs provide information about connection-specific secure protocols, such as HTTPS, IPsec, SSH, and TLS. Each enabled protocol generates a unique protocol log that is populated with information. If a protocol is not enabled, the corresponding protocol log still appears but is not populated with information. Protocol log functionality complies with Common Criteria requirements.

Note: If you enable or disable the protocol log feature, the device restarts.

To enable protocol logs:

1. In the Embedded Web Server, click **Properties > Security > Logs**.
2. Click **Audit Log**.
3. For Secure Protocol Log, click **Enabled**.
4. Click **Apply**.
5. Follow the onscreen instructions to restart the device.

   Note: The protocol logs download in a **.zip** file archive that contains up to five text files. If the protocol log feature is enabled, the protocol log **.zip** file archive contains five text files. The **.zip** file name format appears as `serialnumber_year-month-date-timezone_offset-time_auditfile.zip`.

Saving an Audit Log

1. In the Embedded Web Server, click **Properties > Security**.
2. Click **Audit Log**.
3. Click **Export Audit Log**.
4. Right-click the **Download Log** link, then save the compressed **.zip** file to your computer.
5. Extract the **auditfile.txt** file from the **.zip** file, then open it in a spreadsheet application that can read a tab-delimited text file.

Saving an Audit Log to a USB Flash Drive

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **Security Settings > Audit Log**.
3. Touch **Download Log**.
4. Insert your USB Flash drive into the front USB port. The log file downloads automatically.
5. When the download completes, click **Close**.

Interpreting the Audit Log

The Audit Log is formatted into ten columns:

- **Index**: Column 1 lists a unique value that identifies the event.
- **Date**: Column 2 lists the date that the event happened in mm/dd/yy format.
- **Time**: Column 3 lists the time that the event happened in hh:mm:ss format.

- **Event ID**: Column 4 lists the type of event. The number corresponds to a unique description. For details, refer to Audit Log Event Identification Numbers.
- **Event Description**: Column 5 lists an abbreviated description of the type of event.

  Note:

  - One audit log entry is recorded for each network destination within a Workflow Scanning scan job.
  - For server fax jobs, one audit log entry is recorded for each server fax job, regardless of the number of destinations.
  - For LAN fax jobs, one audit log entry is recorded for each LAN fax job.
  - For email jobs, one audit log entry is recorded for each SMTP recipient within the job.
- **Other Event Details**: Columns 6–10 list other information about the event, such as:
  - **Identity**: User Name, Job Name, Computer Name, Printer Name, Folder Name, or Accounting Account ID display when Network Accounting is enabled.

    Note: Authentication must be configured to record the user name in the Audit Log.
  - **Completion Status**
  - **Image Overwrite Status**: The status of overwrites completed on each job. Immediate Image must be enabled.

Authentication Log

The authentication log contains details of access to the device, including login and logout times, and successful or unsuccessful login attempts.

To download the authentication log:

1. In the Embedded Web Server, click **Properties > Security > Logs > Authentication Log**.
2. Click **Device Authentication Log**.
3. To save the file to your computer, after the information processes, click **Save**.

The file name for the downloaded authentication log appears as `authLog.zip`, prefixed by the date and time.

Network Troubleshooting

The Network Troubleshooting Session provides a way to capture and record all network communication to and from the device.

Note:

- You can use Network Troubleshooting sessions for short-term problem identification.
- Starting a Network Troubleshooting session can result in degraded device performance.
- The data capture stops when either of the following limits is reached:
  - The allotted amount of time
  - The maximum file size
- After 72 hours, the data is removed securely from the device.

To set up a network troubleshooting session:

1. In the Embedded Web Server, click **Properties > Security > Logs > Network Troubleshooting**.
2. For Session Timespan, select a length of time in hours.

   Note: The capture stops automatically after the time duration.
3. To select specific ports for the troubleshooting session, click **Customize Captured Port Filters**.

   Note: All ports are included by default.

   a. For the ports that you want to include, select **Enable**.

      Note: The capture is limited to the selected ports.

   b. To change the properties of a selected port, click **Edit**. If needed, change the service name and port number, then click **Save**.

   c. To limit the capture to only one specific destination, select **Optional Destination IPv4 Address Filter**, then type the IP address.

   d. You can set the packet size of the capture. For Packet Size, type a value from 96–65535.

   e. Click **Save**.
4. To begin the network troubleshooting capture session, click **Start Session Now**, then click **OK**.

   Note:

   - To end a currently running session before the capture time has ended, click **Stop Session Now**, then click **OK**.
   - To delete the captured session, click **Clear Session**, then click **OK**.
5. To save a copy of the captured session, click **Download Log Now**.

Support Logs

Log files are text files of the recent device activity that are created and stored in the device. Log files are used to troubleshoot device and network problems. A Xerox Technical Customer Support representative can interpret the encrypted format log files.

Support Logs can include screenshots that are taken at the device control panel.

To capture a screenshot at the control panel, press the **Power** button, then touch the lower-left corner of the screen. To capture the screenshot, on the alert screen, touch **Take Screenshot**. After the screenshot is taken, the file name of the image appears on the screen. The file name includes the date, time, and serial number of the device.

The device can capture most screens. When pop-up windows are displayed, the device sometimes captures the underlying screen only.

The screenshot images are stored with the log files. The device can store up to three screenshots for a maximum of 7 days. After 7 days, the files are deleted. If more than three screenshots are taken, the older files are deleted.

The device also supports Enhanced Logging.. The Enhanced Logging feature enables the device to capture additional logs for specific functions or activities. A Xerox service representative can use the additional logs to investigate nonrepeatable or intermittent device issues. The device supports enhanced logging for a maximum of three features at a time.

To configure support log settings:

1. In the Embedded Web Server, click **Properties > Security > Logs > Support Logs**.
2. In the Information Level area, select options as needed:
   - To include the audit logs with the support log, select **Audit Logs**.

     Note: To check for Audit Log enablement, refer to Audit Log.

   - To include NVM data with the support log, select **Include NVM Data with Support Log Push**.
3. Click **Save**.
4. In the Download Files area, for Log Content, click **Start Download**.
   The Download Status page appears. This action can take several minutes to complete.
5. To save the files to your computer, after the information processes, click **Download File Now**.
   Save the log file to your computer. This action can take several minutes to complete.
6. To return to the Support Logs page, click **Close**.

   Note: The file name for the downloaded support log appears next to Log Identifier in the Send Files To Xerox area.

   To send files to Xerox for diagnostic purposes, in the Send Files to Xerox area, click **Send**.
7. To enable enhanced logging for specific features, in the Enhanced Logging area, click **Configure**.
   Then, configure settings as needed:

   Note: Enable the Enhanced Logging feature only if a Xerox service representative instructs you to do so.

   a. In the Feature 1 area, for **Feature**, select a feature from the list. Then, for **Log Level**, select **None**, **Low**, **Medium**, or **High**.

   b. To enable enhanced logging for a second feature, in the Feature 2 area, repeat step 7a.

c. To enable enhanced logging for a third feature, in the Feature 3 area, repeat step 7a.

d. In the Additional Logs area, to include SOAP logs, click the check box for **SOAP Logs**.

e. In the Additional Logs area, to include SMB logs, click the check box for **SMB Logs**.

f. In the **Scheduled Turn Off** area, set the duration for enhanced logging in days. The range is 1–30 days. The default value is 7 days. Set the time of day for the logging to stop.

g. Click **Start**.

To clear the settings for enhanced logging, click **Reset to Default**.

Note:

- Enablement of enhanced logging requires a device restart. The device restarts with increased logging levels for the selected features.
- Disablement of enhanced logging requires a device restart. The device restarts with logging set to default levels.

McAfee Embedded Control

McAfee Embedded Control consists of two security features:

- Enhanced Security maintains the integrity of printer software by monitoring system files and alerting you when an unauthorized change is made to a system file. This feature prevents general attacks, such as unauthorized read or write of protected files and directories. Enhanced Security prevents unauthorized files from being added to designated protected directories.
- Integrity Control is a software option that combines enhanced security features with the ability to monitor and prevent unauthorized executable files from running. Enable this option by providing a feature installation key on the Feature Installation page. To get a feature installation key, contact your Xerox representative.

You can configure the printer to send email alerts when a security event occurs. Email alerts can be sent to you or to a centralized management application such as McAfee ePolicy Orchestrator (McAfee ePO), Xerox® CentreWare® Web, or Xerox® Device Manager. For details about McAfee ePO and McAfee Embedded Control, visit www.mcafee.com.

To configure McAfee Embedded Control:

- To configure email alerts, for Email Alerts, click **Edit**.
- To provide details about your McAfee ePO server, for McAfee ePolicy Orchestrator Server, click **Edit**.
- To download and review security events recorded in the audit log, for Export Audit Log, click **Export**.

Note: The audit log is a tab-delimited file, compressed in **.zip** format. Use a file expansion utility, such as 7-zip, winRAR, or StuffIt Expander, and a text editor application, such as Notepad++, to read the file.

After you set the security level and configure alert options, the McAfee Embedded Control page in the Embedded Web Server provides links to related configuration settings.

1. In the Embedded Web Server, click **Properties** > **Security**.
2. Click **McAfee Embedded Control**.

Setting the Security Level

Unless you have acquired McAfee Integrity Control, Xerox recommends that you keep the security level set to the default setting, Enhanced Security.

McAfee Embedded Control has three security levels:

- Enhanced Security
- Integrity Control
- Disabled

Note: Only set the security level if necessary. The device comes standard with an Enhanced Security level, which is adequate in many cases.

1. In the Embedded Web Server, click **Properties** > **Security**.
2. Click **McAfee Embedded Control**.

3. To enable McAfee Embedded Control features, and configure Alert Feedback options, for Device Security Levels, click **Edit**.
4. To set the Security Level, for Security Level, select **Enhanced Security** or **Integrity Control**. To turn off McAfee Embedded Control security features, select **Disable McAfee Embedded Control**. Xerox recommends that you do not disable this feature.
5. If you selected Enhanced Security as the security level, click **Save**.
6. If you selected Integrity Control as the security level, click **Next**, enter the software feature installation key, then click **Apply**.

   Note: When you change the security level setting, the device restarts. The process takes several minutes.

Setting the Alert Options

You can configure the printer to alert you when a security event occurs.

To set the alert options:

1. In the Embedded Web Server, click **Properties > Security**.
2. Click **McAfee Embedded Control**.
3. To configure Alert Feedback options, for Device Security Levels, click **Edit**.
4. To configure the device to send email alerts:
   a. For Locally on the Device, select **Email Alerts**, then click **Save**.
   b. In the Configuration Setting area, for Email Alerts, click **Edit**.
   c. For Recipient Group Addresses, type valid email addresses for each applicable group.
   d. For each group with email addresses, select **Enable Group**.
   e. In the Recipient Group Preferences area, for McAfee Embedded Control, select the groups to receive alerts: **Group 1**, **Group 2**, **Group 3**.
   f. Click **Apply**.
   g. At the prompt, click **OK**.
5. Configure your alert feedback method.
   - To configure the device to send alerts to McAfee ePolicy Orchestrator Server, for McAfee Remote Solutions, select **McAfee's ePolicy Orchestrator Server**.
   - If you use the Embedded Web Server to manage your devices, configure security alerts in the Embedded Web Server.
   - If you use Xerox® CentreWare® Web to manage your devices, you can use Xerox® CentreWare® Web to send security alerts from registered devices.
   - If Xerox manages your devices, use Xerox®Device Manager to send security alerts from registered printers.
6. Click **Save**.

   Note: When McAfee Embedded Control features are enabled, the device records security events in the Audit Log.

Downloading the Audit Log

1. Click **Download Log**.
2. To view the audit log, in the **.zip** file window, click **Open**.
3. To save a copy of the audit log to a **.zip** file, click **Save**.

Testing Your Alert Configuration

To test your alert configuration by generating a test security event, click **Test Feedback Methods**.

Feedback Method Test Results

When the McAfee feature is enabled, it provides security that allows the device to identify and prevent attempts to read, write, or execute files that are stored on the printer. Based on the device configuration, the test generates alerts that are saved in the Audit Log as well as reported using other configured feedback methods. The system administrator can use the Audit Log to confirm that the feedback methods are configured properly. The four feedback methods that are supported include Email Alerts, McAfee ePolicy Orchestrator Server, CentreWare® Web, and Xerox Device Manager.

IPsec

Internet Protocol Security (IPsec) is a group of protocols used to secure Internet Protocol (IP) communications by authenticating and encrypting each IP data packet. It allows you to control IP communication by creating protocol groups, policies, and actions.

IPsec is designed to provide the following security services:

- Traffic encryption: This service prevents unintended recipients from reading private communications.
- Integrity validation: This service ensures that traffic has not been modified along its path.
- Peer authentication: This service ensures that traffic is coming from a trusted source.
- Anti-replay: This service protects against replay of the secure session.

IPsec Configuration Components

To configure IPsec, perform the following tasks.

1. Configure IPsec on the Xerox device.
2. Configure and define the components of IPsec security policies. Refer to Defining a Security Policy.
3. Configure IPsec on the remote host.
4. Send data over a secure connection.

To access the IPsec page, in the Embedded Web Server, click **Properties > Security > IPsec**.

Managing Security Policies

IPsec security policies are sets of conditions, configuration options, and security settings that enable two systems to agree on how to secure traffic between them. You can have multiple policies active at the same time, however, the scope and policy list order determines the overall policy behavior.

Defining a Security Policy

1. Click **Security Policies** at the top of the IPsec page.
2. For Define Policy, select a Host Group from the menu. For details, refer to Managing Host Groups.
3. Select a Protocol Group from the menu. For details, refer to Managing Protocol Groups.
4. Select an Action from the menu. For details, refer to Managing Actions.
5. Click **Add Policy**.

Prioritizing a Security Policy

To prioritize policies, under Saved Policies, select the policy you want to move, then click the **Promote** or **Demote** buttons.

Editing or Deleting a Security Policy

To delete a policy, under Saved Policies, select the policy and click **Delete**.

Managing Host Groups

Host groups are groupings of computers, servers, or other devices that you want to control using security policies. A host group is a set of addresses over which to apply the policy.

Note: The host groups Any and Local Subnet are preconfigured.

Creating a New Host Group

1. Click **Host Groups** at the top of the IPsec page.
2. Click **Add New Host Group**.
3. Type a Name and a Description for the group.
4. Under Address List, select **IPv4** or **IPv6**.
5. Select an Address Type. Options are **Specific**, **All**, or **Subnet**.
6. Type the appropriately formatted IP address.
7. To continue to add addresses to the group, click **Add**.
8. To delete addresses, next to any address, click **Delete**.
9. Click **Save** to apply the new settings or **Undo** to retain the previous settings.

Editing or Deleting a Host Group

To edit or delete a host group, select the host group from the list, and click **Edit** or **Delete**.

Managing Protocol Groups

Protocol groups are logical groupings of selected protocols. To apply specific security policies for selected protocols, create a Protocol Group.

Protocol groups define the upper layer protocols destined to become part of the security policy. The upper layer protocols include All, FTP, HTTP, SMTP, and IPP, and other protocols. You can configure custom protocols. For details, refer to Creating a Protocol Group.

The following protocol groups are predefined:

- **All**: This group includes all protocols.
- **System Services**: This group includes all protocols necessary to start and configure the Xerox device, except ISAKMP, the IPsec port.
- **Non-System Services**: This group includes all protocols that are not included in Systems Services, except ISAKMP.

Creating a Protocol Group

1. On the IPsec page, click **Protocol Groups**.
2. Click **Add New Protocol Group**.
3. Type a Name and a Description for the group.
4. For App Name, select the protocols that you want to add to the group.
5. To control an app that is not listed, in the Custom Protocols area, for Service Name, select the check box. Type a name for the app.
6. For Protocol, select **TCP** or **UDP**.
7. Type the port number, and specify if the printer is the server or client.
8. To apply the new settings, click **Save**. To retain the previous settings, click **Undo**. To return to the previous page, click **Cancel**.

Editing or Deleting a Protocol Group

To edit or delete a protocol group, select the protocol group from the list, and click **Edit** or **Delete**.

Managing Actions

Use actions to more specifically manage how IPsec controls dependent protocols. Two actions are predefined. You can create custom protocols.

The following actions are predefined:

- **Pass**: This action allows unencrypted traffic.
- **Block**: This action blocks unencrypted traffic.

Creating a New Action

1. Click **Actions** at the top of the IPsec page.
2. Click **Add New Action**.
3. On the Step 1 of 2 page, under IP Action Details, type in the Name. This field is required.
4. In the Description field, type a description for the action, if desired.
5. Under Keying Method, select **Manual Keying** or **Internet Key Exchange (IKE)**.

   Note: Select Manual Keying if client devices are not configured for or do not support IKE.

6. If you selected IKE, under Pre-shared Key Passphrase, type the passphrase, then click **Next**.

Configuring Manual Keying Settings

Manual Keying is used when client systems either do not support IKE or are not configured for IKE.

1. For IPsec Mode, select **Transport Mode** or **Tunnel Mode**.
   Transport mode only encrypts the IP payload, whereas Tunnel mode encrypts the IP header and the IP payload. Tunnel mode provides protection for an entire IP packet by treating it as an Authentication Header (AH), or Encapsulating Security Payload (ESP).

2. If you selected Tunnel Mode, for Enable Security End Point Address, select the address type. Options are **Disabled**, **IPv4 Address**, or **IPv6 Address**.
3. For IPsec Security, select **ESP**, **AH**, or **BOTH**.
4. In the Security Parameter Index: IN field, type a 32-bit number larger than 256 that identifies the inbound Security Association (SA).
5. In the Security Parameter Index: OUT field, type a 32-bit number larger than 256 that identifies the outbound Security Association (SA).
6. If you selected ESP under IPsec security, for Hash, select **SHA-1**, **SHA-256**, or **None**.
7. For Enter Keys as, select **ASCII format** or **Hexadecimal number**.
8. If you selected SHA-1 or SHA-256 for Hash, enter a Hash Key. For Hash Key: IN and Hash Key: OUT, type an ASCII key or a Hexadecimal key.

   Note: Hash key lengths are determined by the security selection.

   - For SHA-1, the key lengths are 20 ASCII or 40 Hexadecimal.
   - For SHA-256, the key lengths are 32 ASCII or 64 Hexadecimal.
9. If you selected ESP or BOTH for the IPsec Security type, for Encryption, select an option.

   Note: If you are configuring an IPsec security policy to communicate with a Linux computer, and you selected BOTH for the security type, select 3DES encryption. If you select AES encryption, the data transfer rate is reduced.
10. If you selected encryption, enter an Encryption Key. For Encryption Key: IN and Encryption Key: OUT, type an ASCII key or a Hexadecimal key.

    Note: The Encryption key lengths are determined by the encryption selection.

    - For AES, the key lengths are 16 ASCII or 32 Hexadecimal.
    - For 3DES, the key lengths are 24 ASCII or 48 Hexadecimal.
11. Click **Save**.

Configuring Internet Key Exchange Settings

IKE is a keying protocol that allows automatic negotiation and authentication, anti-replay services, and CA support. It can also change encryption keys during an IPsec session. IKE is used as part of virtual private networking.

IKE Phase 1 authenticates the IPsec peers and sets up a secure channel between the peers to enable IKE exchanges. IKE Phase 2 negotiates IPsec SAs to set up the IPsec tunnel.

1. In the IKE Phase 1 area, for Key Lifetime, type the length of time until the key expires in **Seconds**, **Minutes**, or **Hours**. When a key reaches this lifetime, the SA (Security Association) is renegotiated and the key is regenerated or refreshed.
2. For DH Group, select **DH Group 2** or **DH Group 14**:
   - **Group 2**: This option provides a 1024-bit Modular Exponential (MODP) keying strength.
   - **Group 14**: This option provides a 2048-bit MODP keying strength.

3. In the IKE Phase 2 area, for IPsec Mode, select **Transport Mode** or **Tunnel Mode**.

   Note: Transport mode only encrypts the IP payload, whereas Tunnel mode encrypts the IP header and the IP payload. Tunnel mode provides protection for an entire IP packet by treating it as an Authentication Header (AH), or Encapsulating Security Payload (ESP).

4. If you selected Tunnel Mode, for Enable Security End Point Address, select the address type. Options are **Disabled**, **IPv4 Address**, or **IPv6 Address**.
5. For IPsec Security, select **ESP**, **AH**, or **BOTH**.

   Note: If the IPsec Mode is set to Tunnel Mode, the BOTH option does not appear.

6. Type the Key Lifetime, and select **Seconds**, **Minutes**, or **Hours**.
7. For Perfect Forward Secrecy (PFS), select **None**, **Group 2**, or **Group 14**.
8. For Hash, select **SHA-1**, **SHA-256**, or **None**.
9. If you selected ESP or BOTH for the IPsec Security type, select one or more of the following Encryption types.

   Note: If the IPsec Security type is set to AH, the Encryption type options do not appear.

   - **AES**
   - **3DES**
   - **Null**
10. Click **Save**.

Editing or Deleting an Action

To edit or delete an action, select the action from the list, then click **Edit** or **Delete**.

Enabling IPsec

1. In the Embedded Web Server, click **Properties > Security**.
2. Click **IPsec**.
3. For Enablement, select **Enabled**.
4. To save the new settings, click **Apply**. To retain the previous settings, click **Undo**.

Disabling IPsec at the Control Panel

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **Security Settings > IPsec**.
3. Touch **Disable IPsec**.

   Note: IPsec can be enabled only in the Embedded Web Server.

Security Certificates

A digital certificate is a file that contains data used to verify the identity of the client or server in a network transaction. A certificate also contains a public key used to create and verify digital signatures. To prove identity to another device, a device presents a certificate trusted by the other device. The device can also present a certificate signed by a trusted third party and a digital signature proving that it owns the certificate.

A digital certificate includes the following data:

- Information about the owner of the certificate
- The certificate serial number and expiration date
- The name and digital signature of the certificate authority (CA) that issued the certificate
- A public key
- A purpose defining how the certificate and public key can be used

There are four types of certificates:

- A Device Certificate is a certificate for which the printer has a private key. The purpose specified in the certificate allows it to be used to prove identity.
- A CA Certificate is a certificate with authority to sign other certificates.
- A Trusted Certificate is a self-signed certificate from another device that you want to trust.
- A domain controller certificate is a self-signed certificate for a domain controller in your network. Domain controller certificates are used to verify the identity of a user when the user logs in to the printer using a Smart Card.

Installing Certificates

To ensure that the printer can communicate with other devices over a secure trusted connection, both devices must have specific certificates installed.

For protocols such as HTTPS, the printer is the server, and must prove its identity to the client Web browser. For protocols such as 802.1X, the printer is the client, and must prove its identity to the authentication server, typically a RADIUS server.

For features that use these protocols, perform the following tasks:

- Install a device certificate on the printer.

  Note: When the printer uses HTTPS, a Xerox® Device Certificate is created and installed on the printer automatically.

- Install a copy of the CA certificate that was used to sign the device certificate of the printer on the other device.

Protocols such as LDAP and IPsec require both devices to prove their identity to each other.

For features that use these protocols, perform the tasks listed under one of the following options:

To install certificates, option 1:

- Install a device certificate on the printer.
- Install a copy of the CA certificate that was used to sign the device certificate of the printer on the other device.
- Install a copy of the CA certificate that was used to sign the certificate of the other device on the printer.

To install certificates, option 2:

If the other device is using a self-signed certificate, install a copy of the trusted certificate of the other device on the printer.

Creating and Installing a Xerox® Device Certificate

If you do not have a server functioning as a certificate authority, install a Xerox® Device Certificate on the printer. When you create a Xerox® Device Certificate, the printer generates a certificate, signs it, and creates a public key used in SSL encryption. After you install a Xerox® Device Certificate on the printer, install the Device Root Certificate Authority in any device that communicates with the printer. Examples of other devices include client Web browsers for HTTPS or a RADIUS authentication server for 802.1X.

When the Device Root Certificate Authority is installed:

- Users can access the printer using the Embedded Web Server
- Certificate warning messages do not appear

Note: Creating a Xerox® Device Certificate is less secure than creating a certificate signed by a trusted certificate authority.

1. In the Embedded Web Server, click **Properties > Security**.
2. Click **Certificates**.
3. Click **Security Certificates**.
4. Click the Xerox Device Certificate tab.
5. Select **Create New Xerox Device Certificate**.
6. Complete the form with the requested information.
7. Click **Finish**.

Installing the Device Root Certificate Authority

If the device uses the Xerox® Device Certificate, and users attempt to access the device using the Embedded Web Server, an error message can appear in their Web browser. To ensure that error messages do not appear, in the Web browsers of all users, install the Device Root Certificate Authority.

Note: Each browser provides a method of temporarily overriding the untrusted certificate warning when connecting to a Xerox device Web page. This exception process may not work in some browsers when using the Remote Control Panel. The browser may appear unable to connect to the Remote Control Panel for the device. Some browsers can fail to connect to the device Remote Control Panel. To resolve this issue, install the device certificate.

Installing the Device Root Certificate Authority onto a Personal Computer

1. In the Embedded Web Server, click **Properties > Security**.
2. Click **Certificates**.
3. Click **Security Certificates**.
4. To save the file to your computer, click **Download the Device Root Certificate Authority**.
5. Install the file in your Web browser certificate store location. For details, refer to your Web browser help.

   Note:

   - Windows users: Install the certificate in each browser that is used to connect to a Xerox device.
   - Mac users: Install the certificate using the KeyChain™ application.
   - You can download the Device Root Certificate Authority from the HTTP page at **Properties > Connectivity > Protocols > HTTP**.

Installing the Device Root Certificate Authority onto Multiple Computers or Servers

Installing a Device Root Certificate Authority to Multiple Computers or Servers

To install a Device Root Certificate Authority to multiple computers using an application:

1. Contact your IT department about the method for updating multiple browsers or operating systems simultaneously.
2. Download the Device Root Certificate Authority from the Security Certificates page in the Embedded Web Server.
   a. In the Embedded Web Server, click **Properties > Security**.
   b. Click **Certificates**.
   c. Click **Security Certificates**.
   d. Click **Download the Device Root Certificate Authority**.
3. Send the certificate to your IT department for distribution.

Configuring a Chain Of Trust for an Organization

To configure a chain of trust for an organization:

1. Contact your IT department about the method for obtaining a Certificate Signing Request (CSR). A CSR is needed for each device that is signed by the root certificate for your organization.
2. Download a CSR from the Security Certificates page in the Embedded Web Server.
   a. In the Embedded Web Server, click **Properties > Security**.
   b. Click **Certificates**.
   c. Click **Security Certificates**.

d. Click **Create Certificate Signing Request (CSR)**.

e. On the Create Certificate Signing Request (CSR) page, type information and make selections, as needed.

f. Click **Finish**.

3. Process the CSR using the certificate signing server for your IT department.
4. Install the resulting signed device certificate onto each Xerox® device.

Creating a Certificate Signing Request

If you do not install a Xerox Device Certificate, you can install a CA-signed device certificate. Create a Certificate Signing Request (CSR), and send it to a CA or a local server functioning as a CA to sign the CSR. An example of a server functioning as a certificate authority is Windows Server 2008 running Certificate Services. When the CA returns the signed certificate, install it on the printer.

Creating a Certificate Signing Request

1. In the Embedded Web Server, click **Properties > Security**.
2. Click **Certificates**.
3. Click **Security Certificates**.
4. Click the **CA-Signed Device Certificate(s)** tab.
5. Select **Create Certificate Signing Request (CSR)**.
6. Complete the form with your 2-Letter Country Code, State/Province Name, Locality Name, Organization Name, Organization Unit, and Email Address.
7. Select **Subject Alternative Name** if applicable, then type the MS Universal Principal Name.

   Note: The Subject Alternative Name is only required when using 802.1X EAP -TLS for Windows clients or servers.

8. Click **Finish**.

Uploading a CA-Signed Device Certificate

1. In the Embedded Web Server, click **Properties > Security**.
2. Click **Certificates**.
3. Click **Security Certificates**.
4. Click the **CA-Signed Device Certificate(s)** tab.
5. Select **Install Certificate**.
6. Click **Browse** or **Choose File**, then navigate to the signed certificate in **.pem** or **PKCS#12** format.
7. Click **Open** or **Choose**.
8. Click **Next**.
9. If the certificate is password protected, type the password, then retype it to verify.
10. To help identify the certificate in the future, type a **Friendly Name**.

11. Click **Next**.

    Note:

    - The signed certificate can match a pending CSR created by the device.
    - The signed certificate can be a PKCS#12 certificate generated by a Certificate Authority.

Installing Root Certificates

You can install the certificates for the root certificate authority and any intermediate certificate authorities for your company. You can install the self-signed certificates from any other devices on your network.

Supported certificate encodings and typical file extensions include:

- Distinguished Encoding Rules (.cer, .crt, .der)
- Privacy Enhanced Mode/Base64 (.pem)
- PKCS#7 (.p7b)
- PKCS#12 (.pfx, .p12)

Note: To import a CA-Signed Device Certificate, use the PKCS#12 format.

To install a root certificate:

1. In the Embedded Web Server, click **Properties > Security**.
2. Click **Certificates**.
3. Click **Security Certificates**.
4. Click the **Root/Intermediate Trusted Certificate(s)** tab.
5. Click **Install Certificate**.
6. Click **Browse** or **Choose File**, then navigate to a signed certificate file.
7. Click **Open** or **Choose**.
8. Click **Next**.
9. To help identify the certificate in the future, type a **Friendly Name**.
10. Click **Next**.

The digital certificate appears in the list of Installed certificates.

Installing Domain Controller Certificates

You can install the self-signed certificates from any domain controllers on your network.

Supported certificate encodings and typical file extensions include:

- Distinguished Encoding Rules (.cer, .crt, .der)
- Privacy Enhanced Mode/Base64 (.pem)
- PKCS#7 (.p7b)

- PKCS#12 (.pfx, .p12)

Note: To import a CA-Signed Device Certificate, use the PKCS#12 format.

To install a domain controller certificate:

1. In the Embedded Web Server, click **Properties > Security**.
2. Click **Certificates**.
3. Click **Security Certificates**.
4. Click the **Domain Controller Certificate(s)** tab.
5. Click **Install Certificate**.
6. Click **Browse** or **Choose File**, then navigate to a signed certificate file.
7. Click **Open** or **Choose**.
8. Click **Next**.
9. To help identify the certificate in the future, type a **Friendly Name**.
10. Click **Next**.

The digital certificate appears in the list of Installed certificates.

Viewing, Saving, or Deleting a Certificate

1. On the Security Certificates page, click a certificate type tab.
2. To view or save a certificate, for Action, click **View/Export**.
   Certificate details appear on the View/Save Certificate page.
   1. To save the certificate file to your computer, click **Export (Base-64 encoded-PEM)**.
   2. To return to the Security Certificates page, click **Close**.
3. To delete a certificate, next to the certificate name, select the check box, then click **Delete Selected**.

   Note: You cannot delete the Default Xerox® Device Certificate.
4. To delete all certificates except for the Default Xerox® Device Certificate, click **Reset to Machine/ Device Factory Defaults**.

Specifying the Minimum Certificate Key Length

You can specify the minimum encryption key length required for certificates. If a user attempts to upload a certificate that contains a key that does not meet this requirement, a message appears. The message alerts the user that the certificate they are attempting to upload does not meet the key length requirement.

1. In the Embedded Web Server, click **Properties > Security**.
2. Click **Certificates > Certificate Key Length**.
3. For Minimum Encryption Key Length, select **1024-bit minimum**, **2048-bit minimum**, or **No Minimum**.

4. Click **Apply**.

802.1X

802.1X is an Institute for Electrical and Electronics Engineers (IEEE) standard that defines a method for port-based network access control or authentication. In an 802.1X secured network, the printer must be authenticated by a central authority, typically a RADIUS server, before it can access the physical network.

You can enable and configure the device for an 802.1X secured network. You can configure the device from the control panel or the Embedded Web Server.

Before you begin:

- Ensure that your 802.1X authentication server and authentication switch are available on the network.
- Determine the supported authentication method.
- Create a user name and password on your authentication server.

Enabling and Configuring 802.1X in the Embedded Web Server

1. In the Embedded Web Server, click **Properties > Connectivity > Setup**.
2. For Network, for Wired Connection, click **Edit**.
3. To configure 802.1X settings, for 802.1X, click **Edit**.
4. For Protocol, select **Enable 802.1X**.
5. For Authentication Method, select the method used on your network.

   Note: When the device is in FIPS 140 mode, EAP-TLS authentication is required.

6. For Server Validation - Validate server using, select the root certificate that you want to use to validate the authentication server. If you do not want to validate a certificate, select **No Validation**.

   Note:

   - You can require the device to validate certificates used to encrypt 802.1X only if you selected PEAPv0/EAP-MS-CHAPv2 or EAP-TLS as the authentication method.
   - TLS authentication and server verification both require X.509 certificates. To use these features, install the necessary certificates on the Security Certificates page before configuring 802.1X.
   - The Default Xerox® Device Certificate cannot be used with EAP-TLS in Windows environments. It can be used in FreeRADIUS server environments.

7. To view or save a certificate, select the certificate from the menu, then click **View/Save**. Certificate details appear on the View/Save Device Certificate page.
   a. To save the certificate file to your computer, click **Export (Base-64 encoded - PEM)**.
   b. To return to the previous page, click **Close**.

8. If you selected EAP-TLS as the authentication method, you can allow the device to encrypt 802.1X communication. For Device Certificate (TLS) - Authentication Certificate, select the certificate that you want to use.
9. To view or save a certificate, select the certificate from the menu, then click **View/Save**. Certificate details appear on the View/Save Device Certificate page.
   a. To save the certificate file to your computer, click **Export (Base-64 encoded - PEM)**.
   b. To return to the previous page, click **Close**.
10. For User Name, type the user name for the authentication switch and server.
11. For Password, type and confirm a password.
12. To save the new password, click **Select to save new password**.

    Note: A password is not required for EAP-TLS authentication.

13. Click **Save**.

Enabling and Configuring 802.1X at the Control Panel

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **Network Settings > Advanced Settings**.
3. Touch **802.1X**.
4. Touch **Enabled**.
5. To select the authentication method used on your network, touch the menu.

    Note:

    - When the device is in FIPS 140 mode, EAP-TLS authentication is required.
    - To configure 802.1X settings for EAP-TLS, use the Embedded Web Server.

6. Touch **Username**.
7. To type the user name and server that your authentication switch requires, use the touch screen keypad. Touch **OK**.
8. Touch **Password**, then to type the password, use the touch screen keypad. Touch **OK**.
9. Touch **Finish**.

System Timeout

You can specify how long the printer waits to log out an inactive user.

Setting System Timeout Values

1. In the Embedded Web Server, click **Properties > Security**.
2. Click **Timeout and Resume > System Timeout**.
3. For Touch User Interface System Timeout, type the time that the device waits before it logs a user out of the touch screen.
4. To configure the device to display a warning message before it logs a user out of the touch screen, select **Enable Warning Screen**.
5. To select the Web User Interface System Timeout settings, for Days, Hours, and Minutes, type a value or use the arrows to select a value.
6. Click **Apply**.

Setting the System Timeout Values at the Control Panel

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **Device Settings > Timers > System Timeout**.
3. To specify the time the printer waits to log out an inactive user at the control panel, for Minutes and Seconds, touch the arrows, then select values.
4. To instruct the printer to display a warning message before it logs a user out of the touch screen, for Warning Screen, touch **Enabled**.
5. Touch **OK**.

Overwriting Image Data

Image data is any in-process or temporary user data on the hard drive, such as current jobs, queued jobs, temporary files, saved jobs, and saved folders. To ensure that image data on the printer hard drive cannot be accessed, you can delete and overwrite image data.

Standard Image Overwrite deletes all image data from the printer memory and hard drive, except:

- Jobs and folders stored in the Reprint Saved Jobs feature
- Jobs stored in the Scan to Mailbox feature
- Fax Dial Directories
- Fax Mailbox contents

Note: Standard image overwrite takes approximately 20 minutes to complete.

Full Image Overwrite deletes all image data from the printer memory and hard drive, including:

- Jobs and folders stored in the Reprint Saved Jobs feature
- Jobs stored in the Scan to Mailbox feature
- Fax Dial Directories
- Fax Mailbox contents

Note: Full image overwrite takes approximately 60 minutes to complete.

Immediate Job Overwrite prompts the printer to overwrite each job immediately after it finishes processing.

Manually Deleting Image Data

1. In the Embedded Web Server, click **Properties > Security**.
2. Click **Image Overwrite Security**.
3. Click the **Disk Overwrite** tab.
4. To enable Image Overwrite, click the **Scheduled** tab, then select **Enabled**.
5. To print a report after the device overwrites data, for Confirmation Report, select **On**. To print a report only if an error occurs, select **Errors only**.
6. To start a disk overwrite:
   a. Click the **Overwrite Now** tab.
   b. Click **Advanced Settings**.
   c. For Overwrite Mode, select an option:
      - To overwrite all user image data or job data, except saved or stored jobs and folders, fax dial directories, and fax mailbox contents, select **Standard**. Standard Image Overwrite takes approximately 20 minutes to complete.
      - To overwrite all user image data or job data, fax dial directories, or fax mailbox contents, select **Full**. Full Image Overwrite takes approximately 60 minutes to complete.
   d. Click **Start Disk Overwrite Now**.

e. At the warning message, click **OK**.

Manually Deleting Image Data at the Control Panel

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **Security Settings > Image Overwrite Security**.
3. Touch **Disk Overwrite Now**.
4. To change the overwrite mode, touch **Overwrite Mode**, then touch an option.
5. To set the printer to print a confirmation report after it overwrites data, touch **Confirmation Report**, then select an option.
6. Touch **Overwrite Now**.

   Note: If the number of files to delete is large, the printer can be offline for up to 60 minutes during the deletion process.

7. To acknowledge the message and start the process, touch **Overwrite Now**.

Scheduling Routine Deletion of Image Data

1. In the Embedded Web Server, click **Properties > Security**.
2. Click **Image Overwrite Security**.
3. Click the **Disk Overwrite** tab.
4. Click the **Scheduled** tab.
5. On the Scheduled tab, select **Enabled**.
6. For Frequency, select how often the device overwrites data.
7. To set the time when the device overwrites data, for Time, type the hour and minutes.
8. If you selected Weekly for Frequency, for Day of the Week, select the day when the device overwrites data. If you selected Monthly for Frequency, for Day of the Month, select the date when the device overwrites data.
9. For Confirmation Report for Schedule Overwrites, select an option:
   - **On**: This option directs the device to print a report after the device overwrites data.
   - **Errors Only**: This option directs the device to print a report only if an error occurs.
   - **Off**: This option disables confirmation report printing.
10. For Overwrite Mode, select an option:
    - **Standard**: This option deletes all image data from the device memory and hard drive, except:
      - Jobs and folders stored in the Reprint Saved Jobs feature
      - Jobs stored in the Scan to Mailbox feature
      - Fax Dial Directories
      - Fax Mailbox contents
    - **Full**: This option deletes all image data from the device memory and hard drive.
11. Click **Apply**.

Scheduling Routine Deletion of Image Data at the Control Panel

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **Security Settings > Image Overwrite Security**.
3. Touch **Disk Overwrite**.
4. To specify how often the printer overwrites data, touch **Never**, **Daily**, **Weekly**, or **Monthly**.
5. If you selected Daily, to select the time, touch the arrows. If you selected Weekly or Monthly, touch **Day of Month**, **Day of Week**, or **Overwrite Time**, then touch the arrows.
6. To change the overwrite mode, touch **Overwrite Mode**, then touch an option.
7. To set the printer to print a confirmation report after it overwrites data, touch **Confirmation Report**, then select an option.
8. Touch **OK**.

Immediate Job Overwrite

Immediate Job Overwrite prompts the device to overwrite each job immediately after it finishes processing. Immediate Job Overwrite removes any remnants of all print, copy, scan, and fax jobs from the image disk.

Note: Immediate Job Overwrite is the preferred setting for high security environments and is enabled by default.

Enabling Immediate Image Overwrite

1. In the Embedded Web Server, click **Properties > Security**.
2. Click **Image Overwrite Security**.
3. Click the **Immediate Job Overwrite** tab.
4. On the Immediate Job Overwrite tab, for Enablement, select **Enabled**.
5. Click **Apply**.

Enabling Immediate Image Overwrite at the Control Panel

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **Security Settings > Image Overwrite Security**.
3. Touch **Job Overwrite**.
4. Touch **Enable**.
5. Touch **OK**.

PostScript Passwords

The PostScript language includes commands that allow PostScript print jobs to change the printer configuration. By default, PostScript jobs can use these commands, and a password is not required. To ensure that unauthorized changes are not made, you can require PostScript jobs to include a password.

You can enable the following passwords:

- **Run Start Job**: This password controls the execution of the Sys/Start file.
- **Device Parameters Password**: This password controls the execution of PostScript programs that modify PostScript device parameters.
- **Start Job Password**: This password is used with the Startjob and Exitserver operators to restrict PostScript jobs from running unencapsulated. This prevents unencapsulated jobs from changing default device settings.

For details, refer to the Help in the Embedded Web Server.

Enabling or Creating PostScript Passwords

1. In the Embedded Web Server, click **Properties > Security**.
2. Click **PostScript Passwords**.
3. To enable the Run Start Job password, for Startup Mode, select **Enabled**.
4. For Device Parameters Password, type a password, then retype the password to verify.
5. For Start Job Password, type a password, then retype the password to verify.
6. Click **Save**.

Hiding User Names on the Control Panel

You can hide the user name for the logged-in user to prevent it from displaying on the device control panel touch screen.

1. In the Embedded Web Server, click **Properties > Security > Hide User Name**.
2. To hide the user name, for Hide User Name/Friendly Name within the Device's Touch Interface, click **Yes (Hide)**.
3. Click **Save**.

Verifying the Software

You can test the printer software to confirm that it is operating correctly. The test checks software files to confirm that they are not corrupt. If the printer software appears to be functioning improperly, a Xerox representative can ask you to perform this test.

1. In the Embedded Web Server, click **Properties > Security**.
2. Click **Software Verification Test**.
3. To begin the test, click **Start Test**.
4. To interrupt and cancel the test, click **Cancel**.

Note:

- You can continue to use the device while the test is running.
- If the test fails, the software files are corrupt. Xerox recommends that you reinstall the software. For help, contact a Xerox representative.

Restricting Print File Software Updates

You can restrict users from installing optional software features by sending a print file. This option restricts users from updating the software.

1. In the Embedded Web Server, click **Properties > General Setup**.
2. Click **Feature Installation**.
3. To restrict users from installing features using the .csv file print method, for Allow Print File Updates, select **Disable**.
4. Click **Apply**.

Specifying Email and Internet Fax Recipient Restrictions

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **Security Settings > Valid Recipients**.
3. To allow users to send an email or Internet fax to addresses in the address book only, touch **Limit to Address Book Entries**.
4. Touch **OK**.

System Administrator Password

The administrator password is required when you want to access locked settings in the Embedded Web Server, or at the printer control panel. Most printer models have a default configuration that restricts access to some settings. Access is restricted for settings on the Properties tab in the Embedded Web Server, and settings on the Device menu at the control panel.

After you configure the printer, it is recommended that you change the default administrator password. For details, refer to Changing the System Administrator Password.

Note: If you do not change the default administrator password, each time you log in as administrator to the Embedded Web Server, the device prompts you to change the password. You can disable this reminder prompt.

To set the policy to follow if you forget the administrator password, refer to Enabling the Administrator Password Reset and Disabling the Administrator Password Reset.

Note: To avoid forgetting a single administrator password, it is recommended to create a number of local accounts with administrator rights.

Enabling the Administrator Password Reset

To enable the password reset feature:

1. In the Embedded Web Server, click **Properties > Security**.
2. Click **Password Policies**, then click **Admin Password**.
3. Click the **Reset Policy** tab.
4. For Password Reset Policy, click **Enable Password Reset**.
5. Click **Apply**.

   Note: If you enable the password reset feature, and forget the administrator password, for instructions, contact Xerox Support. For security, you can only reset the password at the device control panel.

Disabling the Administrator Password Reset

To disable the password reset feature:

1. In the Embedded Web Server, click **Properties > Security**.
2. Click **Password Policies**, then click **Admin Password**.
3. Click the **Reset Policy** tab.
4. For Password Reset Policy, click **Disable Password Reset**.
5. Click **Apply**.

   Caution: If you disable the password reset feature, and forget the administrator password, contact a Xerox representative, then schedule a site visit. There is a fee for a Xerox representative site visit to reset the administrator password.

5

Printing

This chapter contains:

Paper Management

Setting Default Paper Type and Color

You can specify the default settings for paper type and color.

Note: When the paper type and color are not specified for the print job, the system applies default settings.

1. In the Embedded Web Server, click **Properties > General Setup > Paper Management**.
2. If necessary, click the **Default Paper Type and Color** tab.
3. For Paper Type, set the default paper type.
4. For Paper Color, set the default paper color.
5. Click **Save**.

Enabling Required Paper Policies

You can configure policies for the paper tray confirmation prompt, nearest paper type match, and paper-size replacement features.

1. In the Embedded Web Server, click **Properties > General Setup > Paper Management**.
2. Click the **Required Paper Policies** tab.
3. To configure the prompt at the control panel when new same-size paper is loaded in a tray, for Automatic Tray Confirmation Prompt, select the paper tray options.
   a. For Bypass Tray, select an option:
      - **Always Show**: This option displays the paper confirmation prompt at the control panel. The prompt remains on the control panel until a user selects **OK**.
      - **Delayed Confirmation**: This option displays the paper confirmation prompt at the control panel for a specified time. For the Confirm and close prompt after setting, select a time period.

      Note: While the prompt appears at the control panel, you can confirm any change to paper type, color, and size. At the end of the specified time, the prompt disappears.

   b. For Other Adjustable Trays, select an option:
      - **Always Show**.
      - **Delayed Confirmation**.
      - **Auto Confirmation**: This option confirms the paper type, color, and size without showing a prompt at the control panel.

      Note: Xerox does not recommend using the Auto Confirmation option unless you always load the tray with paper of the exact same type, color, and size.

4. To replace the requested paper size with the closest replacement paper size, for Nearest Match, select **Enabled**.

   Note: To obtain the best fit of the image on the paper, this option can cause slight scaling of the image.

5. To replace the Legal paper size with one of two replacement paper sizes, for Replace 8.5 x 14", select **Enabled**.

   Note: If the first replacement paper size is not available, the printer uses the second replacement paper size.

6. To set the default Legal paper size for when the scanner cannot detect the paper length, for Default Legal Size, select a paper size.
7. To set an alert for when the required paper is not available, for Jobs Held for Required Paper, select an option.
8. Click **Apply**.

Setting Paper Size Preference

Use Paper Size Preference to control how paper-size measurements appear on the control panel. For the unit of measure, select Inches or Metric. This setting affects custom-size measurement units.

1. In the Embedded Web Server, click **Properties > General Setup > Paper Management**.
2. Click the **Paper Size Preference** tab.
3. For Inches or Metric, select an option:
   - To set the paper size preference to inches, select **Inches**.
   - To set the paper size preference to millimeters, select **Metric**.
4. Click **Apply**.

Setting Paper Size Preferences at the Control Panel

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **Device Settings > Paper Management > Paper Size Preference**.
3. Select an option.
   - **Inches**: This option sets the paper-size preference to inches.
   - **Metric**: This option sets the paper-size preference to millimeters.
4. Touch **OK**.

Selecting Paper Tray Settings

For each paper tray, you can view or configure the mode, priority, and auto-select settings.

1. Access the Embedded Web Server.
2. Access the Paper Management page using one of the following methods:
   - Click **Properties > General Setup > Paper Management**.
   - Click **Home**, then for Trays, click **Settings**.
3. Click the **Tray Content & Settings** tab.

4. To edit a specific paper tray, click **Edit** on that row.
5. For Edit Tray, select an option:
   - **Fully Adjustable**: This option prompts you to confirm the type of paper loaded in the tray.
   - **Dedicated**: This option sets the paper tray as the only paper source for print jobs matching a specific paper size, type and color. This option assumes that the paper you loaded in the tray is the type specified for Paper Types.
   - If you selected Dedicated, to edit the paper size, type, and color for this tray, click the pencil icon.
   - Select the desired options.
   - Click **Save**.
6. For Priority, set the priority for the selected tray.

   For example, the printer uses paper from the Priority 1 tray first. If that tray is empty, the printer then prints using paper from the Priority 2 tray.
7. To have the print driver select the tray, for Auto Selection, select **Enabled**.
8. Click **Save**.

Selecting Tray 1 or Tray 2 Settings

Your device model supports either Tray 1 configuration or Tray 2 configuration, but not both. The Tray 1 Usage setting or the Tray 2 Usage setting notifies the device about the paper tray configuration.

Selecting Tray 1 Settings for Device Models that Support Tray 1 Configuration

To select Tray 1 settings for device models that support Tray 1 configuration:

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **Device Settings > Paper Management > Tray 1 Usage**.
3. Select an option.
   - **Standard Tray Only**: This option indicates that only a Standard paper tray is installed.
   - **Envelope Tray Only**: This option indicates that only the optional Envelope tray is installed.
   - **Both Standard and Envelope Tray**: This option indicates that either of these trays is installed. If you want to change between the Standard and Envelope trays, select this option.

   > **Note:** If you select Both Standard and Envelope Tray, select the check box on the media configuration screen to indicate that the Envelope Tray is installed.
4. Touch **OK**.

Selecting Tray 2 Settings for Device Models that Support Tray 2 Configuration

To select Tray 2 settings for device models that support Tray 2 configuration:

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **Device Settings > Paper Management > Tray 2 Usage**.

3. Select an option.
   - **Standard Tray Only**: This option indicates that only a Standard paper tray is installed.
   - **Envelope Tray Only**: This option indicates that only the optional Envelope tray is installed.
4. Touch **OK**.

Configuring Custom Media Types

The Custom Media Types tab allows you to apply custom names to available media types. You can add, edit, delete, import, or export custom media types. You can also determine what media types are available in the system.

Adding a Custom Media Type

To add a custom media type:

1. In the Embedded Web Server, click **Properties > General Setup > Paper Management**.
2. Click the **Custom Media Types** tab.
3. Click **Add**.
4. In the fields, type descriptive information as needed.
5. To position the paper type in the list, for Position, type a number. To position paper types higher in the list, assign them lower numbers.
6. To hide the paper type from users, for Visibility in the System, select **Hidden**.
7. For Paper Type Profile, select an option.
8. Click **Save**.

Editing a Custom Media Type

To edit a custom media type:

1. For the media type you want to edit, click **Edit**.
2. In the fields, type descriptive information as needed.
3. To position the paper type in the list, for Position, type a number. To position paper types higher in the list, assign them lower numbers.
4. To hide the paper type from users, for Visibility in the System, select **Hidden**.
5. For Paper Type Profile, select an option.
6. Click **Save**.

Arranging the Order of Custom Media Types in the List

To arrange the order of custom media types in the list:

1. Select a custom media type from the list.
2. To move the media type up or down in the list, click the arrows.
3. Click **Apply**.

Note:

- To show all custom media types, for More Actions, select **Show All**.
- To hide all custom media types, for More Actions, select **Hide All**.
- To delete all custom media types and return to factory-default settings, for More Actions, select **Delete All / Return to Factory Defaults**.

Importing a Custom Media Type

To import a custom media type:

1. For More Actions, select **Import**.
2. Click **Browse** or **Choose File**, select the file, then click **Open** or **Choose**.
3. For Encoding, select an option.
4. To import the file, click **Import**.
5. Click **Close**.

Exporting Custom Media Type Settings

To export custom media type settings:

1. For More Actions, select **Export**.
2. For Encoding, select an option.
3. For Delimiter, select an option.
4. To export the file, select **Export**.
5. Click **Close**.

To display custom media names at the top of the media list, select **Always Display Custom Types First**.

Saving and Reprinting Jobs

The Reprint Saved Jobs feature allows you to save your print job on the device so that you can print it at any time.

Enabling the Reprint Saved Jobs Feature

1. In the Embedded Web Server, click **Properties > Apps > Print From**.
2. Click **Reprint Saved Jobs > Enablement**.
3. For Enablement, select **Enabled**.
4. To save the new settings, click **Apply**. To retain the previous settings, click **Undo**.

Creating and Managing Saved Jobs Folders

By default, if Reprint Saved Jobs is enabled, jobs are saved in the Default Public Folder. You can create folders to organize saved jobs.

Managing certain folder types requires that you log in as the creator of the folder or that you have administrator-level permissions. You can delete, rename, or change the permissions for a folder. If you want to limit access to the saved jobs, assign a password to a folder.

Creating a Folder

1. In the Embedded Web Server, click **Jobs > Saved Jobs**.
2. For Folder Operations, click **Create New Folder**.
3. Type a name in the field provided.
4. For Folder Permissions, select the folder type.
5. Click **Apply**.

Managing a Folder

1. Click **Manage Folders**.
2. For the folder, click the pencil icon.
3. If allowed, you can rename the folder and change folder permissions.
4. Click **Apply**.

Deleting a Folder

1. Click **Manage Folders**.

   The list of existing folders appears.
2. Select the folder you want to delete.

   The Delete Folder button activates.

3. Click **Delete Folder**.

   A warning message appears informing you that the delete is permanent.

4. Click **OK** to delete or **Cancel** to exit.

Saving and Printing Jobs

Saving a Job from Your Computer

1. With your file open, click the **File** menu in the application, then click **Print**.
2. From the application Print window, select your printer from the Printer Name menu.
3. Click **Properties** to access the print settings for the job.
4. On the Printing Options tab, click the **Job Type** menu, then select **Saved Job**.
5. Type a Job Name for the job or, to use the document file name being submitted, select **Use Document Name**.
6. From the Save To menu, select the destination folder. Select **Default Public Folder** or type a name for a new folder.
7. To save the job to the printer and print it immediately, click **Save and Print**.
8. To save your job as a secure job, select **Private**, type and retype a 4–10 digit passcode, then click **OK**.

Backing Up Saved Jobs

1. In the Embedded Web Server, click **Properties > Apps > Print From**.
2. Click **Reprint Saved Jobs > Backup Jobs**.
3. For Protocol, select **FTP**.
4. Select the address type for the FTP server to use for backup jobs. Options are **IPv4 Address**, **IPv6 Address**, or **Host Name**.
5. For IP Address: Port, type the appropriately formatted address in the IP Address and Port field. The default port number is 21.
6. For Document Path, type the path to the file repository.
7. For File Name, type the name for the backup file. This name is appended to the end of the document path.
8. For Login Name, type the login name for the FTP server.
9. Type a password, then retype the password.
10. To save the password, select the **Select to save new password** check box.
11. Select an option:
    - To begin the backup, click **Start**.
    - To retain the previous settings, click **Undo**.

Restoring Saved Jobs from an FTP Repository

Caution: When you restore backed-up jobs, existing stored jobs are overwritten, and the Default Public Folder is emptied.

1. In the Embedded Web Server, click **Properties > Apps > Print From**.
2. Click **Reprint Saved Jobs > Restore Jobs**.
3. For Protocol, select **FTP**.
4. Select the address type for the FTP server where the saved jobs are stored. Options are **IPv4 Address**, **IPv6 Address**, or **Host Name**.
5. For IP Address: Port, type the appropriately formatted address in the IP Address and Port field. The default port number is 21.
6. For Document Path, type the path to the file repository.
7. For File Name, type the name for the backup file that you want to restore. This name is appended to the end of the document path.
8. For Login Name, type the login name for the FTP server.
9. Type a password, and then retype the password.
10. To save the password, select the **Select to save new password** check box.
11. Select an option:
    - To begin restoring saved Jobs, click **Start**.
    - To retain the previous settings, click **Undo**.

Printing Jobs from the Embedded Web Server

You can print **.pdf**, **.ps**, **.pcl**, and **.xps** files from the Embedded Web Server.

1. In the Embedded Web Server, click **Print**.

   The Job Submission page appears.

2. Click the File Name field, then type the file name. To select the file from a local network or remote location, click **Browse** or **Choose File**.
3. For Printing, select options for the job as needed.
4. To print the document, click **Submit Job**.

Note: To ensure that the job was sent to the queue, wait for the job submission confirmation message to appear before you close this page.

Configuring General Print Settings

1. In the Embedded Web Server, click **Properties > Apps**.
2. Click **Printing > General**.
3. To print a Configuration Report when the printer is powered on, for Configuration Report, select **Print at Power on**.
4. To restrict printing of the Configuration Report and Information Pages to the system administrator, for Configuration / Information Pages Report, select **Restrict to System Administrator**.
5. To erase all print jobs from the print queue at power-on, select **Delete All print jobs at Power On**.
6. For Held Job Policy, select options as needed.
   - To require active jobs to print in the order received after a held job, for Allow Print Around on Held Jobs, select **No**.
   - To enable the user to print active jobs before a held job prints, for Allow Print Around on Held Jobs, select **Yes**.
   - To allow a job to print to an alternate paper source, for Allow Print on Alternate Paper When Job is Held for Resources, select **Yes**.
7. To set the amount of time that the device holds print jobs before it deletes them, for Delete Held Jobs After, specify the number of days, hours, and minutes.
8. For Banner Sheet, select options as needed.
   - To print a banner page with each print job, for Print Banner Sheets, select **Yes**. To disable this option, select **No**.
   - To allow the print driver to override the setting for banner pages, for Allow the Print Driver to Override, select **Yes**.
   - To select the text that appears on the banner pages, for Banner Sheet Identification, select an option.
9. To print an error sheet when a print job fails, for Print Error Sheets, select **Enable**.
10. For Defaults and Policies, for each setting, select options as needed.
11. Click **Save**.

Printing an Error Sheet

1. In the Embedded Web Server, click **Properties > Apps**.
2. Click **Printing > General**.
3. To print an error sheet when a print job fails, for Output Error Sheet, for Print Error Sheets, select **Enable**.
4. Click **Save**.

Managing Banner Page Printing Options

You can set the device to print a banner page with each print job. The banner page contains information identifying the user and job name. You can set this option in the print driver, in the Embedded Web Server, or at the control panel.

Note: Enable banner page printing in the print driver, at the control panel, or in the Embedded Web Server. Otherwise, a banner page does not print.

Enabling Banner Page Printing in the Embedded Web Server

1. In the Embedded Web Server, click **Properties > Apps**.
2. Click **Printing > General**.
3. In the Banner Sheet area, for Print Banner Sheets, select options as needed.
   - To print a banner page with each print job, for Print Banner Sheets, select **Yes**. To disable this option, select **No**.
   - To allow the print driver to override the setting for banner pages, for Allow the Print Driver to Override, select **Yes**.
   - To select the text that appears on the banner pages, for Banner Sheet Identification, select an option.
4. To save the new settings, click **Save**. To retain the previous settings, click **Undo**.

Enabling Banner Page Printing at the Control Panel

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **App Settings**.
3. Touch **Job Sheets > Banner Pages**.
4. For Print Banner Pages, touch **Yes**.
5. To allow users to turn banner page printing on or off in the print driver, for Allow the Print Driver to Override, touch **Yes**.
6. For Banner Page Identification, select the information that prints on the banner page.
7. Touch **OK**.

Enabling Banner Page Printing in the Print Driver

1. With your file open in the application, click the **File** menu, then click **Print**.
2. From the application Print window, select your printer from the Printer Name menu.
3. To access the print settings for the job, click **Properties**.
4. Click the **Advanced** tab.

5. To select disable Job ID or to select a print option for Job ID, expand Advanced Settings. Open the Job ID menu, then select an option:
   - **Disable Job ID**
   - **Print ID on a Banner Page**
   - **Print ID in Margins – First Page Only**
   - **Print ID in Margins – All Pages**
6. Click **OK**.

   Note: If banner page printing is disabled in the Embedded Web Server or at the control panel, setting the print driver to print banner pages is ignored.

Configuring Secure Print Settings

You can configure Secure Print settings to specify how the printer behaves when a user sends a Secure Print job to the printer.

Configuring Secure Print Device Policies

1. To access the Secure Print page, click **Properties > Apps > Printing > Secure Print**, or click **Security > Secure Print**.
2. Click the **Device Policies** tab.
3. To show or conceal the characters in job names, for Conceal Job names, select an option.

   Note:

   - When a Secure Print job is sent to the printer, by default, the job name appears in the list of jobs on the control panel touch screen.
   - When the characters are concealed, they appear as asterisks in the job name to hide the title of the document that is being printed.
4. To display hidden job names for reporting or accounting, select options as needed:
   - **Show Concealed Job Names in Network Accounting Reports**: This option shows the concealed job names in network accounting reports.
   - **Show Concealed Job Names in Audit Log**: This option shows the concealed job names in the audit log.
5. For Release Policies for Secure Print Jobs Requiring Passcode When the User is Already Logged-In, select an option:
   - **Release Jobs Without Prompting for Passcode**: This option allows users who are logged in to release a Secure Print job without typing a passcode.
   - **Prompt for Passcode Before Releasing Jobs**: This option requires users who are logged in to type a passcode to release the job.
6. Click **Save**.

Configuring Secure Print Driver Defaults

1. On the Secure Print page, click the **Defaults** tab.
2. To set the minimum passcode length, for Secure Print Passcode Length, type a number from 4–10.
3. To set the default login method, for Print Driver, select an option:
   - **Passcode**: This option requires you to log in using the 4–10 digit passcode that you submitted with the print job.
   - **User ID**: This option requires you to log in using your assigned device user ID.
4. Click **Save**.

Hold All Jobs

You can enable and configure the Hold All Jobs feature to require users to release print jobs manually at the control panel.

Configuring the Hold all Jobs Feature

1. In the Embedded Web Server, click **Properties > Apps**.
2. Click **Printing > Hold All Jobs**.
3. For Enablement, select an option.
   - **Hold all Jobs in a Private Queue**: The printer holds sent jobs in a locked folder. Users are required to log in at the control panel to view, print, and delete jobs.
   - **Hold all Jobs in a Public Queue**: The printer holds sent jobs in an unlocked folder. Users are not required to log in at the control panel unless accessing a Secure Print job.
4. For Unidentified Job Policies, select an option.

   Note:

   - Unidentified jobs are jobs that are not associated with a user name. Unidentified jobs originate from a computer that does not require a user to log in. Examples include jobs sent from a DOS or UNIX window environment using LPR, Port 9100, or from the Jobs tab in the Embedded Web Server.
   - Changing the setting for Unidentified Jobs Policy deletes existing unidentified jobs that are waiting for authentication.

   - **Hold Jobs; All Users can Manage Jobs**: This option allows all users to view, print, and delete unidentified jobs. Users are required to enter a passcode to release Secure Print jobs.
   - **Hold Jobs; Only Administrators can Manage Jobs**: This option allows only system administrators to view, print, and delete unidentified jobs. System administrators are required to enter a passcode to release Secure Print jobs.
   - **Delete Jobs Immediately**: This option deletes all unidentified jobs. Deleted jobs appear in a list at the control panel in the Completed Jobs queue.
   - **Print Jobs Immediately**: This option immediately prints all unidentified jobs except for unidentified Secure Print jobs. Users are required to enter a passcode to release Secure Print jobs.
5. For Release Job Policy After Log On, select an option.
6. Click **Save**.

UNIX, Linux, and AS/400 Printing

To provide printer spooling and network print server functionality, UNIX-based printing uses LPD/LPR port 515 or lp to port 9100. Xerox printers can communicate using either protocol.

Xerox® Printer Manager

Xerox® Printer Manager is an application that allows you to manage and print to multiple printers in UNIX and Linux environments.

Xerox® Printer Manager allows you to:

- Configure and check the status of network connected printers.
- Set up a printer on your network as well as monitor the operation of the printer once installed.
- Perform maintenance checks and view supplies status at any time.
- Provide a common look and feel across the many different suppliers of UNIX and Linux operating systems.

Installing Xerox® Printer Manager

Before you begin:

Ensure that you have root or superuser privileges to install Xerox® Printer Manager.

1. Download the appropriate package for your operating system. To locate drivers for your printer, go to www.support.xerox.com. The available files are:
   - Xeroxv5Pkg-AIXpowerpc-x.xx.xxx.xxxx.rpm for the IBM PowerPC family.
   - Xeroxv5Pkg-HPUXia64-x.xx.xxx.xxxx.depot.gz to support HP Itanium workstations.
   - Xeroxv5Pkg-Linuxi686-x.xx.xxx.xxxx.rpm to support RPM-based 32-bit Linux environments.
   - Xeroxv5Pkg-Linuxi686-x.xx.xxx.xxxx.deb to support Debian-based 32-bit Linux environments.
   - Xeroxv5Pkg-Linuxx86_64-x.xx.xxx.xxxx.rpm to support RPM-based 64-bit Linux environments.
   - Xeroxv5Pkg-Linuxx86_64-x.xx.xxx.xxxx.deb to support Debian-based 64-bit Linux environments.
   - Xeroxv5Pkg-SunOSi386-x.xx.xxx.xxxx.pkg.gz for Sun Solaris x86 systems.
   - Xeroxv5Pkg-SunOSsparc-x.xx.xxx.xxxx.pkg.gz for Sun Solaris SPARC systems.
2. To install the custom driver, log in as root then type the following command:
   - AIX: **rpm -U Xeroxv5Pkg-AIXpowerpc-x.xx.xxx.xxxx.rpm**
   - HPUX: **swinstall -s Xeroxv5Pkg-HPUXia64-x.xx.xxx.xxxx.depot.gz /***
   - Linux (RPM based): **rpm -U Xeroxv5Pkg-Linuxi686-x.xx.xxx.xxxx.rpm**
   - Linux (Debian based): **dpkg -i Xeroxv5Pkg-Linuxi686-x.xx.xxx.xxxx.deb**
   - Solaris (x86 based): **pkgadd -d Xeroxv5Pkg-SunOSi386-x.xx.xxx.xxxx.pkg**
   - Solaris (SPARC based): **pkgadd -d Xeroxv5Pkg-SunOSsparc-x.xx.xxx.xxxx.pkg**

   The installation creates a Xerox directory in /opt/Xerox/prtsys.

Launching Xerox® Printer Manager

To launch Xerox® Printer Manager:

1. From your computer, access a command window. At the command prompt, log in as root, then type `xeroxofficeprtmgr`.
2. Press **Enter** or **Return**.

Printing from a Linux Workstation

To print from a Linux workstation, install either a Xerox® print driver for Linux or a CUPS (Common UNIX Printing System) print driver. You do not need both drivers.

Xerox recommends that you install one of the full-featured custom print drivers for Linux. To locate drivers for your printer, go to www.support.xerox.com.

If you use CUPS, ensure that CUPS is installed and running on your workstation. The instructions for installing and building CUPS are contained in the *CUPS Software Administrators Manual*, written and copyrighted by Easy Software Products. For complete information on CUPS printing capabilities, refer to the *CUPS Software Users Manual* available from www.cups.org/documentation.php.

Installing the PPD File on the Workstation

1. On the Xerox Support website, from the Drivers and Downloads page, download the Xerox® PPD for CUPS (Common UNIX Printing System).
2. Copy the PPD file into the CUPS ppd/Xerox folder on your workstation. If you are unsure of the location of the folder, use the **Find** command to locate the PPD files.
3. Follow the instructions that are included with the PPD file.

Adding the Printer

1. Verify that the CUPS (Common UNIX Printing System) daemon is running.
2. Open a Web browser, type `http://localhost:631/admin`, then press **Enter** or **Return**.
3. For User ID, type `root`. For password, type the root password.
4. Click **Add Printer**, then follow the onscreen prompts to add the printer to the CUPS printer list.

Printing with CUPS (Common UNIX Printing System)

CUPS supports the use of both the System V (lp) and Berkeley (lpr) printing commands.

1. To print to a specific printer in System V, type `lp -dprinter filename`, then press **Enter**.
2. To print to a specific printer in Berkeley, type `lpr -Pprinter filename`, then press **Enter**.

AS/400

Xerox provides Work Station Customization Object (WSCO) files to support AS/400 or Iseries, V5R2 or later systems. The WSCO file provides printer-specific PCL codes. The host print transform uses these codes to select the correct tray, 2-sided printing option, font size and type, and orientation. The XTOOLSxxxx library provides a source WSCO for each supported Xerox® printer. You only download and install the library once.

Note:

- The host print transform only works on AFPDS and SCS files. Convert IPDS formatted printer files to AFPDS files to use the WSCO for printing.
- You must have IOSYSCFG permissions to create a device description or a remote queue.
- For details on AS/400, refer to the *IBM AS/400 Printing V, (Red Book)*, available on the IBM website.

Installing the WSCO and Setting up Print Queues

For detailed instructions on installing the library and setting up print queues, refer to the installation instructions that are included with the library.

Print from USB

This feature allows you to print a file that is stored on a USB Flash Drive from the USB port on the printer control panel.

Before you begin:

Enable USB ports. For details, refer to USB Port Security.

Enabling Print from USB

1. In the Embedded Web Server, click **Properties > Apps**.
2. Click **Print From > Print from USB**.
3. For Enablement, select **Enabled**.
4. Click **Apply**.

Print from Mailbox

Print from mailbox allows you to print a file that is stored in a folder on the printer hard drive.

Enabling Print From Mailbox

1. In the Embedded Web Server, click **Properties > Apps**.
2. Click **Print From > Print From Mailbox**.
3. For Scan to Mailbox, select **Enabled**.
4. For Print From Mailbox, select **Enabled**.

   Note: You must enable Scan to Mailbox before you can enable Print From Mailbox.

5. To set the default view to show folders on the Scan tab in the Embedded Web Server, select **On Scan tab, view Mailboxes by default**. If you clear this option, the default becomes Workflows.
6. Click **Save**.

   Note: For instructions on using this feature, refer to the *User Guide* for your printer model.

Allowing Users to Interrupt Active Print Jobs

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **Device Settings > Interrupt Printing Enablement**.
3. Touch **Enable**.
4. Touch **OK**.

Specifying Output Settings

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **Device Settings**.
3. Touch **Output**.
4. To prioritize copy and print jobs, select **Contention Management**. Select an option.
   - **Priority**: This option specifies the relative priority of the copy or print jobs. The lower the number, the higher the priority.
   - **First In/First Out**: This option schedules jobs to print based on their entry into the Job Queue.
5. To specify the default output location for jobs that do not have finishing options, select **Output Location**, then select an option.
6. To specify where the device applies staples to a print job, select **Staple Productivity Mode**, then select an option.
7. To specify how the device handles a print job that requires staples when the stapler is empty, select **Out of Staples Options**, then select an option.
8. To save the settings, touch **OK**.

Note: Not all options listed are supported on all devices. Some options apply only to a specific device model, configuration, operating system, or driver type. Some options are available only if a finisher is installed.

6

Copying

This chapter contains:

Setting Copy Presets

Specifying Default Copy Settings

1. In the Embedded Web Server, click **Properties > Apps**.
2. Click **Copy > Setup**.
3. For color devices, do the following:
   - To require users to select the output color at the control panel, for Color Presets Screen, select **On**. This setting allows you to conserve supplies. For example, when Auto Detect is on, the device detects color in an original document that is almost entirely black and white. This setting prevents you from accidentally copying in color when you intend to copy in black and white.
   - For Output Color, select the color mode that the device uses for copies. If you select Single Color, for Single Color, select the color.
   - For 2-Sided Copying, select an option.
   - To rotate the second side, select **Rotate Side 2**.
4. For monochrome devices, for Toner Saver, select an option.
5. Click **Apply**.

Specifying Feature Defaults for Copy Settings at the Control Panel

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **App Settings > Copy App**.
3. Touch **Feature Defaults**.
4. Edit settings as needed for output, image quality, layout, output format, and job assembly.
5. Touch **Done**.

Note: Not all options listed are supported on all devices. Some options apply only to a specific device model, configuration, operating system, or driver type.

Setting the Color Presets Screen

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **App Settings > Copy App**.
3. Touch **Color Preset Screen** or **Toner Saver**.
4. Select an option.
5. Touch **OK**.

Note: Not all options listed are supported on all devices. Some options apply only to a specific device model, configuration, operating system, or driver type.

Setting Edge Erase Presets

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **App Settings > Copy App**.
3. Touch **Edge Erase Presets**.

Creating an Edge Erase Preset

To create an Edge Erase Preset:

1. Touch **Presets**, then from the list of presets, touch **Available**.
2. To name the preset, touch the existing preset name, then type a new name using the touch screen keyboard.

   Note: The default name for a new preset is [Available].

3. Edit the edge-erase settings as needed.
4. Touch **OK**.

Editing an Existing Preset

To edit an existing preset:

1. Touch **Presets**, then touch the needed preset.
2. To change the preset name, touch the existing preset name, then type a new name using the touch screen keyboard.
3. Touch **Side 1**, then to change the amount to erase from each edge, touch the arrows.
4. Touch **Side 2**, then to change the amount to erase from each edge, touch the arrows, or touch **Mirror Side 1**.
5. To change the preset name, touch the name field, type the new name, then touch **OK**.
6. Touch **OK**.

Setting Image Shift Presets

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **App Settings > Copy App**.
3. Touch **Image Shift Presets**.
4. Touch **Presets**, then touch the desired preset.
5. For Side 1, to change the amount of Up/Down and Left/Right shift, touch the arrows.
6. For Side 2, to change the amount of Up/Down and Left/Right shift, touch the arrows, or touch **Mirror Side 1**.
7. To change the preset name, touch the name field, type the new name, then touch **OK**.
8. To save the settings, touch **OK**.

Setting Reduce/Enlarge Presets

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **App Settings > Copy App**.
3. Touch **Reduce/Enlarge Presets**.
4. To change a proportional preset:
    a. Touch **Proportional %**.
    b. Select a preset.
    c. To type the percentage, use the touch-screen keypad, or touch Plus (**+**) or Minus (**-**).
    d. Touch **OK**.
5. To change a preset that uses an independent percentage for the width and length of the image:
    a. Touch **Independent %**.
    b. Select a preset.
    c. To type the scale percentage, use the touch-screen keypad, or touch Plus (**+**) or Minus (**-**).
    d. Touch **OK**.

Setting the Reading Order Options

You can change the order that pages are scanned in books, which impacts Book Copy and Book Fax features. You can also change the order that pages are printed, which impacts the Page Layout and Booklet Creation features.

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **App Settings > Copy App**.
3. Touch **Reading Order Options**.
4. For Scan Order or Print Order, touch an option.
5. If you selected Show Reading Order, for Default Reading Order, touch **Left to Right** or **Right to Left**.
6. Touch **OK**.

Disabling Automatic Image Rotation

When you have Auto Reduce/Enlarge or Auto Paper selected, the printer automatically rotates the image as needed. You can disable image rotation when either Auto Reduce/Enlarge or Auto Paper is selected.

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **App Settings > Copy App**.
3. Touch **Auto Image Rotation**.
4. For Auto Reduce/Enlarge or Auto Paper, select **Disable Rotation**.
5. Touch **OK**.

Specifying ID Card Copy Settings

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **App Settings > ID Card Copy App**.

Setting ID Card Copy Defaults

To set ID card copy defaults:

1. Touch **Defaults**.
2. Do one or more of the following.
   - To edit the default setting for number of copies to print, touch **Quantity**. Select a number, then touch **Enter**.
   - To set the default percentage that copy output is reduced or enlarged, touch **Reduce / Enlarge**, then select an option.
   - To edit the default setting for paper tray or type, touch **Paper Supply**, then select a paper tray or type.
   - To edit the default setting for the proportion of text to images on the original document, touch **Original Type**, then select an option.
   - To edit the default setting for lightness or darkness, for Lighten / Darken, move the slider.
   - To edit the default setting for Automatic Background Suppression, touch the toggle button.

     Note: A check mark on the toggle button indicates Enabled.

   - To reset all features to the original factory-default settings, touch **Reset**.
3. Touch **Next**.
4. Touch **Done**.

Specifying Output Settings

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **Device Settings**.
3. Touch **Output**.
4. To prioritize copy and print jobs, select **Contention Management**. Select an option.
   - **Priority**: This option specifies the relative priority of the copy or print jobs. The lower the number, the higher the priority.
   - **First In/First Out**: This option schedules jobs to print based on their entry into the Job Queue.
5. To specify the output location for jobs, select **Output Location**, then select an option.
6. To separate print sets within a print job, select **Within Job Offsetting**, then select **Enable** or **Disable**.

   Note: If you select **Disable**, the device stacks all printed sets together.
7. To specify how the device handles a print job that requires staples when the stapler is empty, select **Out of Staples Options**, then select an option.
8. To save the settings, touch **OK**.

   Note: Not all options listed are supported on all devices. Some options apply only to a specific device model, configuration, operating system, or driver type. Some options are available only if a finisher is installed.

7

Scanning

This chapter contains:

Scanning to an Email Address

The email feature allows you to scan a document and send it to an email address as an attachment.

Before you begin:

- Configure SMTP settings. Note the IP Address or host name of your SMTP server. For details, refer to Configure SMTP Server Settings.
- Create an email account for the printer. The printer uses this address as the default text in the From: field of the email.

For instructions on using this feature, refer to the *User Guide* for your printer model.

Email

Configure email settings in the Embedded Web Server, on the Email Setup page. Email settings apply to other apps that use SMTP.

Accessing the Email Setup Page

1. In the Embedded Web Server, click **Properties > Apps**.
2. Click **Email > Setup**.

Editing User Policy Settings

1. On the Email Setup page, click the **Security** tab.
2. To edit permissions roles, for Manage user permissions, click **Edit**.
3. To configure email recipient settings, for Only send to self, click **Edit**.
   - To restrict authenticated users from sending emails to others, for Only send to Self, select **On**. This setting disables the New Recipient and Address Book buttons, preventing users from adding more recipients.
   - To require users to select email addresses from an address book, for Restrict Manual Entry of Email Address, select **On**.
   - To clear the To, CC, and BCC fields after a user presses the Start button on the control panel, for Clear To:, Cc:, and Bcc: fields after selecting Send, select **On**.

Configuring Required Settings

1. On the Email Setup page, click the **Required Settings** tab.
2. To configure SMTP settings, next to SMTP, click **Edit**. For details, refer to SMTP.
3. To configure From Field settings, next to the From Field, under Action, click **Edit**.

Configuring From Field Settings

1. For Default From Address, type the email address you want sent from the printer.
2. To always use the default email address, for Always use Default From Address, select **Yes**.
3. Select the LDAP search result conditions in which authenticated users are allowed to edit the From field.

4. To allow users to edit the From field without authentication, for Edit From Field when Authentication is not Required, select **Yes**.
5. To use sender's name with the email address, select **Add sender's name to email address**.
6. Click **Save**.

Configuring General Email Settings

1. On the Email Setup page, click the **General** tab.
2. For Subject, type the text that you want to appear in the subject line of emails sent from the printer.
3. For Message body, type the text that you want to appear in the body of emails.
4. To include the user name or email address in the body of emails, for User, select **User Name**, **Email Address**, or both.
5. To include attachment information in the message body, select **Number of Images**, **Attachment File Type**, or both.
6. To include information about the printer in the message body, for Multifunction Device System, select the information that you want to include.
7. For Signature, type the information that appears at the end of the email message.
8. For Confirmation Sheet, select an option:
   - **Errors Only**: This option instructs the printer to print a confirmation sheet only when a transmission error occurs. The confirmation sheet lists error information and indicates that the job has reached the SMTP server. The confirmation sheet does not indicate that the email message was delivered.
   - **On**: This option instructs the printer to print a confirmation sheet.
   - **Off**: This option instructs the printer not to print a confirmation sheet. You can find status about a job in the job log.

   Note: To see the job log, at the control panel touch screen, touch **Jobs > Completed Jobs**.
9. To add the email address of the sender to the To field in email, for Auto Add Me, select **Enabled**.
10. Click **Apply**.

Configuring Address Book Settings

1. In the Embedded Web Server, click **Properties > Apps > Email > Setup**.
2. Click the **Address Books** tab.
3. To configure the Address Book settings stored in the device, for Device Address Book, click **Edit**.
4. To use a Network Address book, configure LDAP server settings, for Network Address Book, click **Edit**.
5. If you configured Address Book settings stored in the device, for Use Device Address Book, select an option.
   - To allow users to access the address book, select **Yes**. To show Favorites as the initial view upon entering the address book, select **View Favorites on Email Service Entry**.
   - To restrict users from accessing the address book, select **No**.

6. If you configured a Network Address Book, for Use Network Address Book, select an option.
   - To allow users to access this address book, select **Yes**.
   - To restrict users from accessing the address book, select **No**.
7. To set the policy for creating and editing contacts on the device touch screen, for Create / Edit Contact from Touch Screen, select an option.
   - To allow all users to create and edit contacts on the device touch screen, select **All Users**.
   - To restrict creating and editing contacts on the device touch screen to system administrators, select **System Administrators Only**.
8. Click **Apply**.

   Note: For details, refer to Help in the Embedded Web Server.

Configuring Default Email Settings

1. On the Email Setup page, click the **Defaults** tab.
2. To edit default Scan to Email settings, for Scan to Email, click **Edit**.
3. To edit default Image Options, Image Enhancement, Resolution, and Quality / File Size settings, for Advanced Settings, click **Edit**.
4. To edit default Original Orientation, Original Size, Edge Erase, and Blank Page Management settings, for Layout Adjustment, click **Edit**.
5. To edit default File Format and Filename Extension settings, for Email Options, click **Edit**.
6. To create a custom email attachment file name, for Email Options, click **Edit**.

   Note: For details, refer to Help in the Embedded Web Server.

Setting File Compression Options

1. On the Email Setup page, click the **Compression** tab.
2. Select **.tiff**, **.pdf**, and **.xps** compression settings as needed. For details, refer to the Help in the Embedded Web Server.
3. Click **Apply**.

Configuring Email Security Settings

Configuring Encryption and Signing Settings

1. On the Email Setup page, click the **Security** tab.
2. To edit encryption and signing settings, on the Security tab, under Encryption/Signing, click **Edit**.

Configuring Email Signing Settings

Before you begin:

- Configure Smart Card Authentication. For details refer to Configuring Smart Card Authentication.
- Ensure that signing certificates are installed on all Smart Cards.

1. On the Email Encryption/Signing page, click the **Signing** tab.

2. To enable Email Signing, on the Signing tab, under Email Signing Enablement, select an option:
   - **Always On; Not editable by user** restricts users from turning Email Signing off at the control panel.
   - **Editable by user** allows users to turn on or off Email Signing at the control panel.
3. If you select Editable by user, select the default setting for users at the control panel. Under Email Signing Default, select **On** or **Off**.
4. Under Signing Hash, select a method.
5. Click **Apply**.

Configuring Email Encryption Settings

Before you begin:

- If you want to use the public keys stored on smart cards to encrypt email messages, configure Smart Card Authentication.
- If you want to use the public keys stored in an address book, configure a Network Address Book or the Device Address Book.

Note:

- If you only configure Smart Card Authentication, users can send encrypted emails to themselves only.
- To store public keys in the Device Address Book, configure the Import Using Email feature, and select **Import encryption certificate from signed emails**.

1. Click the **Encryption** tab.
2. To enable Email Encryption, on the Encryption tab, under Email Encryption Enablement, select an option:
   - **Always On; Not editable by user** restricts users from turning off Email Encryption at the control panel.
   - **Editable by user** allows users to turn Email Encryption on or off at the control panel.

   If you select Editable by user, select the default setting for users at the control panel. Under Email Encryption Default, select **On** or **Off**.
3. Under Encryption Algorithm, select an encryption method.
4. Click **Apply**.

Editing Domain and Email Filter Settings

1. On the Email Setup page, click the **Security** tab.
2. To edit domain filter and email filter settings, under Network Policies, click **Edit**.
3. To enable a domain filter list, under Domain Filter settings, select **Allow Domains** or **Block Domains**.
4. Under New Domain, type the domain you want to add to the list and click **Add**.
5. To remove a domain from the list, select a domain, and click **Remove**.

6. To allow LDAP email address searches without the @ symbol, under **Allow LDAP Email Address without the @ Requirement**, select **On**.

   Note:

   - Ensure that your mail server supports this requirement.
   - If you select **On** under **Allow LDAP Email Address without the @ Requirement**, the number of items returned by an LDAP search can increase.

Workflow Scanning

Workflow Scanning allows you to scan an original document, distribute, and archive the scanned image file. The Workflow Scanning feature simplifies the task of scanning many multiple-page documents and saving the scanned image files in one or more file locations.

Note: For instructions on using this feature, refer to the *User Guide* for your device.

To specify how and where scanned images are stored, create a workflow. You can create, manage, and store multiple workflows in a workflow pool repository on a network server.

There are several workflow options:

- Distribution workflows enable you to scan documents to one or more file destinations. File destinations include an FTP site, a website, and a network server. You can add fax destinations to workflows too. To configure the default workflow, refer to Configuring the Default Workflow.
- Scan to Mailbox enables you to scan documents to public or private mailbox folders on the printer hard drive. To configure the Scan to Mailbox feature, refer to Scanning to a Folder on the Device.
- Scan to USB enables you to scan documents to a connected USB Flash drive. To configure the Scan to USB feature, refer to Scan to USB.
- Scan to Home enables you to scan documents to a personal home folder on your network. To configure the Scan to Home feature, refer to Scanning to a User Home Folder.

Enabling Workflow Scanning

1. In the Embedded Web Server, click **Properties > Apps**.
2. Click **Workflow Scanning > Scanning Web Apps**.
3. For Scan Workflow Management, click **Edit**.

   The HTTP page opens.
4. On the HTTP page, for Scan Services, enable **Scan Workflow Management**.
5. Click **Save**.

Configuring File Repository Settings

A file repository is a network location where scanned images are stored. Before you create a workflow, configure the file repository settings.

Note: You can add file destinations to a workflow from the predefined list of file repository settings.

- In the Embedded Web Server, to create a new workflow, you can add file destinations from the predefined list.
- In the Workflow Scanning App, for a selected workflow, you can add more file destinations from the predefined list.

Your device supports the following transfer protocols:

- FTP
- SFTP

- SMB
- HTTP/HTTPS

Note: HTTP/HTTPS scans to a Web server using a CGI script.

FTP or SFTP

Before you begin:

- Ensure that FTP or SFTP services are running on the server or computer being used to store scanned image files. Note the IP address or host name.
- Create a user account and password with read and write access for the printer to use to access the repository folder. Note the user name and password.
- Create a folder within the FTP or SFTP root. Note the directory path, user name, and password. This folder is your file repository.
- Test the connection. Log in to the file repository from a computer with the user name and password. Create a folder in the directory, then delete it. If you cannot create and delete the folder, check the user account access rights.

To configure file repository settings for FTP or SFTP:

1. In the Embedded Web Server, click **Properties > Apps**.
2. Click **Workflow Scanning > File Repository Setup**.
3. Click **Add New**.
4. In the Friendly Name field, type a name for the repository.
5. For Default Repository Protocol, click the arrow, then select **FTP** or **SFTP**.
6. Select the address type. Options for FTP include **IPv4**, **IPv6**, or **Host Name**. Options for SFTP include **IPv4**, or **Host Name**.
7. Type the appropriately formatted address and port number of your server.
8. For Default Repository Document Path, type the directory path of the folder beginning at the root of FTP or SFTP services. For example, //directoryname/foldername.
9. If you want the printer to create **.XSM** subfolders for single page format files, select **Sub-folder (. XSM) for 1 File Per Page, File Format jobs**.
10. For Default Repository Login Credentials, select an option:
    - **Authenticated User and Domain**: This option instructs the device to use the user name and domain of the logged-in user when the device accesses the repository.
    - **Logged in User**: This option instructs the device to log in to the repository with the credentials of the logged-in user.
    - **Prompt at device control panel**: This option instructs the device to prompt users at the control panel for the repository credentials.
    - **Device**: This option instructs the device to use specific credentials when it accesses the repository.
11. For Login Name and Password, type the credentials.
12. To update an existing password, select **Select to save new password**.
13. Click **Save**.

SMB

Before you begin:

- Ensure that SMB services are running on the server or computer where you want to store scanned image files. Note the IP address or host name.
- On the SMB server, create a shared folder. This folder is your file repository. Note the directory path, Share Name of the folder, and the Computer Name or Server Name.
- Create a user account and password with read and write access for the printer to use to access the repository folder. Note the user name and password.
- Test the connection by logging in to the file repository from a computer with the user name and password. Create a folder in the directory, then delete it. If you cannot do this test, check the user account access rights.

To configure file repository settings for SMB:

1. In the Embedded Web Server, click **Properties > Apps**.
2. Click **Workflow Scanning > File Repository Setup**.
3. Click **Add New**.
4. In the Friendly Name field, type a name for the repository.
5. For Default Repository Protocol, click the arrow, then select **SMB**.
6. Select the address type. Options are **IPv4** or **Host Name**.
7. Type the appropriately formatted address and port number of your server.
8. In the Share field, type the share name.
9. For Default Repository Document Path, type the directory path of the folder starting at the root of the shared folder. For example, if you have a folder named scans in the shared folder, type **/scans**.
10. If you want the printer to create **.XSM** subfolders for single-page-format files, select **Sub-folder (. XSM) for 1 File Per Page, File Format jobs**.
11. For Default Repository Login Credentials, select an option:
    - **Authenticated User and Domain**: This option instructs the device to use the user name and domain of the logged-in user when it accesses the repository.
    - **Logged in User**: This option instructs the device to log in to the repository with the credentials of the logged-in user.
    - **Prompt at device control panel**: This option instructs the device to prompt users at the control panel for the repository credentials.
    - **Device**: This option instructs the device to use specific credentials when it accesses the repository.
12. For Login Name and Password, type the credentials.
13. To update an existing password, select **Select to save new password**.
14. Click **Save**.

HTTP/HTTPS

Before you begin:

- Enable HTTP or Secure HTTP (SSL). Ensure that a certificate is installed on the printer if you are using SSL.
- Configure your Web server, and ensure that HTTP/HTTPS services are running. POST requests and scanned data are sent to the server and processed by a CGI script. Note the IP address or host name of the Web server.
- Create a user account and password for the printer on the Web server. Note the user name and password.
  - Create a /home directory for the printer.
  - Create a /bin directory in the home directory.
  - Copy an executable CGI script into the /bin directory. You can create your own script, or download a sample script. For details, refer to CGI Scripts. Note the path to the script. The script can be defined with script_name.extension or by path/script_name.extension.
- Create a folder with read and write permissions on the Web server, or alternate server. Note the directory path, user name, and password. This folder is your file repository.
- Test the connection by logging in to the home directory of the printer on the Web server. Send a POST request and file to the Web server. Check to see if the file is in the repository.

CGI Scripts

A CGI (Common Gateway Interface) script is a program on a Web server that is executed when the server receives a request from a browser. A CGI script is required to allow files to be transferred to your HTTP server from your printer.

When a document is scanned, the printer logs in to the Web server, sends a POST request along with the scanned file, then logs out. The CGI script handles the remaining details of file transfer.

To download a sample CGI script:

1. In the Embedded Web Server, click **Properties > Apps**.
2. Click **Workflow Scanning > File Repository Setup**.
3. Click **Add New**.
4. For Default Repository Protocol, select **HTTP** or **HTTPS**.
5. For Script path and filename, click **Get Example Scripts**.
6. Select a script language supported by your Web server. Right-click and save the appropriate **.zip** or **.tgz** file to your computer.
7. Extract the downloaded file to the root of the Web services home directory.

Configuring File Repository Settings for HTTP/HTTPS

1. In the Embedded Web Server, click **Properties > Apps > Workflow Scanning > File Repository Setup**.
2. Click **Add New**.
3. In the Settings area, configure the following items:
   a. For Friendly Name, type a name for the repository.
   b. For Default Repository Protocol, select **HTTP** or **HTTPS**, then select an address type. Options are **IPv4 Address**, **IPv6 Address**, or **Host Name**.

c. For Default Repository Server, type the appropriately formatted address and port number of your server.

4. To validate the SSL certificate used for HTTPS, select **Validate Repository Certificate**.

   Note: To verify that a digital certificate is installed on the device, click **View Root/ Intermediate Trusted Certificates**.

5. For Script path and filename, type the path to the CGI script, starting at the root. For example: /directoryname/foldername. To download working example scripts, click **Get Example Scripts**.

6. For Default Repository Document Path, type the directory path of the folder. For Web server directories, type the path, starting at the root. For example, //directoryname/foldername.

7. If you want the device to create **.XSM** subfolders for single-page-format files, select **Sub-folder (. XSM) for 1 File Per Page, File Format jobs**.

8. For Default Repository Login Credentials, select an option:
   - **Authenticated User and Domain**: This option instructs the device to use the user name and domain of the logged-in user when it accesses the repository.
   - **Logged in User**: This option instructs the device to log in to the repository with the credentials of the logged-in user.
   - **Prompt at device control panel**: This option instructs the device to prompt users at the control panel for the repository credentials.
   - **Device**: This option instructs the device to use specific credentials when it accesses the repository. If you select Device, type the credentials in the Login Name and Password fields. To update an existing password, select **Select to save new password**.
   - **None**: This option instructs the device to access the repository without providing credentials.

9. To update an existing password, select **Select to save new password**.

10. Click **Save**.

Configuring the Default Workflow

Before you can use the Workflow Scanning feature, create and edit a workflow. A workflow contains scan settings, and at least one destination for the scanned image files.

Configure the default workflow before you create a workflow. After the default workflow is configured, all new workflows inherit the default workflow settings. You can edit new workflows as needed.

The default workflow cannot be deleted.

1. In the Embedded Web Server, click **Properties > Apps**.

2. Click **Workflow Scanning > Default Workflow**.

3. For Destination Services, select an option:
   - To add File Destinations, select **File**.
   - To add Fax Destinations, select **Fax**.

4. Add File Destinations, Fax Destinations, Document Management Fields, then configure other scanning options as needed.

Adding a File Destination

1. For File Destinations, click **Add**.

2. From the menu, select the required **Filing Policy**.
3. Click **Save**.

Adding a Fax Destination

1. For Fax Destinations, click **Add**.
2. Type a fax number in the Add Fax Number field, then click **Add**.
3. For Delivery, select **Delayed Send**, then type a time if you want to send the fax at a specific time.
4. Click **Apply** to save the new settings or **Cancel** to return to the previous screen.

Configuring Other Default Workflow Scanning Options

1. Click **Edit** to edit the following settings. For details, refer to the Help in the Embedded Web Server.
   - Workflow Tags
   - Workflow Scanning
   - Advanced Settings
   - Layout Adjustment
   - Filing Options: To enable the Add to pdf Folder feature for a scan file that already exists, for File Format, select **PDF** and **1 File Per Page**.
   - Job Assembly
   - Filename Extension
   - Report Options
   - Scan to Image Settings
   - Compression Settings
2. To restore the Default Workflow to its original settings, click **Apply Factory Settings**. This action deletes any custom settings applied to the Default Workflow.

Configuring Workflow Scanning General Settings

Workflow Scanning allows you to scan an original document, distribute, and archive the scanned image file. The Workflow Scanning feature simplifies the task of scanning many multi-page documents and saving the scanned image files in one or more file locations.

You can create workflows or edit the default workflow to specify how and where scanned images are stored or sent. Workflows can reside on the printer or in a pool of workflows that are stored on a remote server. When you configure the default workflow, all subsequent workflows inherit the settings from the default workflow.

To configure Workflow Scanning general settings:

1. In the Embedded Web Server, click **Properties > Apps**.
2. Click **Workflow Scanning > General Settings**.
3. For Confirmation Sheet, select when you want a confirmation sheet to print.
   - **Errors Only**: This option instructs the printer to print a confirmation sheet only when a workflow scanning job generates an error.
   - **On**: This option instructs the printer to print a confirmation sheet.

- **Off**: This option instructs the printer not to print a confirmation sheet. You can find status about a job in the job log.

  Note: To see the job log, at the control panel touch screen, touch **Jobs > Completed Job Queue**.

4. To allow users to add file destinations to workflows manually, for Allow Manual Entry of File Destinations, select **Enabled**.
5. To configure the list of workflows contained in a network workflow pool repository to refresh automatically, for Enable Automatic Refresh, select **Enabled**. The list of workflows appears on the control panel.
6. To change the time that workflows update, for Daily Start time, enter the hour and minute, then select **AM** or **PM**.
7. To update the workflow list immediately, click **Refresh Workflow List Now**.
8. To configure the user name to appear in the job log, for Optional Information, select **User Name**. If you added Document Management Fields to a workflow, the job log is stored with scanned image files.
9. Click **Apply**.

Configuring Single-Touch App

You can customize the naming convention of files generated during Workflow Scanning. For example, you can:

- Assign file names in a numbered sequence.
- Select standard options or add custom text.
- Add advanced features such as including the date and time in the name.

To customize file names:

1. In the Embedded Web Server, click **Properties > Apps**.
2. Click **Workflow Scanning > Single-Touch App**.
3. Click **Create**.
4. On the New Service page, type a name and description for the app.
5. Click **Create**.

   Note:

   - After you create an app, you can edit the description, but not the name of the app.
   - You can create up to 10 apps.
   - After you design your app and select a scan workflow for your app, the single-touch app appears on the control panel touch screen.

Configuring Custom File Naming

1. In the Embedded Web Server, click **Properties > Apps**.
2. Click **Workflow Scanning > Custom File Naming**.

3. To add a prefix for the scanned image file name, for File Naming, select **Auto**. For Name, type the prefix.
4. To choose the elements that you want to use to build the file name, select **Custom Naming**.
   a. Select elements as needed. As you select display elements, they appear in the Position field.
      - Date
      - Time
      - Job ID
      - User ID
      - Custom Text

      Note: For Custom Text, type the custom text that you that want to appear in the file name. For example, select the first Custom Text field and then type an underscore (_). The underscore appears in the Position field. You can include up to four Custom Text strings in the file name.

   b. To reposition the order of multiple Custom Text strings, for Position, click a text string. To move the selected text string into the correct position for the file name, use the Arrow buttons. The generated file name uses all of the text strings in order, from top to bottom.
   c. **Advanced**: To create the file name, type a string with variables. For details, refer to the Help in the Embedded Web Server.
5. Click **Apply**.

Setting Workflow Display Settings for the Control Panel

1. In the Embedded Web Server, click **Properties > Apps**.
2. Click **Workflow Scanning > Display Settings**.
3. To specify the workflow that appears at the top of the list, for Workflows, select a workflow, then click **Promote**.
4. To prevent users from using the default scanning workflow, for Display Default Workflow, select **Hide Default Template in the Templates list**.

   Note: If you select Hide Default Template and there are no other workflows, the default workflow appears until you add at least one more workflow.

5. To configure workflow selection when users access the Scan app, for Workflow Selection on Entry of App, select an option:
   - **Automatically select the Promoted template**: This option selects the promoted workflow automatically.
   - **User must select a template before pressing Start**: This option requires users to select a workflow before they touch Start.
6. Click **Apply**.

Enabling Remote Scanning using TWAIN

Enable Remote Start to allow users to scan images into a TWAIN-compliant application using the TWAIN driver.

Before you begin, enable the Scan Extension Web service. For details, refer to HTTP - Web Services.

1. In the Embedded Web Server, click **Properties > Apps**.
2. Click **Workflow Scanning > Remote Start (TWAIN)**.
3. For Start Job via Remote Program, click **On**.
4. Click **Apply**.

Configuring a Validation Server

You can use a validation server to verify scan metadata entered at the printer control panel. A validation server compares the metadata with a list of valid values.

1. In the Embedded Web Server, click **Properties > Apps**.
2. Click **Workflow Scanning > Validation Servers**.
3. Click **Add**.
4. Select **HTTP** or **HTTPS**.
5. For Protocol, select the address type. Options are **IPv4**, **IPv6**, or **Host Name**.
6. Type the appropriately formatted address and port number in the IP Address: Port field. The default port number is 80 for HTTP and 443 for HTTPS.
7. For Path, type the path on the server.

   Note: The format for a directory path for FTP is /directory/directory, whereas the format for a directory path for SMB is /directory/directory.

8. For Response Timeout, type a number in seconds.
9. To save the settings, click **Apply**. To return to the previous screen, click **Cancel**.

Configuring Workflow Pool Repository Settings

You can store scanning workflows on your network in a workflows pool repository. Scanning workflows contain details about scan jobs that can be saved and reused for other scan jobs.

If you use a scanning management application, such as SMARTsend or ScanFlowStore, provide information about the server that hosts the workflows on this page.

1. In the Embedded Web Server, click **Properties > Apps**.
2. Click **Workflow Scanning > Advanced > Workflow Pool Management**.
3. For Settings, from the menu, select the desired protocol.

4. Type the required information for the protocol. Follow the same steps used for setting up a file repository for the protocol.

   Note:

   - For details, in the Embedded Web Server, view the online help for the selected protocol.
   - The format for a directory path for FTP is /directory/directory, whereas the format for a directory path for SMB is /directory/directory.

5. To save the new settings, click **Apply**. To retain the previous settings, click **Cancel**.
6. To reset settings to default values, click **Default All**.

Configuring Unspecified Defaults

1. In the Embedded Web Server, click **Properties > Apps**.
2. Click **Workflow Scanning > Advanced > Unspecified Defaults**.
3. For Advanced Settings, select a scanning resolution.
4. For Filing Options, select a TIFF Rotation Method.
5. For Workflow Distribution Repositories, select a Login Source.
6. Click **Apply**.

Managing Scan Workflows

A workflow contains scan settings and at least one destination for the scanned image files. You can associate a scan workflow with your app or use the default workflow.

Note: If you select Default Workflow, configure the default workflow and add at least one file destination to the workflow.

Viewing a Scan Workflow

To view a scan workflow:

1. In the Embedded Web Server, click **Scan**.
2. For Display, select **Workflows**.
3. Select a workflow from the workflow list.

Creating a Scan Workflow

To create a scan workflow:

1. In the Embedded Web Server, click **Scan**.
2. For Display, select **Workflows**.
3. Click **Create New Workflow**.

Deleting a Scan Workflow

To delete a scan workflow:

1. In the Embedded Web Server, click **Scan**.
2. For Display, select **Workflows**.
3. Select a workflow from the workflow list.
4. At the top of the workflow page, click **Delete**.

Copying a Scan Workflow

To copy a scan workflow:

1. In the Embedded Web Server, click **Scan**.
2. For Display, select **Workflows**.
3. Select a workflow from the workflow list.
4. Click **Copy**.
5. Type the **Workflow Name**, **Description**, and **Owner**details, as needed.
6. Click **Add**.

Editing a Scan Workflow

To edit a scan workflow:

1. In the Embedded Web Server, click **Scan**.
2. For Display, select **Workflows**.
3. Select a workflow from the workflow list.
4. Click **Edit**.
5. On the workflow page, change the settings as needed:
   - To change the settings for a field, for the desired field, select the setting, then click **Edit**. Configure the settings as needed, then click **Apply** or **Save**.
   - To add settings to a field, for the desired field, click **Add**. Configure the settings as needed, then click **Apply** or **Save**.
   - To delete a setting from a field, select the setting, click **Delete**, then click **OK**.

Scanning to a Folder on the Device

The Scan to Mailbox feature allows users to scan files to mailboxes, which are folders created on the device hard drive. These files can then be retrieved through the Embedded Web Server. This feature provides network scanning capability without the need to configure a separate server and is supported in Workflow Scanning. For details, refer to Workflow Scanning.

For instructions on using this feature, refer to the *User Guide* for your device model.

Enabling or Disabling Scan to Mailbox

1. In the Embedded Web Server, click **Properties > Apps**.
2. Click **Scan to Mailbox > Enablement**.
3. For Scan to Mailbox, select **Enabled**.

   Note: When you enable Scan to Mailbox, at the control panel, folders appear as workflows in the list of scanning workflows.

4. To set the default view to show folders in the Embedded Web Server Scan tab, select **On Scan tab, view Mailboxes by default**.
5. To save the new settings, click **Save**. To retain the previous settings, click **Undo**.

Setting Scan Policies

Scan policies allow you to manage how users are allowed to scan files, create folders, and assign passwords to their folders on the printer.

1. In the Embedded Web Server, click **Properties > Apps**.
2. Click **Scan to Mailbox > Scan Policies**.
3. For Scan Policies, select or clear:
   - **Allow scanning to Default Public Folder**: This option allows users to scan files to the Default Public Folder without requiring a password.
   - **Require per job password for public folders**: This option requires users to type a password for every job they scan to the public folder.
   - **Allow additional folders to be created**: This option allows users to create public or private folders on the printer. If **Require password when creating additional folders** is disabled, assigning a password to the folder is optional and creates a public folder. If **Allow additional folders to be created** is disabled, the **Create Folder** button does not appear on the Scan tab.
   - **Require password when creating additional folders**: This option requires users to type a new password every time they create a folder. This feature only allows users to create private folders.
   - **Prompt for password when scanning to private folder**: This option requires users to type the password at the control panel every time they scan a job to a private folder.
   - **Allow access to job log data file**: This option allows users to print a job log containing details for any scanned image. Third-party applications can be used to search, file, and distribute jobs based on job log information.
4. For Password Management, type a minimum and maximum password length. Select password policies as needed.
5. Click **Save**.

Managing Folders and Scanned Files

Creating a Folder

By default, all users are allowed to scan to the Default Public Folder. If this option has been enabled in Scan Policies, users can create and edit additional folders.

To create a folder:

1. In the Embedded Web Server, click **Scan**.
2. For Display, select **Mailboxes**.
3. For Scan to Mailbox, click **Create Folder**.
4. Type a unique name for the folder.

   Type and retype a password as needed.
5. Click **Apply**.

Editing a Folder

To edit a folder:

1. In the Embedded Web Server, click **Scan**.
2. For Display, select **Mailboxes**.
3. Select the folder that you want to edit. If the folder is private, type the password, then click **OK**.
4. To change the folder password, click **Modify Folder**.
5. To edit the default scan settings for the folder, click **Personalize Settings > Edit**. For details, refer to the Help in the Embedded Web Server.

Deleting Scanned Files

1. In the Embedded Web Server, click **Properties > Apps**.
2. Click **Scan to Mailbox > Files**.
3. To remove the files from the server immediately, select an option.
   - To delete all files on the server, select **Delete all files now**.
   - To delete files older than a specified number of days, select **Delete all files older than**. Type how many days old files must be for deletion.
4. Click **Delete Files**.
5. For Schedule Clean Up of Folder Files, specify the files that you want to delete. Type how many days old files must be for deletion.
6. For Cleanup time, select an option.
   - To have files deleted at the beginning of every hour, select **Hourly**.
   - To specify the time of day for the delete process to run, select **Daily**, then type the number of days.

7. Click **Save**.

   Note: You can also delete scanned files from the Scan tab.

Deleting Scan Folders

You can modify or delete scan folders from two locations in the Embedded Web Server. Deleting folders from either location deletes them from the device.

Deleting Folders from the Properties Tab

To delete folders from the Properties tab:

1. In the Embedded Web Server, click **Properties > Apps**.
2. Click **Scan to Mailbox > Folders**.
3. To delete a folder, select the folder, then click **Delete Folder**.

Deleting Folders from the Scan Tab

To delete folders from the Scan tab:

1. In the Embedded Web Server, click **Scan**.
2. For Display, click **Mailboxes**, then select the folder that you want to delete. If the folder is private, type the password, then click **OK**.
3. Click **Modify Folder**, then click **Delete Folder**. If the folder is private, in the Old Password field, type the password again, then click **Delete Folder**.

Managing Folder Passwords

You can modify folder passwords from two locations in the Embedded Web Server. Modifying passwords from either location changes them on the device.

Modifying Folder Passwords from the Properties Tab

To modify folder passwords from the Properties tab:

1. In the Embedded Web Server, click **Properties > Apps**.
2. Click **Scan to Mailbox > Folders**.
3. For Created Folder Operations, select the folder from the list.
4. For Change Folder Password, type a new password.
5. For Confirm Folder Password, retype the password, then click **Save Password**.

Modifying Folder Passwords from the Scan Tab

To modify folder passwords from the Scan tab:

1. In the Embedded Web Server, click **Scan**.
2. Select **Mailboxes**, then select the folder you want to modify.
3. Click **Modify Folder**.

4. Type the old password.
5. For Change Folder Password, type a new password.
6. For Confirm Folder Password, retype the password, then click **Save Password**.

Monitoring Capacity

Capacity is the total space available for all mailboxes.

Note: If the available space is less than 100 MB or the current percentage used is above 99 %, your system requires cleanup to remove old, unneeded mailboxes and files.

To view the current capacity usage:

1. In the Embedded Web Server, click **Properties > Apps**.
2. Click **Scan to Mailbox > Capacity**.
   - **Capacity**: The total amount of space available on the device for scanned images.
   - **Used**: The space currently used to hold scanned images.
   - **Available**: The space left for scanned images.
   - **Percentage Used**: The amount of space used by scanned images as a percentage of the total space.

Scan to USB

You can insert a USB Flash Drive into the printer, scan a document, and store the scanned file on the USB drive.

Before you begin:

Enable USB ports. For details, refer to USB Port Security.

Enabling Scan to USB

1. In the Embedded Web Server, click **Properties > Apps**.
2. Click **Scan to USB > General**.
3. For Enablement, select **Enabled**.
4. To save the new settings, click **Save**. To retain the previous settings, click **Undo**.

Scanning to a User Home Folder

You can use the Scan to Home feature to scan to the home folder, as defined in your LDAP directory, or to a shared network folder.

Before you begin, configure authentication. For details, refer to Configuring Authentication Settings.

1. In the Embedded Web Server, click **Properties > Apps**.
2. Click **Scan to Home > General**.
3. In the Setup area, configure the following items:
   a. For Status, click **Enabled**.
   b. Type a Friendly Name. The Friendly Name is the default description of the workflow that appears when you select the workflow from the list at the control panel.
   c. Type a Workflow Name. The Workflow Name is the name of the workflow that appears in the list of workflows at the control panel. If you leave this field blank, the workflow name defaults to @S2HOME.
4. In the File Path area, configure the following items:
   a. For Home Directory, select an option:
      - To scan to the home folder defined in an LDAP directory, select **LDAP Query**.
      - To scan to a shared network folder, select **No LDAP Query**, then type the complete network path of the external server. For example, type //servername/foldername.

   b. If you created a subdirectory, specify your existing directory structure. For Sub-Directory, configure the following:
      - To create a subdirectory in the network home path, for Subdirectory, type a network path. For example, to scan to //servername/foldername/subdirectoryfoldername, type **/subdirectoryfoldername**.
      - To store scanned images in folders that are named according to each user on your network home path, select **Append User Name to Path**. An example path is //servername/foldername/username. The user name is the name used when logging in at the control panel.
      - To create individual folders for each user, select **Automatically Create User Name directory if one does not exist**.
5. If network authentication is configured to use a Kerberos server, and you want to modify the Kerberos settings, click the link **Prefer Filing with Kerberos Ticket**. Kerberos Tickets let you use the SMB protocol without selecting login credentials.
6. For Login Credentials to Access the Destination, select an option:
   - **Authenticated User and Domain**: This option instructs the device to use the user name and domain of the logged-in user when accessing the repository.
   - **Logged-in User**: This option instructs the device to log in to the repository using the credentials of the logged-in user.
   - **Prompt at User Interface:** This option instructs the device to prompt users at the control panel for the repository credentials.
   - **Device**: This option instructs the device to use specific credentials when accessing the repository. If you select Device, type the credentials in the Login Name and Password fields. To update an existing password, select **Select to save new password**.

7. To save a copy of the job log in the scan repository, for Save Job Log (.XST) in Repository, select **Enable**.
8. Click **Apply**.

Configuring Scan To

The Scan To feature allows you to associate scan destinations with address book contacts. Users can select the contacts when scanning using the Scan To feature.

Users can select multiple scan destinations in a single scan job. Scan destinations include the following locations:

- An email destination associated with an address book contact. Users can select contacts from the Device Address Book or the Network Address Book.
- An FTP, SFTP, or SMB folder location associated with a contact in the Device Address Book.
- A USB Flash drive.
- An SMB shared folder. Users can specify a network folder path or browse to a shared folder.

Note: For instructions on using this feature, refer to the *User Guide* for your device.

Before You Begin

- For scanning to destinations associated with address book contacts:
  - Add at least one contact to the Device Address Book.
  - Add scan destinations to address book contacts.

  For details, refer to Address Books.
- For scanning to an email address, refer to Scanning to an Email Address.
- For scanning to a USB Flash drive, refer to Scan to USB.
- For scanning to an SMB shared folder, refer to SMB.

Configuring Default Scan Settings

Use the Scan To Setup page in the Embedded Web Server to configure default scan settings. For the Required Settings and General tabs, Scan To shares settings with the Email App. The settings on the Defaults tab apply to the Scan To App only.

1. In the Embedded Web Server, click **Properties > Apps**.
2. Click **Scan To > Setup**.
3. Click the **Required Settings** tab. Edit settings as needed. For details, refer to Configuring Required Settings
4. Click the **General** tab. Edit settings as needed. For details, refer to Configuring General Email Settings
5. Click the **Defaults** tab. Edit settings as needed. For details, refer to the Help in the Embedded Web Server.

Configuring Default Scan Settings for Address Books

For address book settings and policies, Scan To shares configuration settings with the Email App.

1. In the Embedded Web Server, click **Properties > Apps**.
2. Click **Scan To > Setup**.
3. Click the **Address Books** tab.
4. To configure the Address Book settings stored in the device, for Device Address Book, click **Edit**.
5. To use a Network Address book, configure LDAP server settings, for Network Address Book, click **Edit**.
6. If you configured Device Address Book settings, for Use Device Address Book, select an option.
   - To allow users to access the address book, select **Yes**. To show Favorites as the initial view upon entering the address book, select **View Favorites on App Entry**.
   - To restrict users from accessing the address book, select **No**.
7. If you configured Network Address Book settings, for Use Network Address Book, select an option.
   - To allow users to access this address book, select **Yes**.
   - To restrict users from accessing the address book, select **No**.
8. To reset the device to factory settings, click **Apply Factory Settings**.
9. Click **Apply**.

Configuring Default Scan Settings for Security

For security settings and policies, the Scan To feature shares some configuration settings with the Email App.

1. In the Embedded Web Server, click **Properties > Apps**.
2. Click **Scan To > Setup**.
3. Click the **Security** tab.
4. To configure security settings, for Scan To Destination, click **Edit**.
5. To edit encryption and signing settings, for Encryption / Signing, click **Edit**. For details, refer to Configuring Email Encryption Settings and Configuring Email Signing Settings.
6. To edit domain filter and email filter settings, for Network Policies, click **Edit**. For details, refer to Editing Domain and Email Filter Settings.
7. To edit user security policies, for User Policies, click **Edit**. For details, refer to Editing User Policy Settings.
8. To allow walk-up users to view all available SMB Share Locations, in the SMB Browsing Enablement area, for Browse to SMB share locations, select **Enabled**.
9. To allow scanning to FTP and SFTP directories, for FTP / SFTP Enablement, select the check boxes for each feature that you want to enable.
   - For Allow scanning to FTP directories, click **Enabled**.
   - For Allow scanning to SFTP directories, click **Enabled**.
10. Click **Save**.

Configuring the Printer for the Xerox® Scan Utility

The Xerox® Scan Utility allows you to scan directly to your computer and helps you manage and distribute scanned image files. Before you can scan, create a workflow in the utility. The workflow is saved on the device. The Xerox® Scan Utility installs when you install scan drivers.

Note:

- Before scanning using the Xerox® Scan Utility, ensure that Secure HTTP (SSL) is enabled and a certificate is installed on the device.
- Ensure that SMB is enabled on your computer. SMB is not enabled by default on Macintosh® computers.
- You cannot delete workflows created in the Xerox® Scan Utility from the device control panel or from the Embedded Web Server. Workflows must be deleted in the Xerox® Scan Utility by the user who created them.
- The Xerox® Scan Utility is available for Macintosh® computers only.

8

Faxing

This chapter contains:

Fax Overview

You can send a fax in one of four ways:

- **Fax**, or embedded fax, scans the document and sends it directly to a fax machine.
- **Server Fax** scans the document and sends it to a fax server, which transmits the document to a fax machine.
- **Internet Fax** scans the document and emails it to a recipient.
- **LAN Fax** sends the current print job as a fax. For details, see the print driver software.

Note: Not all options listed are supported on all printers. Some options apply only to a specific printer model, configuration, operating system, or print driver type. For details, contact your Xerox representative.

Fax

When you send a fax from the printer control panel, the document is scanned and transmitted to a fax machine using a dedicated telephone line. To use the embedded fax feature, ensure that your printer has access to a functioning telephone line with a telephone number assigned to it.

Note:

- Not all printer models can send faxes. Some printers require an optional fax hardware kit.
- Not all printer models have multiple fax lines.

Configuring Required Fax Settings at the Control Panel

Before you can send a fax at the control panel:

- Set the fax country.
- Configure the embedded fax settings.

Setting the Fax Country at the Control Panel

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **App Settings > Fax App > Fax Country Setting**.
3. Select your country from the list.
4. Touch **OK**.

Configuring Embedded Fax Settings

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **App Settings > Fax App**.
3. Touch **Line 1 Setup** or **Line 2 Setup**.
4. Touch **Fax Number**, use the touch screen keypad to type the fax number, then touch **OK**.
5. Touch **Line Name**, use the touch screen keypad to type a Line Name for the printer, then touch **OK**.
6. For Options, select fax send and receive options.
7. If allowed, for Dial Type, select your dialing method. If you have a tone line, select **Tone**. If you have a 10-pulse-per-second line, select **Pulse**. If in doubt, touch **Tone**.
8. Touch **OK**.

   Note:

   - At least one fax line must be configured.
   - Most countries use tone dialing.
   - The Pulse/Tone feature is not available in some countries.

Fax Security

When the Fax Secure Receive feature is enabled, users must type a fax passcode to release a fax. Fax passcodes are also used to secure fax mailboxes. You can specify the required fax passcode length.

Note:

- Existing passcodes are not changed.
- If you edit an existing passcode after changing the passcode length requirement, the new password must meet the current length requirement.

Configuring Fax Passcode Length

1. In the Embedded Web Server, click **Properties > Apps > Fax > Setup > Security**.
2. To configure fax passcode options, for Fax Passcode Length, click **Edit**.
3. To set the passcode length, use the Plus (**+**) and Minus (**-**) buttons.
4. Click **Save**.

Configuring Fax Passcode Length at the Control Panel

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **App Settings > Fax App**.
3. Touch **Fax Passcode Length**.
4. To set the passcode length, touch the arrows.
5. Touch **OK**.

Setting Fax Defaults

Setting Ring Volume

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **App Settings > Fax App > Fax Volume**.
3. For Incoming Ring Volume, touch the desired selection.
4. For Outgoing Ring Volume, touch the desired selection.
5. Touch **OK**.

Setting Incoming Fax Defaults

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **App Settings > Fax App**.
3. To open the Incoming Fax Defaults window, touch **Incoming Fax Defaults**.

Enabling Auto Answer Delay

1. On the Incoming Fax Defaults window, touch **Automatic Answer Delay**.

2. To set the answer delay, touch the arrows.
3. Touch **OK**.

Selecting Default Paper Settings

1. On the Incoming Fax Defaults window, touch **Paper Settings**.
2. To direct the printer to print faxes on the paper size that most closely matches the attributes of the incoming fax, touch **Automatic**. If the exact paper size is not available, the printer prints to the next best match and scales the fax to fit if needed.
3. To specify exact paper attributes for incoming faxes, touch **Manual**. If the specified paper size is not available, incoming faxes are held until resources are available.
4. Touch **OK**.

Enabling or Disabling the Secure Fax Feature

To secure fax transmissions, enable the Secure Fax feature.

When Secure Fax is enabled, a password is required before a fax can be printed or deleted.

1. On the Incoming Fax Defaults screen, touch **Secure Receive Settings**.
2. For Secure Receive, to turn on Secure Receive, touch **Passcode Protect**.

   Note: The default password is **1111**.

3. To change the passcode, use the touch screen keypad to type the new passcode.
4. To allow guest users to turn on or off this feature, under Permission Policy, touch **Allow User to Manage**.

   Note: Guest users cannot change the passcode.

5. Touch **OK**.

Setting Default Output Options at the Control Panel

1. On the Incoming Fax Defaults screen, touch **Default Output Options**.
2. To staple documents, for staple, touch **Enable**.
3. To punch holes in documents, for Hole Punch, touch **Enable**.
4. To set faxes to print on both sides of the page, for 2-Sided, touch **Enable**.
5. Touch **OK**.

   Note: Not all options listed are supported on all printers. Some options apply only to a specific printer model, configuration, operating system, or print driver type. Some options are available only if a finisher is installed.

Disabling Advanced Capabilities

If your printer is not communicating successfully with older fax machines, disable the advanced document transmission speed and resolution capabilities.

1. On the Incoming Fax Defaults screen, touch **Advanced Capabilities**.
2. Touch **Disable**.

3. Touch **OK**.

Setting Outgoing Fax Defaults

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **App Settings > Fax App**.
3. Touch **Outgoing Fax Defaults**.

Setting Automatic Redial

1. On the Outgoing Fax Defaults screen, touch **Automatic Redial Setup**.
2. Use the arrows to set:
   - **Redial Time Interval**: This option sets the time interval before the fax system redials after a failed transmission. The range is 1–25 minutes.
   - **Automatic Redial Attempts**: This option sets the number of attempts the fax system makes before it rejects the job. The range is 0–14.
3. Touch **OK**.

Send Header Text

1. On the Outgoing Fax Defaults screen, touch **Send Header Text**.
2. To type up to 30 characters of text to include in the header for the fax, use the touch-screen keyboard.
3. Touch **OK**.

Automatic Resend

1. On the Outgoing Fax Defaults screen, touch **Automatic Resend**.
2. To set the number of resend attempts the printer makes, for Set Number of Resends, touch the arrows, then select a number between **0–5**.
3. From the list of options, select the condition that prompts the printer to resend jobs automatically.
4. Touch **OK**.

Batch Send

The Batch Send feature allows you to send multiple fax jobs to a single destination during a single fax transmission session. This feature reduces the connection time and cost of call connection that occurs when the faxes are sent independently.

1. On the Outgoing Fax Defaults screen, touch **Batch Send**.
2. To enable Batch Send, touch **Enabled**.
3. Touch **OK**.

Setting Fax Feature Defaults

The printer uses the default fax feature settings on all embedded fax jobs unless you change them for an individual job. You can modify the default fax feature settings.

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **App Settings > Fax App**.
3. Touch **Feature Defaults**.
4. Edit settings for size, resolution, image quality, layout, fax options, and job assembly, as needed.
5. Touch **Done**.

Fax Forwarding

You can configure the printer to forward incoming faxes to email or file destinations by creating a Fax Forward Rule. For different situations, you can configure up to five rules, and apply them to the available fax lines.

Note: After you configure the fax forwarding rule, apply the rule to a fax line.

Editing a Fax Forwarding Rule

1. In the Embedded Web Server, click **Properties > Apps > Fax > Setup > Forwarding**.
2. For the desired rule, click **Edit**.
3. To base the new rule on an existing rule, for Based on Rule, from the list, select a rule.
4. For Rule Name, type a name for the rule.
5. For File Format Type, from the list, select an option.
6. For Print Local Copy, select an option:
   - To print all incoming faxes, select **Always**.
   - To print a copy only if the forwarded fax transmission fails, select **On Error Only**.
7. Add an email address or file destination to the rule.
8. Click **Save**.

Adding Email Addresses to the Rule

1. On the Forwarding page, next to the desired rule, click **Edit**.
2. To forward to an email address, select **Email**.
3. In the Address fields, type the email addresses of the recipients.
4. Type the From Address, From Name, and Subject.
5. To customize the name of the attachment, click **Customize**.
   a. Under Display, select the check boxes next to Date or Time to add the date or time to the file name.
   b. To customize the file name, type the new name in Custom Text, then click **Add**.
   c. Under Position, select an item, and click the arrows to arrange the items as you want them to appear in the file name.
   d. Click **Save**.
6. Type the Message text for the body of the email.
7. Type the Signature text for the email message.

8. Click **Save**.

Adding File Destinations to the Rule

1. On the Forwarding page, next to the desired rule, click **Edit**.
2. To forward to a file location, select **SMB Protocol**.
3. Select **IPv4 Address** or **Host Name**, then type the address or host name.
4. Type the following information:
   a. In the Share field, type the share name.
   b. In the Document Path field, type the directory path of the folder.
   c. Type a Login Name for the printer to use to access the shared folder.
   d. Enter the computer login password for the printer to use to access the shared folder, then confirm it.
5. To update an existing password, type the new password, then click **Select**.
6. To customize the name of the file, click **Customize**.
   a. Under Display, select the check boxes next to Date or Time to add the date or time to the file name.
   b. To customize the file name, type the new name in Custom Text, then click **Add**.
   c. Under Position, select an item, and click the arrows to arrange the items as you want them to appear in the file name.
7. To receive email notifications of forwarded faxes, select Email Notification, then enter your email address.
8. To send an email confirmation when file transfer is complete, select **Email Notification (without Attachment)**, and type the email address in the Notification Address field.
9. Click **Save**.

Applying a Fax Forwarding Rule

1. In the Embedded Web Server, click **Properties > Apps > Fax > Setup > Forwarding**.
2. For the desired rule, click **Edit**.
3. To apply a rule, select **Apply to Fax Line 1** or **Apply to Fax Line 2**.
4. Click **Apply**.

Disabling Fax Forwarding

1. In the Embedded Web Server, click **Properties > Apps > Fax > Setup > Forwarding**.
2. To disable fax forwarding for a line, for No Fax Forwarding, select **Apply to Fax Line 1** or **Apply to Fax Line 2**.
3. Click **Apply**.

Fax Mailboxes

You can store faxes locally in the printer or on a remote fax machine. You can use Remote Polling to print or access a stored fax. There are 200 available fax mailboxes.

Editing a Fax Mailbox

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **App Settings > Fax App**.
3. Touch **Mailbox Setup**.
4. From the list, touch a mailbox.
   - To edit a mailbox name, touch **Friendly Name**. Use the touch screen keypad to type a name for the mailbox up to 30 characters, then touch **OK**.
   - To assign a passcode to the mailbox, touch **Passcode & Notification**, then touch **Passcode Protect**. To type a 4-digit passcode, use the numeric keypad, then touch **OK**.

     Note: The passcode is required when users store faxes to the mailbox or print faxes from the mailbox.

   - To notify users of mailbox status changes, touch **Passcode & Notification**, then for Mailbox Notification, touch **Enabled**.
   - To reset and delete mailbox contents, touch **Reset Mailbox & Cont**, then touch **Reset**.
   - To print mailbox content, touch **Print Mailbox List**.
5. Touch **Close**.

Deleting a Fax Mailbox

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **App Settings > Fax App**.
3. Touch **Mailbox Setup**.
4. Touch the assigned mailbox that you want to delete, then touch **Reset Mailbox & Contents**.

   Caution: If you touch **Reset Mailbox**, the mailbox and all documents that it contains are deleted permanently.

5. At the Delete Mailbox confirmation prompt, to delete the mailbox, touch **Reset**, or to exit, touch **Cancel**.
6. Touch **Close**.

Fax Reports

You can configure three different reports:

- Activity Report
- Confirmation Report
- Broadcast and Multipoll Report

Setting Up Fax Reports

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **App Settings > Fax App**.
3. Touch **Setup Fax Reports**.
4. Touch **Fax Activity Report**, then touch an option:
   - To print an activity report that shows all fax transactions, select **Auto Print**.
   - To disable printing activity reports, select **Off**.
5. Touch **OK**.
6. Touch **Confirmation Report**, then for Report Options, touch an option:
   - To print a confirmation report only when a fax transmission error occurs, select **Print On Error**.
   - To print a confirmation report when a user sends a fax, select **Always Print**.
   - To disable printing a confirmation report when a user sends a fax, select **Off**.
7. For Print Options, touch a thumbnail printing option:
   - To print a smaller thumbnail image of the first page of the fax on the confirmation report, select **Reduced Image**.
   - To print a larger thumbnail image of the first page of the fax on the confirmation report, select **Cropped Image**.
   - To disable printing thumbnail images of the first page of the fax on the confirmation report, select **No Image**.
8. Touch **OK**.
9. Touch **Broadcast & Multipoll Report**, then touch an option:
   - To print a confirmation report only when a fax transmission error occurs, select **Print On Error**.
   - To print a confirmation report every time a user sends a fax, select **Always Print**.
   - To disable printing confirmation reports when a user sends a fax, select **Off**.
10. Touch **OK**.
11. Touch **Close**.

Printing a Fax Report

You can print the following fax reports from the printer control panel:

- Activity Report
- Protocol Report
- Fax Address Book Report
- Options Report
- Pending Jobs Report

To print a fax report:

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **App Settings > Fax App**.
3. Touch **Print Fax Reports**.
4. Touch the desired report, then touch **Print**.
5. Touch **Close**.

Deleting Sent Fax Jobs from Memory

1. At the control panel touch screen, touch **Jobs**.
2. Touch the Down arrow, then touch **Scan and Fax Sent Jobs**.
3. Touch the pending fax in the list.
4. Touch **Delete**.

Server Fax

Server fax allows you to send a fax over a network to a fax server. The fax server then sends the fax to a fax machine over a phone line.

Before you can send a server fax, configure a fax filing repository, or filing location. The fax server retrieves the documents from the filing location and transmits them over the telephone network. You can also print a transmission report.

Note: Not all printer models support this feature.

Configuring a Server Fax Filing Repository

Before you can send a server fax, configure fax repository settings. Once configured, the printer transfers faxed images to the repository. The fax server then sends the fax to its destination over the phone line.

You can set up a repository that uses one of the following protocols:

- FTP
- SFTP
- SMB
- HTTP/HTTPS: A Web server using a CGI script.
- SMTP: A mail server.
- NetWare

Configuring a Fax Repository Using FTP or SFTP

Before you begin:

- Ensure that FTP or SFTP services are running on the server or computer where images faxed by the printer are stored. Note the IP address or host name.
- Create a user account and password for the printer. When the server fax feature is used, the printer logs in using the account, transfers the file to the server or computer and logs out. Note the user account and password.
- Create a directory within the FTP or SFTP root to be used as a fax repository. Note the directory path.

To configure a fax repository using FTP or SFTP:

1. In the Embedded Web Server, click **Properties > Apps**.
2. Click **Server Fax > Fax Repository Setup**.

3. Select the address type. Options for FTP include **IPv4**, **IPv6**, or **Host Name**. Options for SFTP include **IPv4**, or **Host Name**.
4. In the Repository Server field, type the appropriately formatted address and port number for the FTP or SFTP location.
5. In the Document Path field, type the directory path of the folder, beginning at the root of FTP or SFTP services. For example, //directoryname/foldername.
6. Under Login Credentials to Access the Destination, select an option.
   - **Authenticated User and Domain**: This option instructs the device to use the user name and domain of the logged-in user when it accesses the repository.
   - **Logged-in User**: This option instructs the device to log in to the repository using the credentials of the logged-in user.
   - **Device**: This option instructs the device to use specific credentials when accessing the repository. If you select Device, type the credentials in the User Name and Password fields. To update an existing password, select **Select to save new password**.
7. Click **Apply**.

Configuring a Fax Repository Using SMB

Before you begin:

- Create a shared folder to be used as a fax repository. Note the share name of the folder and the computer name or server name.
- Create a user account and password for the printer with full access rights to the fax repository. Note the user account and password.

To configure a fax repository using SMB:

1. In the Embedded Web Server, click **Properties > Apps**.
2. Click **Server Fax > Fax Repository Setup**.
3. From the Protocol menu, select **SMB**.
4. Select the address type. Options are **IPv4** or **Host Name**.
5. Type the appropriately formatted address in the Repository Server field for the server where the file repository is located.
6. In the Share field, type the share name.
7. In the Document Path field, type the directory path of the folder starting at the root of the shared folder. For example, if you have a folder named scans in the shared folder, type **/scans**.
8. Under Login Credentials to Access the Destination, select an option.
   - **Authenticated User and Domain**: This option instructs the device to use the user name and domain of the logged-in user when it accesses the repository.
   - **Logged-in User**: This option instructs the device to log in to the repository using the credentials of the logged-in user.
   - **System**: This option instructs the device to use specific credentials when accessing the repository. If you select System, type the credentials in the User Name and Password fields. To update an existing password, select **Select to save new password**.
9. Click **Apply**.

Configuring a Fax Repository Using HTTP/HTTPS

Before you begin:

- Ensure that Web services are installed on the server where you want to store scanned images. Examples of Web servers include Microsoft Internet Information Services (IIS) and Apache. Note the IP address or host name of the server.
- For HTTPS, ensure that your Web server is installed with a secure certificate.
- Create a user account and password for the printer. When a document is scanned, the printer logs in using the account, transfers the file to the server or workstation and logs out. Note the user account and password details.
- Create a directory on the HTTP/HTTPS server to use as a scan filing location. Note the directory path.
- Note any script that is required to be run.

To configure a fax repository using HTTP/HTTPS:

1. In the Embedded Web Server, click **Properties > Apps**.
2. Click **Server Fax > Fax Repository Setup**.
3. From the Protocol menu, select **HTTP** or **HTTPS**.
4. Select the address type. Options are **IPv4 Address**, **IPv6 Address**, or **Host Name**.
5. Type the appropriately formatted address and port number of your server.
6. To verify that a digital certificate is installed on the printer, for HTTPS, click **View Trusted SSL Certificates**.
7. To validate the SSL certificate used for HTTPS, select **Validate Repository SSL Certificate**.
8. In the Script path and filename field, type the path to the CGI script starting at the root. For example, //directoryname/foldername.
9. In the Document Path field, type the directory path of the folder.
10. Under Login Credentials to Access the Destination, select an option.
    - **Authenticated User and Domain**: This option instructs the device to use the user name and domain of the logged-in user when it accesses the repository.
    - **Logged-in User**: This option instructs the device to log in to the repository using the credentials of the logged-in user.
    - **System**: This option instructs the device to use specific credentials when it accesses the repository. If you select System, type the credentials in the User Name and Password fields. To update an existing password, select **Select to save new password**.
    - **None**: This option instructs the device to access the repository without providing credentials.
11. Click **Apply**.

Configuring a Fax Repository Using SMTP

1. In the Embedded Web Server, click **Properties > Apps**.
2. Click **Server Fax > Fax Repository Setup**.
3. For Protocol, select **SMTP**.
4. In the Domain Name field, type the domain name of your SMTP server.

5. In the Default "From:" Address field, type the address you want to display automatically on the fax.
6. For Enable Email Security, select **Enable**.
7. To save the settings, click **Apply**. To retain the previous settings, click **Undo**.

Configuring Server Fax General Settings

1. In the Embedded Web Server, click **Properties > Apps**.
2. Click **Server Fax > Defaults and Policies**.
3. For General, click **Edit**.
4. For Save Job Log in Repository, select the options to include on the Job Log. The device adds the selected fields to the job log saved on the server.
5. For Confirmation Sheet, select an option.
   - **Errors Only**: This option instructs the device to print a confirmation sheet only when a transmission error occurs. The confirmation sheet lists error information and indicates that the job has reached the SMTP server. The confirmation sheet does not indicate that the email message was delivered.
   - **On**: This option instructs the device to print a confirmation sheet after every server fax job. The confirmation sheet specifies the success or failure of the server fax job. If the fax is successful, the location of the document on the fax server is also specified.
   - **Off**: This option instructs the device not to print a confirmation sheet.
6. Click **Save**.

Configuring Server Fax Settings

1. In the Embedded Web Server, click **Properties > Apps**.
2. Click **Server Fax > Defaults and Policies**.
3. For Server Fax, click **Edit**.
4. Select options as needed.
5. Click **Save**.

Configuring Server Fax Image-Quality Settings

1. In the Embedded Web Server, click **Properties > Apps**.
2. Click **Server Fax > Defaults and Policies**.
3. For Image Quality, click **Edit**.
4. Select options as needed.
5. Click **Save**.

Configuring Layout Adjustment Settings

1. In the Embedded Web Server, click **Properties > Apps**.
2. Click **Server Fax > Defaults and Policies**.
3. For Layout Adjustment, click **Edit**.
4. Select options as needed.

5. Click **Save**.

Configuring Server Fax Filing Options

1. In the Embedded Web Server, click **Properties > Apps**.
2. Click **Server Fax > Defaults and Policies**.
3. For Filing Options, click **Edit**.
4. Select options as needed.
5. Click **Save**.

Internet Fax

Internet fax allows you to scan documents at the control panel, send them to destination email addresses, or receive and print emails with attachments. You can also print a transmission report. A telephone line connection is not required.

Accessing the Internet Fax Setup Page

1. In the Embedded Web Server, click **Properties > Apps**.
2. Click **Internet Fax > Setup**.

Configuring Required Settings

1. On the Internet Fax Setup page, click the **Required Settings** tab.
2. To configure SMTP settings, next to SMTP, click **Edit**. For details, refer to SMTP.
3. To configure POP3 settings, next to POP3, click **Edit**. For details, refer to POP3.

Configuring General Internet Fax Settings

1. On the Internet Fax Setup page, click the **General** tab.
2. To print a report after all recipients receive the fax, next to acknowledgment report, select **Print Report**.

   Note: The report can be delayed depending on the response time of the recipient.

3. To print an activity report after 50 jobs have been processed, next to Activity Report, select **Enable**. An activity report lists Internet fax jobs and the current delivery status of each job. To print an activity report, click **Print Activity Report**.
4. To set the time that the printer waits for a delivery confirmation from recipients, type the time in hours next to Delivery Confirmation Timeout.
5. For Subject, type the text that you want to appear in the subject line of emails sent from the printer.
6. Next to Message body, type the text that you want to appear in the body of emails.
7. To include the user name or email address in the body of emails, under User, select **User Name** or **Email Address**.
8. To include attachment information in the message body, select **Number of Images**, or **Attachment File Type**.
9. To include information about the printer in the body, under Multifunction Device System, select the information that you want to include.
10. Next to Signature, type the information that appears at the end of the email message.

11. Next to Confirmation Sheet, select an option:
    - **Errors Only** instructs the printer to print a confirmation sheet only when a transmission error occurs. The confirmation sheet lists error information and indicates that the job has reached the SMTP server. The confirmation sheet does not indicate that the email message was delivered.
    - **On** instructs the printer to print a confirmation sheet.
    - **Off** instructs the printer not to print a confirmation sheet. You can find status about a job in the job log. To see the job log, at the control panel, press **Job Status > Completed Jobs**.
12. Click **Apply**.

Configuring Internet Fax Receive Settings

1. On the Internet Fax Setup page, click the **Receive Settings** tab.
2. To print email messages without attachments, on the Receive Settings Tab, under Filter Options, select **Accept Email with no attachment**.
3. Under Accept the following attachments, select what types of attachments can be received.
4. Under Finishing Options, click the drop-down menu and select the desired settings for **Stapling** and **2-Sided Printing**.
5. To send a Mail Delivery Notification (MDN) email to the requester when the fax job completes, under Receipt Options, select **Send confirmation reply when requested**.
6. To print a cover sheet containing the email message of the requester before printing the fax job, select **Print cover sheet with incoming Email messages**.
7. Click **Apply**.

Configuring Address Book Settings

1. On the Internet Fax Setup page, click the **Address Books** tab.
2. To configure the Address Book settings stored in the printer, on the Address Books tab, next to Device Address Book, under Action, click **Edit**.
3. To use a Network Address book, configure LDAP server settings. Next to Network Address Book (LDAP), under Action, click **Edit**.
4. If you configured Address Book settings stored in the printer, under Policies, Use Device Address Book, to allow users to access the book, select **Yes**. To restrict users from accessing the address book, select **No**.
5. If you configured a Network Address Book, under Policies, under Use Network Address Book (LDAP) to allow users to access this address book, select **Yes**. To restrict users from accessing the address book, select **No**.
6. To set the default address book that users see at the control panel, under Default Address Book View, select an address book.
7. To allow users to create or edit contacts in the Device Address Book from the printer control panel, select **All Users**.

8. Click **Apply**.

   Note: If the Network Address Book does not appear, on the LDAP Server configuration page, ensure that Internet fax is not set to No Mappings Available. This setting prevents the Network Address Book from displaying on the Internet fax page. If your LDAP server does not contain a unique Internet fax address field, it can be set to match the heading for email address.

Configuring Default Internet Fax Settings

1. On the Internet Fax Setup page, click the **Defaults** tab.
2. To edit default Internet fax settings, for Internet Fax, click **Edit**.
3. To edit default Image Options, Image Enhancement, Resolution, and Quality/File Size settings, for Advanced Settings, click **Edit**.
4. To edit default Original Orientation, and Original Size settings, for Layout Adjustment, click **Edit**.
5. To edit default File Format and Filename Extension settings, for Internet Fax Options, click **Edit**.

   Note: For details, refer to the Help in the Embedded Web Server.

Setting File Compression Options

1. On the Internet Fax Setup page, click the **Compression** tab.
2. Select TIFF and PDF settings as needed. For details, refer to the Help in the Embedded Web Server.
3. Click **Save**.

Editing Internet Fax Network Policies

1. On the Internet Fax Setup page, click the **Security** tab.
2. To set the user policies for Internet fax, next to Access Control for Internet Fax Service, click **Edit**.
3. To set domain filter and email filter settings, under Network Policies, click **Edit**.
4. To enable a domain filter list, under Domain Filter settings, select **Allow Domains** or **Block Domains**.
5. Under New Domain, type the domain you want to add to the list and click **Add**.
6. To remove a domain from the list, select a domain, and click **Remove**.
7. To allow LDAP email address searches without the @ symbol, under **Allow LDAP Email Address without the @ Requirement**, select **On**.

   Note: If you select **On** under **Allow LDAP Email Address without the @ Requirement**, the number of items returned by an LDAP search can increase.

LAN Fax

Local Area Network (LAN) Fax allows you to send faxes using the print driver on your computer to a fax machine over a telephone line.

For details about using or configuring LAN Fax, see the print driver software help.

Note: Not all printer models support this feature. Some printers require an optional fax hardware kit.

9

Accounting

This chapter contains:

Xerox® Standard Accounting

Xerox® Standard Accounting tracks the numbers of copy, print, scan, and fax jobs for each user. You can set limits to restrict the total number of jobs by type that a user can produce. You can generate reports that list usage data for individual users and groups. When Xerox® Standard Accounting is enabled, users are required to enter an accounting code to access the apps. Before users can print documents from their computer, they must enter an accounting code in the print driver.

Note:

- You can create a maximum of 2497 unique user IDs, 500 General Accounts, and 498 Group Accounts.
- All user IDs must be assigned to one or more group accounts.
- Xerox® Standard Accounting settings and account data are stored in the printer.
- Xerox recommends that you use the Cloning feature to back up settings. If Xerox® Standard Accounting settings are lost or deleted, you can restore them using the cloning backup file.

Enabling Xerox Standard Accounting

1. In the Embedded Web Server, click **Properties > Login/Permissions/Accounting > Accounting Methods**.
2. For Control Panel & Website Login Methods, click **Edit**.
3. For Current Accounting Method, select **Xerox Standard Accounting**.
4. Click **Save**.

Setting Service Tracking Options

1. On the Accounting page, in the Action section, for Service Tracking, click **Edit**.
2. For Presets, select an option:
   - **Disable tracking for all services**:This option instructs the device not to track Copies, Prints, Scans, and Faxes.
   - **Enable tracking for all services**: This option instructs the device to track Copies, Prints, Scans, and Faxes.
   - **Enable color tracking only**: This option instructs the device to track color Copies and Prints.
   - **Custom**: This option allows you to enable tracking for specific apps. If you select Custom, select **Enabled** or **Color Tracking Only**. for the apps you want to track.

   Note: Not all options listed are supported on all devices. Some options apply only to a specific device model, configuration, operating system, or driver type.
3. Click **Save**.

General and Group Accounts

You can create a group account to track and limit the number of copies, prints, scans, and faxes for a group of users. The number of copies, prints, scans, and faxes of each user are tracked against the user account and the group account. You can limit the usage for each user.

You can create a general account to track the total usage for a group of users. The number of copies, prints, scans, and faxes of each user are not tracked against the user account. The usage is tracked against the general account only. You cannot specify usage limits for a general account.

If a user is associated with a group account and a general account, they can access the printer using the accounting code for either account. Individual copies, prints, scans, and faxes, are tracked against the user and group accounts if the user accesses the printer using the group account. If the user accesses the printer using a general account, the usage is tracked against the general account only and not the user account.

Creating an Account

1. In the Embedded Web Server, click **Properties** > **Login/Permissions/Accounting** > **Accounting Methods**.
2. In the Configuration Settings area, for Group & General Accounts, click **Edit**.
3. Click the **Group Accounts** tab or the **General Accounts** tab.
4. For Add New Group Account, type a unique Account ID number. Type a unique Account Name for the new group.
5. Click **Add Account**.

Editing, Viewing, or Deleting an Account

1. In the Embedded Web Server, click **Properties** > **Login/Permissions/Accounting** > **Accounting Methods**.
2. In the Configuration Settings area, for Group & General Accounts, click **Edit**.
3. On the Group & General Accounts page, click **Group Accounts** or **General Accounts**.
4. To edit the account name, or assign users to an account, under Actions, click **Edit**.
   - To assign users to the account, select the check box next to a user ID.
   - To edit the Account Name, under Account Name, type a new name.
   - Click **Save**.
5. To view usage details for an account, under Actions, click **View Usage**.
6. To delete an account, in the table at the bottom of the page, select the check box next to the account and click **Delete Selected**.

Adding a User and Setting Usage Limits

Before you can associate users with an accounting group, add or import user information to the user database. To edit the user database, see Configuring Authentication Settings.

To add a user and set usage limits for the user:

1. On the Accounting Methods page, in the Configuration Settings area, for Users and Limits, click **Edit**.
2. Click **Add New User**.
3. For Display Name, type a name for the user. This name is associated with the user in the user database.

4. For User Name, type a unique user name for the new user. To log in at the control panel, the user types this name.
5. Set limits for the user in the Usage Limits area:
   - Color Impressions, in the User Limits field, type the maximum number of impressions or sent images allowed for Prints or Copies.
   - For Black Impressions, in the User Limits field, type the maximum number of impressions or sent images allowed for Prints or Copies.
   - For Scanned Images, in the User Limits field, type the maximum number of impressions or sent images allowed for Scans.
   - For Fax Images, in the User Limits field, type the maximum number of impressions or sent images allowed for Sent or Black Faxed Impressions.

   Note: Not all options listed are supported on all devices. Some options apply only to a specific device model, configuration, operating system, or driver type.
6. Click **Apply**.

Managing User Information

You can import or export user information and accounting data as a **.csv** file. For details, refer to the Embedded Web Server help.

Importing User Information

Setting Up File Importing

1. On the Accounting Methods page, for Users & Limits, click **Edit**.
2. From the Management Actions menu, select **Import**.
3. For File, click **Browse** or **Choose File**, select your .csv file, then click **Open** or **Choose**.
4. For Delimiting Character, select an option.
5. For Language, select the language of the text in your .csv file.
6. For When importing your File, select an option:
   - **Append to existing**: This option adds user information from the .csv file to the existing user information stored in the database.
   - **Overwrite existing data**: This option replaces all user information in the database with user information from your .csv file.
7. Click **Next**.
8. Continue to Editing the Fields for Importing.

Editing the Fields for Importing

1. In the Required Fields area, for Imported Heading, select the column heading from your .csv file containing information for User Name and Display Name.
   - To build User Name and Display Name from First Name and Last Name, for First Name and Last Name, select a column heading.
   - For User Name and Display Name, select **Build from First and Last Name**.

2. If you created your .csv file by exporting from a non-Xerox® device, the .csv file format can contain unwanted characters. To remove unwanted characters from all fields, select **Remove Unwanted Characters**.

   - For Leading Characters, Body Characters, and Trailing Characters, select an option.

   - If you selected Custom String, type the string of characters that you want to remove from each field.

3. For Limits, select an option:
   - **Quick Setup for All Users**: This option allows you to set a default limit for all services for all users. For Default for All Services, type the limit.
   - **Manual Setup for All Users**: This option allows you to set the limit for each service and impression type. For User Limits, type the limit.
   - **Import Existing Limits from File**: This option allows you to import limits from your .csv file. For Imported heading, for the limit for each service and impression type, select the column heading from your .csv file.

   Note: Limits must be in the range of 0–16,000,000. If you do not assign a limit, the limit is set to 16,000,000.

4. Continue to Setting Up Account Permissions.

Setting Up Account Permissions

1. For Accounts, under Group Accounts, select the default group to which you want to add imported users:
   - **Use System Default**: This option adds all users to the current system default group.
   - **Assign New Account**: This option allows you to create an account and add all users to the account. Under Group Account ID, type a unique Account ID number. Type a unique Account Name for the new group. Select **Make this the new system default group** account as needed.
   - **Import Existing Accounts from File**: This option allows you to import accounts from your .csv file. For Imported heading, for the Group Account ID and Group Account Name, select the column heading from your .csv file.

   Note:

   - Combine Account ID and Account Name in a single column. Use a colon (:) to separate Account Name and Account ID. For example, **123:account_A**.

   - You can associate a user with multiple accounts. Separate the account names using a number (**#**) symbol. For example, **111:account_A#222:account_B**. The first account is the default user account. To associate a user with multiple accounts, but use the default system account, type the **#** symbol, then type the account names. For example, **#222: account_B**.

2. For General Accounts, select an option:
   - **No General Accounts**: This option does not add users to a General Account.
   - **Import Existing Accounts from File**: This option allows you to import accounts from your .csv file. For Imported heading, for the General Account ID and General Account Name, select the column heading from your .csv file.

   Note:

   - Combine Account ID and Account Name in a single column. Use a colon (**:**) to separate Account Name and Account ID. For example, **123:account_A**.
   - You can associate a user with multiple accounts. Separate the account names using a number (**#**) symbol. For example, **111:account_A#222:account_B**.
3. Click **Import**.

Downloading a Sample File

You can download a sample file to see how to format your **.csv** file for import.

1. On the Accounting page, next to Users and Limits, click **Edit**.
2. From the Management Actions menu, select **Download Sample**.
3. Under Delimiting Character, select an option.
4. Under Language, select the language of the text in your **.csv** file.
5. Click **Generate**.

Exporting User Information

1. On the Accounting page, next to Users and Limits, click **Edit**.
2. From the Management Actions menu, select **Export**.
3. Under Delimiting Character, select an option.
4. Under Language, select the language of the text in your **.csv** file.
5. Click **Export**.

Assigning Users to an Account

1. On the Accounting page, next to Users and Limits, click **Edit**.
2. Select the check box next to the User ID of the user that you want to add to an account.
3. Under Action, click **Access, Limits, & Accounts**.
4. Click the **Group Accounts** tab or the **General Accounts** tab.
5. Select the check box next to the User ID of the user that you want to add to an account.
6. Click **Apply**.

Usage Limits

When users reach their maximum usage limit, they can no longer use that feature until the administrator resets their limit. When they log in to the printer, they are presented with a notification message that indicates that their limit has been reached for that feature.

Any impressions made after users reach their limit are subtracted from their limit after it is reset. If the user limit is reached before a print job completes, an error report prints that notifies the user that their limit has been reached. The job is deleted from the print queue, and any sheets remaining in the paper path finish printing.

Note:

- The maximum number of impressions or images sent is 16,000,000.
- Cover sheets, banner pages, fax acknowledgment reports, and scan confirmation reports count as impressions.
- Color Impression Prints includes all color print jobs and received server fax documents. Color Impression Copies includes all color copies.
- Black Impression Prints includes all black and white print jobs and received server fax documents. Black Impression Copies includes all black and white copies.
- Scanned Images includes documents sent over the network, including network scans, scans to email, server faxes, and Internet faxes.
- Fax Images Sent includes faxed documents. The total number of documents is the number of faxed documents, including cover sheets, multiplied by the number of destinations. Documents sent using the server fax feature are not included.
- Black Fax Impressions includes received fax documents that are printed. Documents sent using the server fax feature are not included.
- Not all options listed are supported on all printers. Some options apply only to a specific printer model, configuration, operating system, or print driver type.

Downloading a Usage Report

The usage report lists the number of impressions recorded for each user and each account. You can download a usage report as a **.csv** file.

1. In the Embedded Web Server, click **Properties > Login / Permissions / Accounting > Accounting Methods**.
2. Click **Report and Reset**.
3. On the Usage Report tab, for Show User ID in Report, select an option.
   - To include the user ID in the report, select **Yes**.
   - To exclude the user ID from the report, select **No**.
4. Click **Download Report (.csv)**.
   The **.csv** file is downloaded to the Downloads folder.
5. Click **Close**.

Resetting Usage Limits

1. In the Embedded Web Server, click **Properties > Login/Permissions/Accounting > Accounting Methods**.
2. Click **Report and Reset > Resets**.
3. To reset all usage data to zero, click **Reset Usage Data**.
4. Click **OK**.

Configuring Validation Policies and Print Job Exceptions

You can set validation policies and configure print job exceptions for unidentified print jobs. Unidentified jobs are jobs that are not associated with a user name.

Unidentified jobs originate from a computer that does not require a user to log in. Examples are a job sent from a DOS or UNIX window using LPR, Port 9100, or from the Jobs tab in the Embedded Web Server. Unidentified print jobs can originate from IPP clients, including mobile clients that support AirPrint and Mopria.

Validating Accounting Codes

Setting The Printer To Validate The Accounting Code For All Jobs

To set the printer to validate the accounting code for all jobs:

1. In the Embedded Web Server, click **Properties > Login/Permissions/Accounting > Accounting Methods**.
2. In the Configuration Settings area, for Validation Polices / Print Job Exceptions, click **Edit**.
3. For Validate Accounting Code, select **Yes**.

   Note: When you select Yes for Validate Accounting Code and tracking is enabled for Print, unidentified jobs are deleted.
4. Click **Save**.

Configuring Validation Options For Unidentified Print Jobs

To configure validation options for unidentified print jobs:

1. In the Embedded Web Server, click **Properties > Login / Permissions / Accounting > Accounting Methods**.
2. In the Configuration Settings area, for Validation Policies / Print Job Exceptions, click **Edit**.
3. For Validate Accounting Code, select **Yes with Exceptions**.
4. To allow the device to print unidentified print jobs from any computer, for Exceptions for Jobs Not Containing an Accounting Code, select **Guest Mode**.

5. To allow IPP print jobs, for Exceptions for Jobs Not Containing an Accounting Code, select **IPP Exception Mode**. Select an option.
   - **Track IPP jobs with invalid accounting codes against the IPP Exception User and Account IDs**: Use this option to allow print jobs with invalid accounting codes from IPP sources. This configuration prevents IPP clients from rejecting jobs such as AirPrint and Mopria™.
   - **Reject IPP jobs with invalid accounting codes**: Use this option to reject print jobs with invalid accounting codes.

   Note: Some Apple iOS and OSX clients send an unalterable accounting user ID value during job submission. To allow jobs from these clients, select **Track IPP jobs with invalid accounting codes against the IPP Exception User and Account IDs**. For details, refer to the AirPrint User Guide.

6. To allow unidentified print jobs from specific sources only, for Exceptions for Jobs Not Containing an Accounting Code, select **Designated Source Mode**. The device deletes invalid unidentified print jobs.

   a. To specify the computers or other sources that are allowed to send unidentified print jobs in Designated Source Mode, click **Add Device**.

   b. Select IPv4 Address or Host Name.

   c. Type the address of the source that is allowed to send unidentified print jobs.

   d. For User ID, select the information that the printer uses for the User ID. If you selected Custom, type the User ID.

   e. Click **Save**.

7. To save the settings, click **Save**.

Network Accounting

Network Accounting tracks print, scan, fax, Internet fax, server fax, and copy jobs by User ID and Account ID and stores them in a job log. You can use this information to manage device usage and to perform detailed cost analysis. Users are prompted for accounting information when submitting jobs to the device. You can compile job log information from the accounting server and produce formatted reports.

Before you begin, complete the following items:

- Install and configure Xerox® certified network accounting software on your network. For help, refer to the manufacturer instructions.
- Test communication between the accounting server and the device. Open a Web browser, type the IP Address of the printer in the address bar, then press **Enter**. The device Embedded Web Server home page appears.
- To track print and LAN Fax jobs, install device drivers on all user computers.

Enabling Network Accounting

1. In the Embedded Web Server, click **Properties > Login/Permissions/Accounting > Accounting Methods**.
2. Click **Edit**.
3. For Current Accounting Method, select **Network Accounting**.
4. Click **Save**.

Setting Network Accounting Workflow Options

1. On the Accounting Methods page, for Accounting Workflow, click **Edit**.
2. For each Job Type, select an option from the Accounting Workflow list:
   - **Pre-Authorization and Capture Usage**: This option requires a job limits server to approve each job that a user attempts to send or print. The job limits server approves a job based on the credentials of the user and the configured job attributes.
   - **Capture Usage**: This option does not require pre-authorization and the job validation is performed only after the job is submitted.
3. Click **Save**.

Configuring Job Limits Server Settings

1. On the Accounting Methods page, for Job Limits Server (Pre-Authorization), click **Edit**.

   Note: The Job Limits Server setting is only visible when pre-authorization is selected for a job type.
2. For Server URL, type the URL of your job limits server.
3. For Timeout, type the time in seconds that the printer waits for the job limits server to respond to job approval requests before it disconnects.
4. Click **Save**.

Disabling the Job Limits Web App

If your accounting solution provider recommends disabling the Job Limits Web service, or if your job limits server only requires client-based calls, disable the service.

1. On the Accounting Methods page, for Job Limits (Web Service), click **Edit**.

   Note: The Job Limits setting is only visible when pre-authorization is selected for a job type.

2. In the Authentication and Accounting area, for Job Limits, clear the check box.
3. Click **Save**.

Configuring User Prompts

You can customize accounting prompts. An accounting prompt is the text that prompts users to enter accounting information at the control panel. You can enable up to two prompts, as your validation server requires. For example, if your company uses a unique numeric identifier for each department, you can use that number as the accounting code. Then, you can customize the prompt text to ask users for a Department ID Code, rather than a User ID or Account ID.

Note: Not all options listed are supported on all devices. Some options apply only to a specific device model, configuration, operating system, or driver type.

To customize accounting prompts:

1. On the Accounting Methods page, for User Accounting Prompts, click **Edit**.
2. To display prompt 1 or 2, for Display Prompt, select **Yes**. To hide prompts, select **No**.
3. For Label and Default Value, type the text that you want to appear at the control panel.
4. To hide text typed at the control panel, for Mask Entries, select **Yes**. Asterisks * replace any characters typed in the field.
5. For Prompt Options, select a Preset option from the list, or select **Prompt**, **No Prompt**, or **Color Prompting**for each app as needed.
6. Click **Save**.

   Note: When prompts are turned off, jobs that do not contain an accounting ID are tracked with a generic code.

Configuring Validation Policies and Print Job Exceptions

You can set validation policies and configure print job exceptions for unidentified print jobs. Unidentified jobs are jobs that are not associated with a user name.

Unidentified jobs originate from a computer that does not require a user to log in. Examples are a job sent from a DOS or UNIX window using LPR, Port 9100, or from the Jobs tab in the Embedded Web Server. Unidentified print jobs can originate from IPP clients, including mobile clients that support AirPrint and Mopria.

Validating Accounting Codes

Setting the Device to Validate the Accounting Code for All Jobs

To set the device to validate the accounting code for all jobs:

1. In the Embedded Web Server, click **Properties > Login / Permissions / Accounting > Accounting Methods**.
2. On the Accounting Methods page, for Validation Policies / Print Job Exceptions, click **Edit**.
3. For Enablement, select **Enabled**.
4. For Validate Accounting Code, select **Yes**.
5. Click **Save**.

Configuring Validation Options for Unidentified Print Jobs

To configure validation options for unidentified print jobs:

1. In the Embedded Web Server, click **Properties > Login/ Permissions/ Accounting > Accounting Methods**.
2. On the Accounting Methods page, in the Configuration Settings area, for Validation Policies / Print Job Exceptions, click **Edit**.
3. For Enablement, select **Enabled**.
4. For Validate Accounting Code, select **Yes with Exceptions**.
5. To allow the device to print unidentified print jobs from any computer, for Exceptions for Jobs Not Containing An Accounting Code, select **Guest Mode**.
6. To allow IPP print jobs, for Exceptions for Jobs Not Containing an Accounting Code, select **IPP Exception Mode**. Select an option.
   - **Track IPP jobs with invalid accounting codes against the IPP Exception User and Account IDs**: Use this option to allow print jobs with invalid accounting codes from IPP sources. This configuration prevents rejection of jobs from IPP clients such as AirPrint and Mopria.
   - **Reject IPP jobs with invalid accounting codes**: Use this option to reject print jobs with invalid accounting codes.

   Note: Some Apple iOS and OSX clients send an unalterable accounting user ID value during job submission. To allow jobs from these clients, select **Track IPP jobs with invalid accounting codes against the IPP Exception User and Account IDs**. For details, refer to the AirPrint User Guide.
7. To allow unidentified print jobs from specific sources only, for Exceptions for Jobs Not Containing an Accounting Code, select **Designated Source Mode**.

   Note: The device deletes invalid unidentified print jobs.

   a. To specify the computers or other sources that are allowed to send unidentified print jobs in Designated Source Mode, click **Add Device**.

   b. Select **IPv4 Address** or **Host Name**.

   c. Type the address of the source that is allowed to send unidentified print jobs.

   d. For User ID, select the information that the device uses for the User ID. If you selected Custom, type the User ID.

  e. Click **Save**.

8. To save the settings, click **Save**.

Accounting Using an Auxiliary Access Device

You can configure the printer to use an auxiliary access device for accounting.

Before you begin, purchase and install the Auxiliary Interface Kit. An Auxiliary Interface Kit, or a Foreign Device Interface Kit, is a third-party access and accounting device. These kits, such as a coin operated printer accessory or a card reader, can be attached to the printer. Installation instructions are included with the Foreign Device Interface Kit.

Enabling Accounting Using an Auxiliary Access Device

1. In the Embedded Web Server, click **Properties** > **Login/Permissions/Accounting** > **Accounting Methods**.
2. Click **Edit**.
3. For Accounting Method, select **Auxiliary Access Device**.
4. Click **Save**.

Displaying Your Company Logo on the Blocking Screen

You can customize the blocking screen to display your company logo. The blocking screen appears on the printer touch screen when card reader authentication or an auxiliary accounting device is configured. The screen displays a message when a user attempts to access a restricted feature, reminding users to swipe an identification card to access the feature.

Changing the Window Title and Instructional Text

1. In the Embedded Web Server, on the Accounting Methods page, for Import Customer Logo, click **Import**.
2. For the area that you want to change, click the area on the sample screen. Type the text that you want to appear in that area:
   - In the area near the top of the sample screen, type a title.
   - In the area below the title, type instructions for users. For example, type **Swipe your employee badge over the card reader to log in**.

Importing the Company Logo

1. In the Embedded Web Server, on the Accounting Methods page, for Import Customer Logo, click **Import**.
2. Click **Browse** or **Choose File**.
3. Select a **.png** file that is not larger than 300 x 200 pixels, then click **Open**.
4. Click **Import**.
5. Click **Restart Device**.

Deleting the Company Logo

1. In the Embedded Web Server, on the Accounting Methods page, for Import Customer Logo, click **Import**.
2. For Logo Placement, click **Delete Image**, then click **OK**.
3. To ensure that the changes take effect, click **Restart Device**.

Setting the Auxiliary Device Type

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **Accounting Settings > Accounting Mode**.
3. Touch **Auxiliary Access > Auxiliary Device Type**.
4. Touch your auxiliary access device type.
5. Touch **OK**.

Selecting Apps to Restrict or Track

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **Accounting Settings > Accounting Mode**.
3. Touch **Auxiliary Access > App Access and Accounting**.
4. To track usage of the copy and printing apps, for Track App Usage, select an option.
5. To restrict particular apps, for Restrict App Access, select options as needed.
6. Touch **OK**.

Setting the Job Timeout

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **Accounting Settings > Accounting Mode**.
3. Touch **Auxiliary Access > Job Timeout**.
4. Touch **Enabled**.
5. To specify the amount of time that the printer waits before it deletes a job, for Job Timeout, enter the time in seconds using the Up and Down arrows.

   Note: The printer only deletes held network print jobs or jobs that are waiting for payment.
6. Touch **OK**.

Specifying Double Count Large Impressions

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **Accounting Settings > Accounting Mode**.
3. Touch **Auxiliary Access > Double Count Large Impressions**.

4. Touch **Count Once** or **Count Twice**.
5. Touch **OK**.

Premium Select

Premium Select allows you to specify that Legal-sized paper (8.5 x 14 in.) is counted for large impressions.

To change the Premium Select setting:

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **Accounting Settings > Accounting Mode**.
3. Touch **Auxiliary Access > Premium Select**.
4. Select an option.
   - **Legal 8.5 x 14**: This option enables Premium Select.
   - **None**: This option disables Premium Select.
5. Touch **OK**.

Enabling Accounting in Print Drivers

Enabling Accounting in a Windows Print Driver

1. To open the Windows® control panel, on your computer, in the Windows® search bar, type `control`.
2. From the search results, select **Control Panel**, then select **Devices and Printers**.
3. Right-click the printer in the list, then select **Properties > Configuration > Accounting**.
4. From the Accounting System menu, select **Xerox Standard Accounting** or **Xerox Network Accounting**.
5. For Tracking Options, select a tracking option. To track all jobs, select **Tracking for All Jobs**.
6. To prompt users to type their User ID and Account ID each time they print, set Print-Time Prompt to **Enabled**. If you do not want users to log in, select **Disabled**.
7. Click **Accounting Codes > Setup**.
8. In the Default User ID and Default Account ID fields, type the user information. To show characters as asterisks when an ID is entered, set Mask User ID and Mask Account ID to **Enabled**.
9. To show the last entered code when users are prompted for their Account ID, for Remember Last Entered Codes, select **Enabled**.
10. Click **OK**.

Enabling Accounting in an Apple Macintosh Print Driver

Users must select this preset each time they print or send a LAN fax using the print driver.

1. Open a document and select **File**, then select **Print**.
2. Select the Xerox® printer.
3. From the menu, select **Xerox Features > Advanced**.
4. Click **Accounting**.
5. For Accounting System, select **Xerox Standard Accounting** or **Xerox Network Accounting**.
6. Select a tracking option.
7. If you want users to type their User ID and Account ID every time they print, select **Print Time Prompt**.
8. To show characters as asterisks when the user types an ID, select **Mask User ID** and **Mask Account ID**.
9. To specify the default User ID and Account ID, type them in the Default User ID and Default Account ID fields. If you are using Xerox Standard Accounting, select the default account type.
10. To close the Accounting configuration dialog, click **OK**.
11. To save your settings, click the **Presets** menu, then select **Save Current Settings As Preset**.

12. Type a name for the preset and select a preset availability option:
    - **All printers**
    - **Only this printer**
13. Click **OK**.

Printing a Copy Activity Report

The copy activity report is a usage report that prints after each copy session. The report lists details about the job and the number of copies made during the session.

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **Accounting Settings > Copy Activity Report**.
3. Touch **Enabled**.
4. Touch **OK**.

10

Administrator Tools

This chapter contains:

Viewing Device Status and Configuring Frequently Used Functions

The Home page in the Embedded Web Server displays device status and information. The Home page provides a quick view of notifications, supplies usage, tray settings, app configuration, and billing information. The Quick Links provide access to device driver downloads, reports, the Remote Control Panel, and other frequently used functions.

Note: For details on the Embedded Web Server, refer to Configuration Steps.

Notifications: To configure control panel alerts and emails, click **Settings**. For details, refer to Configuring Alerts.

Trays: To manage paper and tray settings, click **Settings**. For details, refer to Tray Content and Settings in Paper Management.

Supplies: To view detailed information for toner, cleaning kits, and other user-replaceable items, click **Details**.

Billing: To view billing meter and usage details, click **Usage**.

Apps: You can use this section to view the configuration status and configure any app, or device function, installed on the device. To configure apps and device functions, click the link associated with the app or function that you want to edit.

Note: The apps listed here are configured to appear on the control panel touch screen. User-installed apps appear at the end of this list. For details, refer to Displaying or Hiding ConnectKey Apps.

- To configure the copy function, click **Copy**. For details, refer to Specifying Default Copy Settings.
- To show or hide the ID Card Copy app, click **ID Card Copy**. For details, refer to Displaying or Hiding ConnectKey Apps.
- To configure Scan to Destination, click **Scan To**. For details, refer to Configuring Scan To Destination.
- To enable or disable Print from USB or Print from Mailbox, click **Print From**. For details, refer to Print From USB.
- To configure the Fax function, click **Fax**. For details, refer to Faxing.
- To manage file repositories, click **Workflow Scanning**. Refer to File Repository Setup.
- To configure the fax repository, click **Server Fax.** For details, refer to Fax Repository Setup.
- To configure email functions, click **Email**. For details, refer to Email Setup.
- To configure display settings and permissions for custom apps, click **Xerox® App Gallery**. For details, refer to Weblet Management.
- To configure Internet fax functions, click **Internet Fax**. For details, refer to Internet Fax Setup.
- To show or hide other weblets or EIP Apps, click the weblet or EIP App name. For details, refer to Displaying or Hiding ConnectKey Apps.

Quick Links: You can use the links in this section for quick access to frequently used features. To access a feature, click the appropriate Quick Links icon.

- To create or install a clone file, click **Cloning**. For details, refer to Cloning.
- To download the most current print driver, click **Download Driver**.
- To enable or disable remote control panel access, or to use the remote control panel feature, click **Remote Control Panel**. For details, refer to Remote Control Panel.
- To view or print a Configuration Report or other information, click **Information Pages**. For details, refer to More Information.
- To access remote services settings, click **Remote Services Upload**. For details, refer to Remote Services.
- To restart the device, click **Reboot Device**.
- To view or print current device settings, including hardware descriptions, software versions, and other information, click **Configuration Report**. For details, refer to Configuration Report.

Display Device Information

You can specify the details, such as device model, IPv4 address, host name, contact name, or HTTP address, to appear on the control panel.

1. In the Embedded Web Server, click **Properties > General Setup > Display Device Information**.
2. To display the required device information, for Information Field, select an option from the list.
3. Click **Apply**.

Customizing Device Contact Information

The Support page in the Embedded Web Server displays contact information for service and supplies and for your system administrator. You can customize this information to display your company details for device users.

To add your own custom information:

1. In the Embedded Web Server, click **Support**.
2. Click **Edit Settings**.
3. Update the fields with your information, then click **Apply**.

Configuring Alerts

You can configure the following warnings and alerts:

- Low supply and scan disk memory warnings to appear on the control panel
- Email alerts
- Status LEDs and sounds

To view alerts, in the Embedded Web Server, click the **Home** tab.

To configure alerts:

1. Access the Embedded Web Server.
2. Access the Notification Settings page using one of the following methods:
   - Click **Properties > General Setup > Notification Settings**.
   - Click **Home**, then for Notifications, click **Settings**.

Control Panel Alerts

You can specify when you want the device to display a warning on the control panel touch screen.

Setting Scan Disk Memory Warning

You can specify when you want the printer to display a warning on the control panel if the printer scan disk memory is low. Low memory can cause the printer to slow down or lose jobs.

1. In the Embedded Web Server, click **Properties > General Setup**.
2. Click **Notification Settings > Control Panel Alerts**.
3. For Scan Disk Memory Warning, select the estimated number of scanned pages that the device can hold in scan memory before a warning appears.

   Note: The higher the number of pages that you select, the more frequently warnings appear.

Setting Low Supply Warning

You can set the device to display a warning on the control panel when supplies reach a low level.

1. In the Embedded Web Server, click **Properties > General Setup**.
2. Click **Notification Settings > Control Panel Alerts**.
3. To display low supply warnings on the control panel, select **Display Low Supply Warnings on the device's touch screen**.
4. To display a low toner warning on the control panel, for Toner, select **Show Warning**.
5. Click **Apply**.

Configuring Low Supply Warning

To set when the device displays low supply warnings:

1. In the Embedded Web Server, click **Properties > General Setup**.
2. Click **Notification Settings > Control Panel Alerts**.
3. In the Days Remaining area, for each supply, select when you want the device to display an alert. The range is 1–20 days.
4. Click **Apply**.

   Note: To view current supplies status, on the Home tab, navigate to Supplies, then click **Details**.

Email Alerts

You can define groups to receive email notifications when selected status alerts occur on the printer.

1. In the Embedded Web Server, click **Properties > General Setup**.
2. Click **Notification Settings > Email Alerts**.
3. For Recipient Group Addresses, select which group you want to enable. You can type up to five email addresses to receive selected alerts.
4. In the Recipient Group Preferences area, for the group you created, select the type of alerts that cause email notifications to occur. You can set up to three groups to receive any combination of email alerts.
5. In the Status Codes area, for Email billing meters for manual submission, click **Edit**. Select the days and times to send a billing meter report, then click **Apply**.
6. To view definitions of the alert types, in the Recipient Group Preferences area, for Status Codes, click **(Glossary)**.
7. For "Reply to:" Email Address, type the email address of the administrator or user designated to receive any replies sent by Alert Notification group members.
8. Specify how long the device waits after a jam is detected before sending an email status message. For Set jam timer for release of status to selected groups, type a number between 0–60 minutes. The default time is 0 minutes.
9. Click **Apply**.

Status LED and Sounds

You can configure the device to enable Status LED lights to flash and play sounds to alert users to various device conditions or events. You can enable or disable Status LED lights and sounds independently of each other. You can set the volume for each sound independently of each other.

Note: Status LED lights and sounds are enabled by default.

Status LED lights flash blue when:

- A print job, copy job, or receive-fax job has completed
- A user has swiped a card for authentication
- The device is powering on
- A mobile client is using AirPrint to locate the device

Status LED lights flash amber when:

- The device has an error or shows an alert. The LED flashes on and off to indicate a more serious condition, which can require a call for service.
- The device requires user attention. The LED fades in and out to indicate a less serious condition.

Sliders allow you to control the sound volume independently for each of the following events:

- **Touch**: A sound plays when a user interacts with the control panel touch screen.
- **Job Completion**: A sound plays when a print job, copy job, or receive-fax job completes.
- **Login**: A sound plays when a user swipes an authentication card.
- **Fault/Alert**: A sound plays when the device issues an alert or when the device requires user attention.
- **Power**: A sound plays when the device is powering down.
- **Energy Saver**: A sound plays when the device enters or exits Energy Saver mode.

Displaying the Status LED

Configuring the Status LED in the Embedded Web Server

To configure the status LED in the Embedded Web Server:

1. In the Embedded Web Server, click **Properties > General Setup > Status LED & Sounds**.
2. Select **Display Status LED**.
3. Click **Apply**.

Configuring the Status LED at the Control Panel

To configure the status LED at the control panel:

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **Device Settings > General > Status LED**.
3. For Status LED, select the toggle button.

   Note: A check mark on the toggle button indicates Enabled.

4. Touch **OK**.

Configuring Sounds

Configuring Sounds in the Embedded Web Server

To configure sounds in the Embedded Web Server:

1. In the Embedded Web Server, click **Properties > General Setup > Status LED & Sounds**.
2. To enable sounds, select **Enable Sounds**.
3. To adjust the sound volume for an event, move the appropriate volume slider control as needed.
4. Click **Apply**.

Configuring the Sounds at the Control Panel

To configure the sounds at the control panel:

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **Device Settings > General > Sounds**.
3. For Enable Sounds, select the toggle button.

   Note: A check mark on the toggle button indicates Enabled.

4. To adjust the sound volume for an event, move the appropriate volume slider control as needed.
5. Touch **OK**.

Energy Saving Settings

Setting Energy Saver Mode

Note: Any user activity or network activity that is related to the device brings the device out of Sleep mode or Low Power mode. This rule applies to all Energy Saver modes.

Configuring Energy Saver Settings in the Embedded Web Server

To configure Energy Saver settings in the Embedded Web Server:

1. In the Embedded Web Server, click **Properties > General Setup > Energy Saver**.
2. For Exit Sleep Mode Strategy, select an option.
   - **Intelligent Ready**: When this option is enabled, the device wakes and sleeps based on previous usage.
   - **Job Activated**: When this option is enabled, the device wakes when it detects activity.

     For devices that support Low Power Mode:

     - To set the delay before the device enters Low Power Mode, for Ready Mode, enter the minutes.
     - To set the delay before the device enters Sleep Mode, for Low Power Mode, enter the minutes.
     - To allow the device to power off after a time in Sleep Mode, select **Auto Power Off**.

     For devices that do not support Low Power Mode:

     - To set the delay before the device enters Sleep Mode, for Ready Mode, enter the minutes.
     - To allow the device to power off after a time in Sleep Mode, select **Auto Power Off**.

       Note: Selecting Auto Power Off is not recommended because the device does not respond until you power it on manually.

     - To set the delay before the device powers off, for Sleep Mode, enter the hours.
   - **Sleep and wake up at scheduled times**: The device wakes and sleeps according to a schedule that you specify. To specify the schedule:
     - To allow the device to wake when it senses activity on a specific day of the week, for Schedule Based on, select **Activity**.
     - To allow the device to wake and sleep at a specific time of day, for Schedule Based on, select **Time**. For Wake Up time and Sleep, select the time of day.
3. Click **Apply**.

   Note: Not all options listed are supported on all devices. Some options apply only to a specific device model, configuration, operating system, or driver type.

Configuring Energy Saver Settings at the Control Panel

To configure Energy Saver settings at the control panel:

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **Device Settings > General > Energy Saver**.

   Note: If this feature does not appear, log in as a system administrator. For details, refer to Accessing the Control Panel as a System Administrator.

3. To configure the device to wake and sleep based on previous usage, select **Intelligent Ready**.
4. To configure the device to wake when it detects activity, select **Job Activated**.

   a. To change the default power saver timeout periods, touch **Sleep Timers**.

   - For devices that support Low Power Mode, to change the number of minutes before the device enters low-power mode, for Low Power Mode, touch Plus (**+**) or Minus (**-**).
   - To change the number of minutes before the device enters sleep mode, for Sleep Mode, touch Plus (**+**) or Minus (**-**).
   - To enable auto power off from sleep mode, for Allow auto power off from sleep mode, touch the toggle button. To change the number of hours before the device powers off after entering sleep mode, for Power Off, touch Plus (**+**) or Minus (**-**).

     Note: A check mark on the toggle button indicates that the feature is enabled.

   b. Touch **OK**.

5. To configure the device to wake and sleep according to a schedule that you specify, select **Scheduled**.

   a. To specify the schedule, touch **Scheduled Settings**.

   - To allow the device to wake when it senses activity on a specific day of the week, touch a day of the week. For Schedule Based on, touch **Activity**.
   - To allow the device to wake and sleep at a specific time of day, touch a day of the week. For Schedule Based on, touch **Time**. To select the time of day for wake and sleep, touch **Wake Up Time** or **Sleep Time**. To set the time, for Hours, touch the arrows. Touch **AM** or **PM**.

   b. Touch **OK**.

6. Touch **OK**.

Screen Saver

The screen saver protects the display against damage from burn-in. When the display is on for extended periods of time, burn-in can occur.

Use this page to configure a value for the screen-saver timer. When the screen-saver timer expires, the device enters screen-saver mode.

The device starts the screen-saver timer in the following situations:

- When the printer starts up
- When the printer restarts
- When the printer wakes from sleep mode

- When the printer exits from screen saver mode

The device stops the screen-saver timer in the following situations:

- When the screen-saver mode activates
- When the printer enters sleep mode
- When you reset the screen-saver timer

To configure screen-saver settings:

1. In the Embedded Web Server, click **Properties > General Setup > Screen Saver**.
2. To specify when the screen saver is activated, for **Start After**, select an option from the list.
   - **Never**: This option disables the screen saver.
   - **… Minutes**, where … refers to a number of minutes: This option activates the screen saver after the specified number of minutes. The number of minutes ranges from 5–25 in increments of 5 minutes.
3. Click **Apply**.

   Note: When you change the screen-saver timer, the current timer value resets to zero.

Configuring USB Port State in Sleep Mode

The USB Port State in Sleep Mode feature controls power supply to USB (Type A) accessories when the device is in Sleep Mode. To remain active, accessories, such as Xerox® Wireless Network Adapter and USB card readers, require that power is maintained to the USB port in sleep mode.

Configuring USB Port State Sleep Mode in the Embedded Web Server

To configure USB Port State Sleep Mode in the Embedded Web Server:

1. In the Embedded Web Server, click **Properties > Connectivity > Setup**.
2. For USB Port State in Sleep Mode, select **Edit**.
   - To permit USB accessories to operate during Sleep Mode, select **Powered**.

     Note: The Powered option can cause an increase in power consumption during Sleep Mode.

   - To disconnect power from USB accessories during Sleep Mode, select **Not Powered**.

     Note: When wireless networking is active on the device, you cannot disconnect power from USB accessories. The Not Powered option is not available.
3. Click **Save**.

Enabling USB Port State Sleep Mode at the Control Panel

To enable USB Port State Sleep Mode at the control panel:

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **Network Settings > USB Settings**.

3. Touch **USB Port State in Sleep Mode**.
4. For Power USB Port in Sleep Mode, select the toggle button.

   Note: A check mark on the toggle button indicates Enabled.

5. Touch **OK**.

Remote Control Panel

The Remote Control Panel allows you to access the control panel of the printer from a Web browser.

To enable the Remote Control Panel feature:

1. In the Embedded Web Server, click **Support > Remote Control Panel** or click **Home > Remote Control Panel**.
2. For Configuration, click **Edit**.
3. For Enablement, select **Enable**, then select an option:
   - **For Admin only**: This option allows system administrators to access the Remote Control Panel.
   - **For Admin and Diagnostics Users Only**: This option allows system administrators and Xerox representatives to access the Remote Control Panel.
   - **For All Users**: This option allows all users to access the Remote Control Panel.
4. Click **Save**.

To restrict other users from accessing the control panel when you are connected, select **Block device control panel**. If a user attempts to access the control panel, a message appears.

To access the control panel remotely, click **Start Remote Session**.

Entry Screen Defaults

You can set the default screens that appear on the touch screen when you press buttons on the device control panel.

Selecting the Entry Screen Defaults

1. In the Embedded Web Server, click **Properties > General Setup**.
2. Click **Entry Screen Defaults**.
3. For Default Walkup Screen, select the screen that appears when you walk up to the printer.
4. For Default Screen when Originals are Detected, select the screen that appears when you load original documents into the automatic document feeder or onto the document glass.
5. Click **Apply**.

Remote Services

Remote Services is a suite of features that simplify printer ownership and administration. It provides free services to enable administration of metered billing and supplies replenishment plans for printers on a network.

Before you begin, if your network uses an HTTP proxy server, provide information about your proxy server. For details, refer to Proxy Server.

Configuring Remote Services

1. In the Embedded Web Server, click **Properties > General Setup > Remote Services Setup**.
2. For Remote Services, select **Enabled**.
3. Configure Remote Permissions:
   - To allow the printer to request software files from Xerox, for Software Download, select **Enabled**.
   - To allow the printer to synchronize with the Xerox licensing server, for Feature Activation, select **Enabled**.
   - To allow a Xerox remote server to modify internal device settings, for Update Device Settings, select **Enabled**.
   - To allow the printer to send diagnostic information to Xerox when an error occurs, for Automatically Send Diagnostic Information, select **Enabled**.
4. To synchronize the printer with the Xerox® Remote Services data center on a defined schedule, for Daily Synchronization Time, type the time.
5. To verify communication with the Xerox® Remote Services data center, click **Synchronize Now**.

   A status message appears.
6. If your network uses an HTTP proxy server, to set or update your proxy server, for HTTP Proxy Server, click **Edit**.
7. Click **Save**.

Remote Management Server Setup

The Remote Management Server Setup feature allows the printer to detect, and communicate with one or more remote management servers in the network. The remote management servers can be Xerox CentreWare® Web, Xerox Device Manager, or other Xerox partner servers.

The Remote Management Server Setup feature is enabled by default. The setup feature uses industry-standard DNS mechanisms to locate management servers in the network. Ensure that you set up DNS server addresses on the printer. The simplest way to set up DNS is to use DHCP, at least temporarily. When the printer is set up, you can switch to a DHCP reserved address, or a static IP address.

The feature uses the Xerox Discovery Service to detect the remote-management servers. To detect the remote-management server, the feature queries your DNS server.

- The feature searches for a server called XeroxDiscoverService in the same network domain as the printer, for example yourdomain.com. If you have only one remote-management server in your network, name the remote-management server **XeroxDiscoverService.yourdomain.com** in your DNS servers.
- The Remote Management Server Setup feature looks for a server with an alias address. For example, if the remote-management server is called server1.yourdomain.com, create a DNS alias **XeroxDiscoverService.yourdomain.com**. Use the alias to refer to server1.yourdomain.com.
- The feature looks in DNS for DNS-SD records. DNS-SD records are DNS text records that contain service discovery keywords. The DNS server can have many remote-management servers listed with a XeroxDiscoverService keyword. DNS returns the server list to the printer. The printer works down the list of up to 10 servers, then attempts to check in to all of them.
- If your DNS servers do not have DNS-SD records, enter the remote-management server address using an IP address, host name, or IPv6 address.

The service discovery runs after the printer starts, or when you request that the printer performs the discovery.

For more information on setting up the Xerox Discovery Service in DNS, refer to www.xerox.com.

Configuring a Remote Management Server Connection

1. In the Embedded Web Server, click **Properties > General Setup > Remote management server setup**.
2. For Enablement, select **Enabled**.
3. To discover a management server, click **Discover servers**.
4. If needed, to enter the remote-management server address manually, for Server address, enter the IP address, host name, or IPv6 address.
5. To test communication between the remote-management server and the printer, click **Check in now**.
   Information about the last check-in appears in the Last status results area.
6. Click **Apply**.

Fleet Orchestrator

The Fleet Orchestrator feature allows you to configure many devices in similar ways, automatically. After you configure one device, you can distribute any of the configuration settings to other devices, as needed. You can set up schedules to share configuration settings regularly and automatically.

The Fleet Orchestrator feature enables you to share the following types of configuration files:

- Software upgrade files: A software upgrade file contains the latest firmware for the device. Xerox releases upgrades when needed.
- Clone files: A clone file contains configuration settings from a device. When you install a clone file on another device, the clone file changes the configuration settings to match the settings on the cloned device.
- 1-Touch Add-On files: A 1-Touch Add-On file adds workflows to a device without overwriting existing apps or workflows.

Software Upgrade Files

When Xerox releases a new version of software for your device, you can use Fleet Orchestrator to install the software upgrade file. Software upgrade files do not overwrite printer configuration settings.

Note: You can update your device manually, using a USB Flash drive. For details, refer to Manually Updating the Software Using a USB Flash Drive.

Setting the Security Installation Policy for Software Upgrade

To set the installation policy for software upgrades:

1. In the Embedded Web Server, click **Properties > Security > Installation Policies**.
2. To allow software upgrades to install on the device, for Software Upgrade, select **Allow Software Upgrades**.
   This setting allows software upgrades at the control panel touch screen, at the Embedded Web server, automatic software upgrades using FTP, and using print submission.
3. Click **Apply**.

Installing a Software Upgrade File

To install a software upgrade file:

1. In the Embedded Web Server, click **Properties > Fleet Orchestrator**.
2. Click **Create/Install File > Install a File**.
3. Click **Software Upgrade File**.
4. To change the installation policy, in the Details area, for Installation Policy, click the current policy setting. Change the policy as needed, then navigate back to the Install Configuration File page.
5. In the File to Install field, click **Browse**, then select the software upgrade file that you want to install.

6. If you are installing the upgrade on a publisher, and are using file sharing, select the **Share This File** option.
7. Click **Install**.

Software installation begins several minutes after you submit the software to the device. When installation begins, the Embedded Web Server is disabled. You can monitor the installation progress from the control panel touch screen.

After the upgrade completes, the device restarts, then prints the following reports:

- Configuration Report
- Software upgrade report
- Vocal fax modem upgrade report: This report prints only if the machine has a vocal fax modem and if the device upgrade file contained a vocal fax upgrade component.

To verify that the software has updated, check the Extended Software Upgrade Details, or the Configuration Report.

Enabling Automatic Software Upgrade

You can configure the device to connect to an FTP directory on your network to update the device software. To use this feature, download the latest software file, then copy it to an FTP server. After the software upgrade completes, the device retains all configured network settings and installed options.

Note: You can use the file-sharing function of Fleet Orchestrator to manage clone files and 1-Touch Add-On files. You can manage software upgrades using either the Fleet Orchestrator file-sharing function, or automatic software upgrades with FTP. It is recommended that you use only one software-upgrade method.

To schedule automatic upgrades:

1. In the Embedded Web Server, click **Properties > Fleet Orchestrator**.
2. Click **Create/Install File > Install a File**.
3. Click **Automatic Software Upgrade**.
4. To change the installation policy, in the Details area for Installation Policy, click the current policy setting. Change the policy as needed.
5. In the Schedule area, select **Enabled**.
6. For Refresh Start Time, select **Hourly** or **Daily**. If you select **Daily**, type the time in hours and minutes.
7. Enter the FTP server information:
   a. In the Connection area, for Host, select the address type. The options are **IPv4**, **IPv6**, or **Host Name**.
   b. For Host, type the appropriately formatted address and port number of the server where the upgrade software is located. The default port number is 21.
   c. For Directory Path, type the full path to the .dlm software upgrade file on the server.
   d. For Login Name, type the name that the device uses to access the server.
   e. Type the password, then type the password again to verify.

   f. To update an existing password, select **Save Password**.

8. Click **Save**.

Extended Software Upgrade Details

If there are software upgrades installed on your device, you can view information about the upgrades:

1. In the Embedded Web Server, click **Properties > Fleet Orchestrator**.
2. In the Configuration Files area, for Software Upgrade, click **View**.
   - Current Software: The Current Software section shows the date and time of the most recent installation, and the current software version number.
   - Last Upgrade Attempt: The Last Upgrade Attempt section shows the date and time of the most recent software upgrade attempt, the software version, and the installation status.
3. Click **Close**.

Clone Files

Clone files contain configuration settings from a device. You can use the clone file to overwrite the configuration settings on another device with the configuration settings from the original device.

You can create clone files to suit your cloning strategy. For example:

- To standardize general device settings across a group of devices, create a clone file that contains configuration settings from one device.
- To standardize security settings on all your devices, create a clone file with a set of specific settings, such as security policies.

Note: Unique configuration settings, such as an IP address, are not cloned.

The Fleet Orchestrator feature allows you to create, install, and share clone files.

Note: You can use a clone file to create a backup file of the configuration settings for your printer, except for unique settings such as the IP address. For information on creating a complete backup, refer to Backup and Restore Settings.

Setting the Security Installation Policy for Cloning

To set the installation policy for cloning:

1. In the Embedded Web Server, click **Properties > Security > Installation Policies**.
2. For Cloning, select an option.
   - To limit clone file installation to encrypted clone files only, select **Only encrypted clone files can be installed**.
   - To allow any clone file installation, select **Both encrypted and unencrypted clone files can be installed**.

     Note: Clone files from older devices are unencrypted. Select this option when installing unencrypted clone files.

   - To prevent clone file installation, select **Clone files cannot be installed**.

3. To allow clone files to install by sending a print job, select **Allow Print Submission**. This option allows you to send a clone file to multiple devices by writing a script and printing the file.

   Note: The Allow Print Submission option is valuable for use with older software versions, but because the print path is not authenticated, this option can present a security risk. For details, click **Fleet Management & Print Submission Tips**.

4. Click **Apply**.

Creating a Clone File

To create a clone file:

1. In the Embedded Web Server, click **Properties > Fleet Orchestrator**.
2. Click **Create/Install File > Create a File**.
3. In the Create Configuration File area, click **Clone File**.
4. In the Details area, modify the settings for the clone file:
   - **File Name**: To use a unique filename, type a filename. The default filename is Cloning.dlm.
   - **Share This File**: To share the file if the device is a publisher device in a file-sharing group, select this option.
   - **Download This File**: To download the clone file, select this option.
5. In the Configuration Settings area, select the settings that you want to clone:
   - To choose individual items, select or clear individual check boxes.
   - To view the details of an individual setting, click **Details**.
   - To select all settings, click the Select information icon, then click **Select All Groups**.
   - To clear all settings, click the Select information icon, then click **Deselect All Settings**.
   - To show or hide the configuration file settings, click **Show Settings** or **Hide Settings**.
6. Click **Create**.
7. To download the clone file, right-click the clone file link, then click **Save As** or **Save Target As**. Select a name and location for the file, then click **Save**. Do not change the **.dlm** file extension.
8. Click **Close**.

Installing a Clone File

You use the Fleet Orchestrator feature to install a clone file.

Note: To install a clone file manually on a single device using Fleet Orchestrator, disable FIPS 140-2. After the clone file installation is complete, you can reenable FIPS. If you are using the file-sharing function of Fleet Orchestrator, you do not have to disable FIPS to receive clone files. For information on FIPS settings, refer to FIPS 140–2.

To install a clone file manually:

1. In the Embedded Web Server, click **Properties > Fleet Orchestrator**.
2. Click **Create/Install File > Install File**.
3. To install a clone file, in the Install Configuration File area, select **Clone File**.
4. To change the installation policy, in the Details area, for Installation Policy, click the link.

5. To select the clone file, in the Additional Options area, for File to Install, click **Browse**. Navigate to the clone file that you want to install, then click **Open**.
6. To share the file, if file sharing is on, and you are installing the clone file on a publisher, select **Share This File**.
7. Click **Install**.
8. Click **OK**.

Note: If the device is in a file-sharing group, you can set the device to receive clone files from the file-sharing group. A clone file received from the file-sharing group overwrites a manually installed clone file.

If you are using FIPS 140-2 and the file sharing function of Fleet Orchestrator:

- Devices using the FIPS security modes can share configuration files with other devices in a file-sharing group, using the file-sharing function of the Fleet Orchestrator feature. Manual clone file installation is not allowed.
- If you share the clone files, FIPS files on the subscribing devices remain on the devices. Set FIPS on each device.
- The publisher device can enable or disable FIPS without affecting the subscriber devices. The default setting is disabled.
- To set up a publisher device that is in FIPS mode already, configure settings individually, then create the clone file to share. If you have a clone file to apply to a publisher device, enable FIPS 140-2 temporarily.

Extended Clone Details

If there are clone files installed on your device, you can view information about the latest clone file installations:

1. In the Embedded Web Server, click **Properties > Fleet Orchestrator**.
2. In the Configuration Files area, for Clone, click **View**.
3. To filter the list, select an option:
   - To display all status information, select **Show All**.
   - To display status information for areas that installed with exceptions, select **Exceptions Only**.
4. For information about exceptions, click **Troubleshooting**.
5. Click **Close**.

1-Touch Add-On Files

A 1-Touch Add-On file contains all 1-Touch Apps that are on a device. You can use the 1-Touch Add-On file to install the 1-Touch Apps from the originating device onto one or more devices.

Note: 1-Touch Add-On files work differently than clone files:

- When you install a clone file that includes 1-Touch Apps, the 1-Touch Apps in the clone file replace the 1-Touch Apps that were on the device.
- When you install a 1-Touch Add-On file, the 1-Touch Apps are added to the 1-Touch Apps on the device.

For information on creating 1-Touch Apps at the control panel, refer to 1-Touch Apps.

Creating a 1-Touch Add-On File

After creating 1-Touch Apps at the control panel, you can create a 1-Touch Add-On file to add the 1-Touch Apps to other devices. If you have not created any 1-Touch Apps, the 1-Touch Add-On file is empty. To create a 1-Touch Add-On file:

1. In the Embedded Web Server, click **Properties > Fleet Orchestrator**.
2. Click **Create/Install File > Create a File**.
3. In the Create Configuration File area, click **1-Touch Add-On File**.
4. In the Details area, select options for the 1-Touch Add-On file:
   - **File Name**: To use a unique filename, type a filename. The default filename is Add-on.dlm.
   - **Share This File**: To share the file if the device is a publisher device in a file-sharing group, select this option.
   - **Download This File**: To save the 1-Touch Add-On file to your computer, select this option.
5. Click **Create**.
6. To download the 1-Touch Add-On file, right-click the file link, then click **Save As** or **Save Target As**. Select a name and location for the file, then click **Save**. Do not change the **.dlm** file extension.
7. Click **Close**.

Installing a 1-Touch Add-On File

To install a 1-Touch Add-On file:

1. In the Embedded Web Server, click **Properties > Fleet Orchestrator**.
2. Click **Create/Install File > Install a File**.
3. In the Install Configuration File area, select **Add-On File**.
4. In the Additional Options area, for File to Install, click **Browse**. Navigate to the 1-Touch Add-On file that you want to install, select the file, then click **Open**.

   Note: All 1-Touch Add-On files have a file extension of .dlm.

5. To share the file, if file sharing is on, and you are installing the 1-Touch Add-On file on a publisher, for **Share This File**, select the check box.
6. Click **Install**.
7. Click **OK**.

Extended 1-Touch Add-On Details

If there are 1-Touch Add-On files installed on your device, you can view information about the 1-Touch Add-On file installations:

1. In the Embedded Web Server, click **Properties > Fleet Orchestrator**.
2. In the Configuration Files area, for 1-Touch Add-On, click **View**.
3. To filter the list, select an option:
   - To display the status information for all installed Add-On files, select **Show All**.
   - To display the status information for Add-On files that installed with exceptions, select **Exceptions Only**.
4. For information about exceptions, click **Troubleshooting**.
5. Click **Close**.

Automatic File Sharing

The Fleet Orchestrator feature allows you to share files automatically between devices in your fleet. The Fleet Orchestrator feature can share files from one device to other devices in a distribution tree. To share files, set up a trust community. Devices in a trust community work together automatically, without manual intervention. The Fleet Orchestrator feature uses the following terms:

- File Sharing Group: A set of devices set up to trust each other for sharing files. The file-sharing group is referred to as a trust community.
- Tree: A collection of trusted devices organized into a hierarchy to balance the workload of sharing files. You can set up more than one tree.
- Publisher: The top node of the tree. The publisher is the only device that can add, remove, or update the files that are shared within the tree. The publisher device sets up and monitors the rest of the tree. A publisher distributes files to subscribers in the tree.
- Subscriber: Any device in the tree besides the publisher. A subscriber pulls files from a distributor, based on the subscriber device schedule.
- Distributor: An intermediate device that distributes files to other subscribers lower in the tree.
- Unassociated: A device that is part of the file-sharing group, but is not connected into the tree. An unassociated device continues to share files with the subscriber devices, but the unassociated device no longer receives new files. You can move devices from the tree so that they become unassociated devices. You can reconnect unassociated devices to the distribution tree at a later time.

You can set up the publisher device to share files with other linked devices within a trust community. A trust community forms when the publisher device links to one or more devices. When file-sharing groups are formed, the devices within the trust community can share files. The publisher device maintains and manages the trust relationship for the devices in the tree. The trust relationship remains intact until you revoke it.

Configuration Overview

To set up file sharing, on the publisher device, you can arrange trusted devices into a hierarchy called a tree. File sharing includes the following tasks:

- Designate a device as the publisher device of the tree.
- Designate a friendly name for the publisher device. The friendly name of the publisher device becomes part of the name for the file sharing group. The file sharing group is called the trust community.
- Create a tree structure for the file sharing group. To create a tree, add subscriber and distributor devices to the file sharing group. The added devices form a trusted relationship.

  Note: For customers who use Xerox® Device Manager or Xerox® CentreWare® Web software: The publisher device in the trust relationship can be a printer, Xerox® Device Manager, or Xerox® CentreWare® Web software
- Create download and installation schedules for each device.
- Make files available for distribution.

Note: If two or more devices need a device-specific clone file or software upgrade, you can create as many separate distribution trees as required.

On the publisher device, you can view the complete tree structure. On subscriber devices, you can view only certain parts of the tree structure.

The Fleet Orchestrator pages for each device in a file sharing group have links to other devices in the tree. To navigate to a device, click the link. As you add more devices, you can use this system to send files to one device, then cascade the files to other devices.

Note: To find solutions to common problems for the file-sharing feature, refer to Troubleshooting.

Setting the Security Installation Policy for File Sharing

You can use the file-sharing function of the Fleet Orchestrator feature to share configuration files in a file-sharing group. The security installation policy for file sharing is enabled by default. When this policy is enabled, a subscriber device receives files through file sharing, even if the separate cloning and software upgrade security installation policies are disabled.

To change the security installation policy:

1. In the Embedded Web Server, click **Properties > Security > Installation Policies**.
2. Select or clear **Allow File Sharing**.
3. Click **Apply**.

Configuring File Sharing

You can use the Configure File Sharing feature to configure your printer as a Publisher device.

To set up file sharing:

1. In the Embedded Web Server, click **Properties > Fleet Orchestrator**.
2. In the Share Configuration Files area, click **Configure File Sharing**.
3. Click **Publish Files & Manage File Sharing Group**.
4. To set the preferred address, for Preferred Address, select the IP address or Fully Qualified Domain Name of the publishing device.

5. Click **Start Sharing**.
6. Click **Close**.

File sharing is active. On the publishing device, the Share Configuration Files area on the Fleet Orchestrator page provides information about the file sharing group.

Managing a File Sharing Group

To manage a file sharing group from the publisher device:

1. In the Embedded Web Server, click **Properties > Fleet Orchestrator**.
2. In the Share Configuration Files area, for File Sharing Group, click **Manage**.
3. On the File Sharing page, in the Share Configuration Files area, select an option:
   - **Add Device**: Refer to Adding a Device from a Publisher.
   - **Edit Selected**: Refer to Editing a Device.
   - **Delete Selected**: Refer to Deleting a Device.
   - **Advanced**: This option allows you to perform advanced actions:
     - **Restrict File Sharing**: Refer to Restricting File Sharing at the Publisher.
     - **Reset File Sharing Group**: Refer to Resetting a File Sharing Group.
     - **Troubleshooting**: Refer to Troubleshooting.
4. To change the management view, click **Tree** or **Table**. To manage more than one device at the same time, use the Table view.
5. To rearrange the devices in the file sharing group, in the Tree view, select an option:
   - Drag and drop a device into the publisher or distributor group.
   - Drag and drop a device into the Unassociated Devices group. Refer to Unassociated Devices.
6. To view information about any device in the group, in the Tree view, select the device.
7. Click **Close**.

Adding a Device

You can add devices to the file sharing group from the publisher device. You can subscribe to the file sharing group from a subscriber device.

Adding a Device from a Publisher

To add a device to the file-sharing group from the publisher device:

1. In the Embedded Web Server, click **Properties > Fleet Orchestrator**.
2. In the Share Configuration Files area, for File Sharing Group, click **Manage**.
3. Click **Add Device**.
4. Enter the host details for the subscriber:
   a. For Host, select an address type:
      - **Host Name**: Enter the Fully Qualified Domain Name.
      - **IPv4 Address**: Enter the IPv4 Address.

   b. Type the user name and the password for the subscriber device.

   c. To check the details of the device that you are adding, click **Get Device Details**.

5. For the Download schedule, select options:

   a. For Frequency, select **Monthly**, **Weekly**, or **Daily**.

   b. For Time, choose a download time.

   c. For Download Files From, select a device from which to download files.
   You can select a publisher or a distributor device.

   d. For Random Download Delay, select a number of minutes for the random delay..
   Setting the Random Download Delay minutes ensures that devices do not pull configuration files from a distributor device at the same time.

6. For Install Schedule, select options:

   a. For Install Policy, select an option:

      - **Install New Files Only**: Select this option to install configuration files only if they have changed.

      - **Always Install File**: Select this option to install files based on the install schedule. For example, to ensure that settings are restored every day, you can reapply a clone file containing security settings.

   b. For Frequency, select **Weekly**, **Daily**, or **Immediately**. If you choose Weekly, select a day of the week.

   c. For Time, choose a time for the installation.

7. Click **Add**.
   The Share Configuration Files page appears. You can use the page to manage the file-sharing group:

   - To view the details of any device, click the device that appears in the Tree.

   - To show different views of the device information, select **Tree** or **Table**.

   - To move devices within the Tree, drag and drop one device to another.

     Note: You cannot change the publisher device, but you can change the relationships between distributor and subscriber devices.

8. To return to the Share Configuration Files page, click **Close**.

Adding a Device from a Subscriber

To subscribe to a file-sharing group from a device that you want to act as a distributor or subscriber:

1. In the Embedded Web Server, click **Properties > Fleet Orchestrator**.

2. In the Share Configuration Files area, click **Configure File Sharing**.

3. In the Configuration File Sharing area, click **Subscribe & Distribute Files**.

4. In the Receiving Details area, enter the host details of the publishing device. For Host, select an address type:

   - **Host Name**: Enter the Fully Qualified Domain Name.

   - **IPv4 Address**: Enter the IPv4 Address.

5. Click **Start Sharing**.

The Fleet Orchestrator feature displays the Add Device page of the publishing device. To add the download schedule and installation settings for the subscriber device, use the Add Device page. For more information, refer to Adding a Device from a Publisher.

Editing a Device

From the publisher device, you can edit the download schedule and installation settings for subscriber devices. To edit a device from the publisher:

1. In the Embedded Web Server, click **Properties > Fleet Orchestrator**.
2. In the Share Configuration Files area, click **Manage**.
3. On the File Sharing page, in the Devices area, select a device.
4. In the Share Configuration Files area, click **Edit Selected**.
5. To alter the download schedule, in the Download schedule area, select the options that you want to change.
   - **Frequency**: Select this option to change the frequency to **Monthly**, **Weekly**, or **Daily**.
   - **Time**: Select this option to change the time of the download.
   - **Download Files From**: Select this option to select a distribution device from the list.
   - **Random Download Delay**: Select this option to change the time delay for the file download.
6. To alter the installation schedule, in the Install Schedule area, select the options that you want to change.
   - **Install Policy**: Select this option to set the installation policy. Choose **Install New Files Only** or **Always Install Files**.
   - **Frequency**: Select this option to change the frequency to **Weekly**, **Daily**, or **Immediately**. If you select Weekly, select a day.
   - **Time**: Select this option to change the download time.
7. Click **Update**.
   The Share Configuration Files page appears. To change the file-sharing group, use the options on this page.
8. To close the Share Configuration Files page, click **Close**.

Deleting a Device

At the publisher device, to delete a subscriber device from the file sharing group:

1. In the Embedded Web Server, click **Properties > Fleet Orchestrator**.
2. In the Share Configuration Files area, click **Manage**.
3. On the File Sharing page, in the Devices area, select a device.

   Note: To select multiple devices, choose Table view, then select the check box for each device to be deleted.

4. Click **Delete Selected**, then confirm the deletion.

Deleting a Device Connection

The preferred method for deleting a device is from the publisher. For information, refer to Deleting a Device.

Caution: Deleting the connection from a subscriber device is recommended only if you no longer have access to the publisher. Deleting a device connection from a subscriber can cause problems with the file sharing group.

At the subscriber device, to delete the connection to the file sharing group:

1. In the Embedded Web Server, click **Properties > Fleet Orchestrator**.
2. In the Share Configuration Files area, click **View**.
3. On the Receive Files page, in the Share Configuration Files area, click **Delete Connection**.
4. To confirm the deletion, click **Delete**.

Getting Files Now on a Subscriber

From a subscriber device, you can get shared files at any time, using the Get Files Now feature. The Get Files Now command downloads available files from the publisher or distributor, and installs the files immediately.

1. In the Embedded Web Server, click **Properties > Fleet Orchestrator**.
2. In the Share Configuration Files area, click **View**.
3. On the Receive Files page, in the Share Configuration Files area, click **Get Files Now**.
4. Click **Continue**.

Restricting File Sharing

You can use the Restrict File Sharing feature to prohibit communication and sharing with other devices in the file-sharing group. The restriction includes management controls such as add, edit, and delete. Operations vary, depending on the device that you are navigating from. When you restrict sharing, the restriction affects only the device that you are using.

Restricting File Sharing at the Publisher

To restrict the publishing device from communicating with other devices in the file-sharing group:

1. In the Embedded Web Server for the publishing device, click **Properties > Fleet Orchestrator**.
2. In the Share Configuration Files area, click **Manage**.
3. On the File Sharing page, in the Devices area, select a device.
4. In the Shared Configuration Files area, click **Advanced > Restrict File Sharing**.
5. Click **Close**.

Restricting File Sharing at a Subscriber

To restrict file sharing on a subscriber device:

1. In the Embedded Web Server for the subscriber device, click **Properties > Fleet Orchestrator**.
2. In the Share Configuration Files area, click **View**.

3. On the Receive Files page, in the Share Configuration Files area, click **Restrict Sharing**.
4. Click **Close**.

Unassociated Devices

Unassociated devices are connected to the file sharing group. Unassociated devices are not associated with a distributor device, and do not receive updated configuration files.

A device is unassociated when:

- You drag a subscriber device to the Unassociated row within the Tree view.
- You add or edit a device, then select the Unassociated option for Download Files From. For details, refer to Adding a Device from a Publisher or Editing a Device.
- The distributor device for the device is deleted.

Reconnecting Unassociated Devices

To reconnect an unassociated device to the file sharing group on the publisher:

1. In the Embedded Web Server, click **Properties > Fleet Orchestrator**.
2. In the Share Configuration Files area, click **Manage**.
3. On the File Sharing page, in the Devices area, using the Tree view, drag an unassociated device to the publisher or a distributor device.
4. Click **Close**.

To edit the device after reconnecting it, refer to Editing a Device.

Stopping File Sharing

To stop publishing a Clone or Add-On file from the publisher:

1. In the Embedded Web Server, click **Properties > Fleet Orchestrator**.
2. In the Configuration Files area, to stop file sharing, on the Clone or Add-On file, click **Stop Publishing File**.
3. To confirm, click **OK**.

Resetting a File Sharing Group

You can reset your file sharing group to delete your device connections and shared files. This action allows you to create a different file sharing group, or to operate your fleet without file sharing.

Note: It is recommended to back up the publisher device before resetting the file sharing group.

To reset your file sharing group:

1. In the Embedded Web Server, click **Properties > Fleet Orchestrator**.
2. In the Share Configuration Files area, click **Manage**.
3. On the File Sharing page, in the Shared Configuration Files area, click **Advanced > Reset File Sharing Group**.

4. To confirm, click **Reset**.

   Caution: The reset will delete all device connections and file sharing settings. This action cannot be undone.

Troubleshooting

Errors can occur when you are managing your devices. The best way to troubleshoot is to open the publisher device and the subscriber device, then view the status of each device.

To view troubleshooting information from the publisher device:

1. In the Embedded Web Server, click **Properties > Fleet Orchestrator**.
2. In the Share Configuration Files area, click **Manage**.
3. On the File Sharing page, in the Share Configuration Files area, click **Advanced > Troubleshooting**.

Cloning

Clone files contain configuration settings from your device. You can install the clone file on other printers, or keep the clone file as a backup of the configuration settings for your device. You can create and install a clone file using the Embedded Web Server, or a USB Flash drive.

Creating and Installing a Clone File in the Embedded Web Server

To create and install a clone file in the Embedded Web Server, use the Fleet Orchestrator feature. For details, refer to Fleet Orchestrator.

Creating a Clone File on a USB Flash Drive

Before you begin, ensure that a USB port is enabled. For details, refer to Enabling or Disabling USB Ports.

Note: To create or install a clone file on a USB Flash drive, log in as an administrator. For details, refer to Accessing the Control Panel as a System Administrator.

To create a clone file on a USB Flash drive:

1. At the control panel touch screen, touch **Device** > **Tools**.
2. Touch **General** > **Cloning**.
3. Insert a USB Flash drive into a USB port on the printer, then touch **Create Clone File**.
   The device creates a clone file called cloning.dlm in the root directory on the USB Flash drive. The clone file contains all the printer configuration settings, except for unique settings, for example, the IP address.
4. Click **Close**, then remove the USB Flash drive from the printer.

Installing a Clone File from a USB Flash Drive

Before you begin, ensure that the Cloning feature is enabled. For details, refer to Setting the Security Installation Policy for Cloning.

Note: If the Cloning feature is disabled, a clone file does not appear in the file list on the USB Flash drive.

To install a clone file from a USB Flash drive:

1. Insert the USB Flash drive into a USB port on the printer.
2. At the control panel touch screen, touch **Install File**.
3. Select the cloning.dlm file, then touch **Install**.
4. To confirm the installation, touch **Install**.
5. When prompted, remove the USB Flash drive from the USB port.

   Caution: To avoid corrupting the installation, do not remove the USB Flash drive until directed to do so.

After the clone file installation, the device restarts, then prints a Configuration Report. The cloned settings are effective when the device restarts.

Language and Keyboard

You can configure the default language settings and the default keyboard for the device. You can also configure the device to allow walk-up users to change the language on the Home screen for their session. When this option is enabled, a globe icon appears on the device Home screen.

Note: A language or keyboard change at the device control panel is in effect for the current user session only. The device language for the Home screen resets to the default language specified for any of the following conditions:

- The user logs out
- The user presses Reset
- The session times out

Setting Language and Keyboard Options

Configuring the Language and Keyboard Options in the Embedded Web Server

To configure the language and keyboard options in the Embedded Web Server:

1. In the Embedded Web Server, click **Properties > General Setup > Language & Keyboard**.
2. To set the default display language, for Choose a Default Language, select a language.
3. To set the default display keyboard, for Choose a Default Keyboard, select a language.
4. To allow users to select a session language on the control panel Home screen, select **Language Option on Home Screen**.
5. Click **Apply**.

Configuring the Language and Keyboard Options at the Control Panel

To configure the language and keyboard options at the control panel:

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **Device Settings > General > Language / Keyboard Selection**.
3. To set the default display language, select a language.
4. To set the default display keyboard:
   a. Touch **Keyboard Layout**, then select a language.

      Note: To view the keyboard in the selected language, touch **View Keyboard**.

   b. Touch **OK**.
5. To allow users to select a session language on the control panel Home screen, for Language Option on Home, select the toggle button.

   Note: A check mark on the toggle button indicates Enabled.

6. Touch **OK**.

Backup and Restore Settings

The Backup and Restore feature allows you to save device settings and to restore them. The device automatically saves a backup of its configuration settings periodically. You can create a backup file of your device settings manually, at any time. These backup files contain the specific settings for your device.

You can store a manual backup file on the device or in an external folder. Xerox recommends that you create a backup of your device settings when the device is operating as expected. This practice is useful for restoring the device settings at any time, such as when the settings have changed in error.

You can restore the device settings from an automatic backup file or from a manually created backup file that is stored locally or externally.

Note: Only backup files created on this device can be restored to this device. For details on copying the settings from a device that is configured to one or more devices, refer to Cloning.

Before you begin, set the installation policy to allow backup file restoration.

Setting the Security Installation Policy for Backup and Restore

To set the security installation policy for backup file restoration:

1. In the Embedded Web Server, click **Properties > General Setup > Backup & Restore Settings**.
2. Set the installation policy as needed.
   - To allow backup file installation, click **Allow Installation**.
   - To prevent backup file installation, click **Restrict Installation**.
3. Click **OK**.

Note: To view all installation policies, click **Security Installation Policy**.

Restoring Settings

You can restore settings from a backup file stored on the device or from a previously exported backup file. When restoring from a file stored on the device, you can choose a manual backup file or an automatic backup file. Automatic backup files are created daily. These backup files contain the state of the settings at the time the automatic backup starts.

Restoring Settings from a File Stored on the Device

To restore settings from a file stored on the device:

1. In the Embedded Web Server, click **Properties > General Setup > Backup & Restore Settings**.
2. To locate the backup file that you want to restore, for Locally Stored Backup Files, use the information in the Date/Time column and Type column.
3. In the Actions column, for the backup file, click **Restore**.

Restoring Settings from an Exported Backup File

To restore settings from a previously exported backup file:

1. In the Embedded Web Server, click **Properties > General Setup > Backup & Restore Settings**.
2. Click **Browse** or **Choose File**.
3. Navigate to the location of the file that you want to import, then click **Open**.
4. Click **Import and Restore**.

Creating a Manual Backup File that is Stored on the Device

Caution: If a manual backup file exists in the list, the new file overwrites it. The previous manual backup file cannot be recovered.

1. In the Embedded Web Server, click **Properties > General Setup > Backup & Restore Settings**.
2. For Create Backup, click **Create Local**. The new backup file appears in the list.

Creating and Downloading a Backup File

1. In the Embedded Web Server, click **Properties > General Setup > Backup & Restore Settings**.
2. Click **Create and Export**.
3. To download the new backup file, click the file name link.

Deleting a Backup File

1. In the Embedded Web Server, click **Properties > General Setup > Backup & Restore Settings**.
2. For Locally Stored Backup Files, locate the file that you wish to remove, then click **Delete**.

   Note: Only backup files that were created manually can be deleted. The device overwrites the automatic backup files during the daily automatic backup.

Billing Impression Mode

The Billing Impression Mode defines how the printer tracks impressions made on large-size paper, such as A3 or tabloid size paper.

There are two modes.

- A3 Impressions counts all impressions equally.
- A4 Impressions counts large impressions (A3/Tabloid) as the A4/Letter equivalent.

A Xerox representative sets the Billing Impression Mode for your device.

Changing the Billing Impression Mode

1. In the Embedded Web Server, click **Properties > General Setup**.
2. Click **Billing Impression Mode**.

   Note: A personal identification number (PIN) is required to change the billing impression mode. To obtain a PIN, contact your Xerox representative and provide the sequence and serial number information that appears on the Billing Impression Mode page.
3. For PIN, type the number that you obtained from your Xerox representative.
4. Click **Apply**.

Configuration Watchdog

The Configuration Watchdog feature monitors selected printer configuration settings. If a configuration setting changes, the Configuration Watchdog resets that configuration setting. The Configuration Watchdog feature reports reset configuration settings as remediations.

To use the Configuration Watchdog feature, configure the printer settings, select which configuration settings to monitor, then set the monitoring frequency. You can specify contacts in the Notification Settings page to notify you when the Configuration Watchdog feature resets printer settings.

Note: To prevent unintentional changes to settings and a device restart, configure the required printer settings first, then select the configuration settings that you want to monitor.

Configuring the Configuration Watchdog Feature

1. In the Embedded Web Server, click **Properties > General Setup > Configuration Watchdog**.
2. To check or edit the configuration settings for the feature that you want to monitor:
   a. Ensure sure that feature check box for **Monitored** is clear.
   b. Click **link to feature**, configure the setting, then click **Apply**, or **Save**.
   When you save or close the feature setup page, you are returned to the Configuration Watchdog feature page.
3. In the Monitored Features area, select the features that you want to monitor:
   - To select an individual feature to monitor, select **Monitored**.
   - To select all features, click **Select All**.
   - To disable monitoring for all features, click **Deselect All**.

   When you select one or more features, the Configuration Watchdog feature is enabled and the Configuration Monitoring status is Active.
4. To specify how often the selected features are monitored, for Configuration Monitoring, select a Frequency option.
5. To check feature compliance for monitored features at any time, click **Check Now**.
6. To view or select group notification settings, for Notifications, click **Notification Settings**.
7. Click **Save**.

The configuration setting for each monitored feature appears in the Current Compliance Setting column.

The Notifications area shows the results of the latest check:

- **Compliant**: The monitored settings for the feature did not change since the last check.
- **Remediated**: The monitored settings for the feature changed since the last check, and were reset to the configuration settings that you set for the printer.
- **Failed to Remediate**: The monitored settings for the feature changed since the last check, but the Configuration Watchdog feature did not return the settings to the configuration settings that you set for the printer.

Address Books

An address book is a list of individual contacts, each associated with an email address, fax number, or scan destination. You can configure the printer to use a Network Address Book or the Device Address Book for email or Internet fax. The Network Address Book looks up addresses from an LDAP directory. If you do not have an LDAP server, you can use the Device Address Book. If you configure both address books, users are presented with a choice to use either address book at the control panel.

Device Address Book

The Device Address Book is an address book that is stored on the device locally. You can configure the printer to use the Device Address Book instead of a Network Address Book. You can add contacts manually, import directly from emails that are sent to or from the device, or import them from a .csv file.

Viewing Contacts

A contact is a user with an associated email address, fax number, or scan destination. Contacts can be added to groups or marked as a Favorite.

To view a contact, in the Embedded Web Server, click the **Address Book** tab, then do one of the following:

- To view all contacts in the address book, for Address Book, select **All Contacts**.
- To view a specific type of contact, for Email, Fax, or Scan To Destination, select **Contacts**.
- To view specific contact information, select the contact from the list.

Manually Editing the Address Book

You can use contacts, groups, or Favorites to edit and organize the address book manually.

Adding or Editing a Contact

1. In the Embedded Web Server, click **Address Book**.
2. To add or edit a contact in the address book:
   - To add a contact to the address book, click **Add**.
   - To edit a contact in the address book, select the contact, then click **Edit**.

   Note: If the Add button is unavailable, the address book has reached its limit. The Device Address Book can contain up to 5000 contacts.
3. Type the contact information:
   a. To associate a scan destination with this contact, for Scan To Destination, click the Plus (**+**) button. For details, see the Help in the Embedded Web Server. For details about configuring the Scan To Destination feature, refer to Configuring Scan To Destination.

   b. To mark a contact as a Favorite for email, fax, or scan to destination, click the star next to the appropriate field. If you click the star next to Display Name, the contact becomes a Global Favorite.
4. Click **Save**, or select **Add Another Contact After Saving**, then click **Save**.

Removing a Contact from the Address Book

To remove a contact from the address book, select the contact, click **Delete**, then click **OK**.

Deleting All Contacts from the Address Book

To delete all contacts from the address book, from the Management list, select **Delete All**.

Managing Groups

Groups allow you to send a file to multiple address book contacts at the same time. Unknown Groups are unrecognized groups that were created in an address book that you imported from another printer. You can convert unknown groups to a fax group, then add or remove contacts from the group as needed.

Adding or Editing a Fax Recipient Group

1. In the Embedded Web Server, click **Address Book**.
2. To add or edit a fax recipient group, for Fax, select **Groups**.
   - To add a fax group, click **Add Group**.
   - To edit a fax group, select the group, then click **Edit Group**.
3. For Group Name, type a name for the group.
4. To set this group as a favorite, for Add Fax Favorite, click the star icon.
5. To convert an unknown group to a fax group, for Group Location, select a group type.
6. To add a contact to the group, from the list of available contacts on the left, select the contact. Contacts in the group appear in the Group Members list to the right. To add all available contacts, click **Add All**.
7. To remove a contact from the group, from the Group Members list on the right, select the contact. To remove all contacts, click **Remove All**.
8. Click **Save**.

Adding or Editing an Email Recipient Group

1. In the Embedded Web Server, click **Address Book**.
2. To add or edit an email recipient group, for Email, select **Groups**.
   - To add an email group, click **Add Group**.
   - To edit an email group, select the group, then click **Edit Group**.
3. For Group Name, type a name for the group.
4. To set this group as a favorite, for Add Email Favorite, click the star icon.
5. To convert an unknown group to an email group, for Group Location, select a group type.
6. To add a contact to the group, from the list of available contacts on the left, select the contact. Contacts in the group appear in the Group Members list to the right. To add all available contacts, click **Add All**.
7. To remove a contact from the group, from the Group Members list on the right, select the contact. To remove all contacts, click **Remove All**.
8. Click **Save**.

Managing Favorites

You can mark contacts that you frequently use as favorites. A star next to a contact in the list indicates a Favorite. You can mark a favorite as a Global Favorite for all services or as a Favorite for email, fax, or scan to destinations.

To manage favorites:

1. In the Embedded Web Server, click **Address Book**.
2. To edit a contact marked as a Favorite:
   a. Select the contact from the Favorites list for the appropriate section, then click **Edit Favorite**.
   b. Edit the contact information as needed, then click **Save**.
3. To clear a contact marked as a Favorite:
   Select the contact from the Favorites list for the appropriate section, then click **Delete Favorite**.
4. Click **OK**.

Importing Addresses Using Email

The Import Using Email feature adds email addresses to the Device Address Book from emails sent to the printer. Use this feature to populate the address book without manually typing address information. You can allow users to send encrypted email by storing encryption certificates from received signed email.

Note: Xerox recommends that you disable the Import Using Email feature after the Device Address Book is populated sufficiently. When this feature is enabled, the Device Address Book can fill quickly. For example, if you send an email message to the printer containing 30 recipient addresses in the CC field, and you allow the printer to add addresses in the CC field, all 30 addresses are added to the address book.

Before You Begin

Configure the POP3 settings. For details, refer to POP3.

Configuring Import Using Email

1. In the Embedded Web Server, click **Address Book**.
2. From the Management list, select **Import Using Email**.
3. For Enablement, select **On**.
4. In the Policies area, for Email Type, select an option:
   - To allow the device to add the email addresses of all senders to the Device Address Book, select **All Emails**.
   - To add email addresses contained in emails sent with a digital signature only, select **Only Signed Emails**.
5. To save digital certificates sent with signed email messages, select **Import encryption certificate from signed emails**.
6. To add email addresses to the Device Address Book from the From, To, and CC fields, for Add all recipients contained in the following email fields, select one or more fields.
7. Click **Save**.

Importing Device Address Book from File

You can import address book contacts from a **.csv** file.

Note:

- The device recognizes the second row in the **.csv** file as the first address book entry. The first row contains headings for the information in each column.
- To view an example of the appropriate format for the **.csv** file, download a sample file.

Importing an Address Book File

1. In the Embedded Web Server, click **Address Book**.
2. From the Management list, select **Import from File**.
3. For Select an Address Book file to Import, click **Browse** or **Choose File**, then select your **.csv** file. Click **Open** or **Choose**.
4. For Record Delimiter, select an option.
5. Some device manufacturers allow you to export address book contacts to a **.csv** file, but contact information is enclosed in brackets. To remove brackets when importing this type of **.csv** file, select **Remove brackets from the beginning and end of text fields**.
6. For Existing Contact Management, select an option:
   - **Add new contacts to the existing Device Address Book**: This option adds user information from the **.csv** file to the existing user information stored in the database.
   - **Replace existing Device Address Book with the new contacts**: This option replaces all user information in the database with user information from your **.csv** file.
7. Click **Upload File**.
8. For Verify Address Book Field Mappings, click **Import**.
9. To upload a different address book file or revise the settings, click **Change File/Options**.
10. If the current address book fields match exactly the imported file fields, the headings do not appear. To see the mapped fields, click **Show Headings List**.
11. If the current address book fields do not match exactly the imported file fields, the headings appear. The unmapped fields are highlighted. To assign a mapping to the field, select a heading from the list.
12. Click **Import Address Book**.

Editing the Device Address Book as a .csv File

To manage many addresses, you can create and edit a list in a spreadsheet application. You can save the list as a **.csv** file and upload it to the printer.

Downloading a Sample .csv File

To back up your current address book, you can export the address book as a **.csv** file. To view an example of the appropriate format for the **.csv** file, download a sample file. You can use the sample file as template, replacing the existing values with your own information.

1. In the Embedded Web Server, click **Address Book**.

2. From the Management list, select **Download Sample**.
3. For Delimiter, select an option.
4. Select **Export in Legacy Mode** as needed. Legacy Mode omits favorites, groups, fax, and Scan To Destination contact information. Display Name is changed to Friendly Name, allowing you to import the file directly to an older Xerox® printer without mapping address book fields.
5. To exclude Email, Scan to Destination, Fax, or Internet Fax, clear the option.
6. Click **Download**.

Exporting an Address Book File

To back up your current address book, or to import it to another device, you can export your current address book contacts as a **.csv** file.

1. In the Embedded Web Server, click **Address Book**.
2. From the Management list, select **Export**.
3. For Delimiter, select an option.
4. Select **Export in Legacy Mode** as needed. Legacy Mode omits favorites, groups, fax, and Scan To Destination contact information. Display Name is changed to Friendly Name, allowing you to import the file directly to an older Xerox® printer without mapping address book fields.
5. Click **Export**.

Configuring Device Address Book Security Settings

You can allow users to edit the Device Address Book, or restrict editing to system administrators only.

1. In the Embedded Web Server, click **Address Book**.
2. To set user permissions to view and manage the address book, from the Management list, select **Security: User Permissions**.
3. Select an option:
   - To require users to log in as an administrator to edit the address book, select **Only System Administrators**.
   - To allow anyone to edit the address book, select **Open to All Users**.
4. Click **Save**.

Network Address Book

The Network Address Book looks up addresses from an LDAP directory. If you do not have an LDAP server, you can use the Device Address Book.

Configuring the Network Address Book for Email

Before you begin, configure LDAP server settings. For details, refer to LDAP.

1. In the Embedded Web Server, click **Properties > Apps > Email > Setup > Address Books**.
2. In the Policies area, for Use Network Address Book (LDAP) to allow users to access this address book, select **Yes**.

3. Click **Apply**.

Configuring the Network Address Book for Internet Fax

Before you begin, configure LDAP server settings. For details, refer to LDAP.

1. In the Embedded Web Server, click **Properties > Apps > Internet Fax > Setup > Address Books**.
2. In the Policies area, for Use Network Address Book to allow users to access this address book, select **Yes**.
3. Click **Apply**.

LAN Fax Address Book

The LAN Fax feature has a separate directory for storing and managing addresses. For details about using or configuring the LAN Fax address book, refer to the driver help.

Font Management Utility

The Xerox® Font Management Utility is a utility that allows you to manage fonts for one or more printers on your network. You can use the font management utility to download your company branded fonts or unicode fonts to support multiple languages on your printer. You can add, delete, or export fonts. You can select printers in the utility printer list that you want to display.

To download Xerox® Font Management Utility, go to www.support.xerox.com, enter your product name, then select **Drivers and Downloads**.

Note: Not all options listed are supported on all printers. Some options apply only to a specific printer model, configuration, operating system, or driver type.

Network Logs

Log files are text files of recent printer activity that are created and stored in the printer. Log files are used to monitor network activity or troubleshoot network problems. A Xerox customer support representative can interpret the encrypted format log files.

Downloading a Network Log

1. In the Embedded Web Server, click **Properties > General Setup > Network Logs**.
2. For Information Level, select options as needed. To include NVM data with network log push, select the check box.
3. Click **Save**.
4. Click **Start Download**.
5. After the information processes, click **Download File Now**, then save the files to your computer.
6. To send files to Xerox for diagnostic purposes, click **Send**.

   Note: A log identifier is required for service of a Xerox device. After logs are sent to Xerox, save the log identifer.

Downloading a Network Log to a USB Flash Drive

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **Network Settings > Network Logs**.
3. Insert a USB Flash drive into the USB port on the back of the device, then touch **Download Log Files**.

   Caution: Do not remove the USB Flash drive until the download completes. If you remove the USB Flash drive during the download process, the USB Flash drive can become damaged.

   When the download completes, a confirmation message appears.
4. Remove the USB Flash drive, then touch **Close**.

Restarting the Device in the Embedded Web Server

To restart the device, log in as a system administrator. For details, refer to Accessing the Embedded Web Server as a System Administrator. To restart the device:

1. In the Embedded Web Server, click **Home**.
2. At the bottom of the page, click **Reboot Device**, then click **OK**.

The device restarts.

Restarting the Device at the Control Panel

Using Software Resets to restart the device is faster than powering the device off and on. Restarting the device can take up to five minutes during which time the Embedded Web Server is not available.

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **Troubleshooting**.
3. Touch **Resets**.
4. Touch **Software Resets**.
5. For Reset Options, select the type of reset that you want.
   - **All Software**

     Note: The All Software option has the same function as pressing Power on the device and then touching Restart.

   - **Network Software**
   - **Copy Software**
6. Touch **Restart**.

Taking the Device Offline

To prevent the device from sending or receiving jobs over the network at any given time, you can take the device offline. Taking the device offline allows you to perform device maintenance without jobs being sent to the device. When the device is offline, any apps, such as Workflow Scanning, are unavailable.

1. At the control panel touch screen, log in as Administrator.
2. Touch **Device**, then touch **Tools**.
3. Touch **Network Settings**.
4. Touch **Online / Offline**.
5. Touch **Online** or **Offline**.
6. Touch **Close**.
7. To log out, touch **Admin**.

   Note: When you are finished, ensure that you put the device back online to allow jobs to process.

Erase Customer Data

You can use the Erase Customer Data feature to prepare a printer for removal from the network. This feature clears all customer-specific information including jobs, configurations, and settings from the printer. Printer-specific values, such as total images and supply counters, are not cleared.

Note: When the Erase Customer Data process begins, the device is unavailable for use.

Caution: The erase process permanently removes all jobs, customer configurations, and data. The device IP address options are also reset to factory default, which typically changes the device IP address.

To erase customer data:

1. To configure the device to print a status report after it completes the erase process, load paper in the device.
2. To prevent customer data from reaching the device, disconnect the device from the network. If necessary, disconnect the Ethernet cable.
3. At the control panel touch screen, touch **Device**, then touch **Tools**.
4. Touch **Device Settings > General > Erase Customer Data**.
5. Touch **Erase Customer Data > Erase All Customer Data**.
6. Touch **Confirm**.

   Caution: Do not power off the device during the erase process. Doing so can damage the device.

   Note:

   - The erase customer data process restarts the device and displays messages. The device does not require your attention during the process.
   - The erase process takes 30–50 minutes to complete. When the process completes, a report prints.
7. Power off the device, then disconnect the power cord and other cables from the back of the device.

   The device is ready for moving.

Resetting the User Interface to Factory Default Settings

Note: This procedure resets only a limited number of user interface settings. To clear all customer-specific settings, refer to Erase Customer Data.

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **Device Settings**, then touch **Reset UI to Factory Settings**.
3. Touch **Restart**.

Reverting to Previous Settings

You can revert your device to the settings created during the most recent software upgrade:

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **Device Settings > General > Revert to Previous settings**.
3. Touch **Restart**.

   The device restarts and reverts to the previous settings.

Updating the Device Software

When Xerox releases a new version of software for your device, you can install the software upgrade file using the Embedded Web Server or a USB Flash drive.

Updating the Software in the Embedded Web Server

To install a software upgrade file in the Embedded Web Server, use the Fleet Orchestrator feature. For details, refer to Fleet Orchestrator.

Manually Updating the Software Using a USB Flash Drive

When a new version of software is available, download the software upgrade file to your computer, then copy the file to a USB Flash drive.

To install a software upgrade file from a USB Flash drive, log in as an administrator. For details, refer to Accessing the Control Panel as a System Administrator.

To install the software upgrade file:

1. Insert the USB Flash drive into a USB port on the printer.
2. At the control panel touch screen, touch **Install File**.
3. Browse for the software upgrade .dlm file, then touch **Install**.
4. To confirm the file installation, touch **Install**.
5. When you are prompted, remove the USB Flash drive from the USB port.

   Caution: To avoid corrupting the installation, do not remove the USB Flash drive until directed to do so.

The device installs the software upgrade file. After the upgrade completes, the device restarts, then prints the following reports:

- Configuration Report
- Software upgrade report
- Vocal fax modem upgrade report: This report prints only if the machine has a vocal fax modem and if the device upgrade file contained a vocal fax upgrade component.

Adjusting Color, Image, and Text Detection Settings

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **Device Settings**.
3. Touch **Input**.
4. Adjust how the printer detects color, images, and text in original documents.
    - **Auto Color Detection**: This option allows you to customize the bias based on the type of original documents being scanned and the output required.
        - **Scan from Document Glass**: This option selects the bias toward color or monochrome when scanning using the document glass.
        - **Scan from Document Feeder**: This option selects the bias toward color or monochrome for the document feeder.
    - **Photo/Text Settings**: This option selects the bias toward photo or text quality based on which quality is more important.
5. Touch **OK**.

Note: Not all options listed are supported on all devices. Some options apply only to a specific device model, configuration, operating system, or driver type.

11

Customization and Expansion

This chapter contains:

Xerox Extensible Interface Platform

The Xerox Extensible Interface Platform® allows independent software vendors and partners to develop personalized and customized document management solutions. These solutions can be integrated and accessed directly from the printer control panel. These solutions can leverage existing printer infrastructure and databases. Examples of applications include ScanFlow Store, Scan to PC Desktop, Equitrac Office, and others. For more information on Xerox Extensible Interface Platform® applications for your printer, contact your Xerox representative or refer to www.xerox.com/en-us/office/eip on the Xerox website.

Configuring Extensible Services

1. In the Embedded Web Server, click **Properties > General Setup**.
2. Click **Extensible Service Setup > Settings**.
3. Ensure that the following services are enabled on the HTTP Web Services page:
   - Extensible Service Registration Web service
   - Web services required by solutions that are being installed
4. To enable Extensible Service Registration and other services, for Extensible Service Registration, click **Edit**.
5. If your Xerox Extensible Interface Platform® application requires the user password, for Enable Extensible Services, select **Export password to Extensible Services**.
6. For Browser Settings:
   a. Select **Enable the Extensible Services Browser**.
   b. To check the certificates on the remote server, select **Verify server certificates**.
   c. To show the control panel keypad within EIP apps, select **Show based on individual app setting**. To hide the control panel keypad within EIP apps, select **Hide within all apps**.
7. For EIP Advanced Setting, enter the number of times that EIP applications are allowed to load before the EIP Browser restarts.
8. Configure Proxy Server settings as needed.
   a. For Proxy Server, from the list, select **Proxy**.
   b. To configure HTTP proxy server settings, in the HTTP area, for Enabled, click **Edit**.
   c. To use the same proxy server for HTTPS, select **Use settings for all protocols**.
   d. To use a separate proxy server for Xerox Extensible Interface Platform® applications that use HTTPS, for HTTP, HTTPS, select **Edit**.
   e. To apply the HTTP proxy server settings to the HTTPS proxy server, select **Use settings for all protocols**.
   f. For Bypass Proxy Rules, type the required values, and separate them with commas.
9. Click **Apply**.

Extensible Service Scan Settings

You can configure EIP settings that are specific to scan applications.

To configure scan settings:

1. In the Embedded Web Server, click **Properties > General Setup**.
2. Click **Extensible Service Setup > Scan Settings**.
3. For Scan Workflow Management Settings, select one or both options:
   - **Require System Administrator Authentication for workflow operations**: Enabling this option allows you to apply a security measure that restricts access to scan workflows on the device.
   - **Include user network filing account password in the exported workflow**: Enabling this option includes the user network filing account password during a workflow export operation. Some scan workflows require this password. Disabling this option allows the user to view a workflow without exposing a password.
4. To enable Remote Start, for Start Job via Remote Program, click **On**.
5. Click **Apply**.

Extensible Service Diagnostics

The Diagnostics page displays device connectivity information. Connectivity settings directly impact EIP applications. Improper settings can impair functionality for these applications. You can use this page to diagnose problems with tests for the following settings:

- **Proxy**: These settings allow the device to reach external networks.
- **DNS**: These settings allow the device to convert device names into IP addresses.
- **IP**: These settings allow the device to reach the local network.

To test connectivity for a connection type:

1. In the Embedded Web Server, click **Properties > General Setup**.
2. Click **Extensible Service Setup > Diagnostics**.
3. For a connection type, click **Test**.

Extensible Service Setup for Apps

The Extensible Services Apps page lists the EIP applications that are registered on the device. You can use this page to test the application settings and to test device access to specific URLs.

Accessing Extensible Services Setup for Apps

To access Extensible Services setup for apps:

1. In the Embedded Web Server, click **Properties > General Setup**.
2. Click **Extensible Service Setup > Apps**.

Testing Individual Application Settings

To test individual application settings:

1. For the EIP application to be checked, click **Test**. The results for the application appear in a new page.
2. Follow the instructions on the results page as appropriate.

Testing Specific URLs

To test specific URLs:

1. For Test Connection to URL, enter the URL that you want to test.

   Note: To resize the URL box, drag the lower-right corner.

2. Click **Test**. The results for the tested URL appear in a new page.
3. Follow the instructions on the results page as appropriate.

Extensible Service Advanced Setup

The Extensible Service Advanced Setup page displays the device memory allocation, and usage for the EIP Browser. You can use this page to determine memory usage for EIP applications and appropriate memory allocation for the EIP Browser.

To configure memory allocation for the EIP Browser:

1. In the Embedded Web Server, click **Properties > General Setup**.
2. Click **Extensible Service Setup > Memory Profile**.
3. To update the memory allocation and usage information, click **Refresh**.
4. To change the EIP Browser memory allocation, for Memory Allocation Setup, select an option.
5. Click **Apply**.

Auxiliary Interface Kit

An Auxiliary Interface Kit, or a Foreign Device Interface Kit, is a third-party access and accounting device. These kits, such as a coin operated printer accessory or a card reader, can be attached to the printer. Installation instructions are included with the Foreign Device Interface Kit.

To configure your device to use the Auxiliary Access Accounting method:

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **Accounting Settings**.
3. Touch **Accounting Mode > Auxiliary Access**.
4. Touch **Auxiliary Device Type**, then select your device type.
5. Touch **OK**.

Driver Download Link

The driver installation link appears on the Home, Print, and Support pages in the Embedded Web Server. This link accesses the default driver and downloads page for your printer on the Xerox Support website. You can hide or customize this link to access a location on your network where you post driver installation files for users.

Customizing or Hiding the Driver Download Link

1. In the Embedded Web Server, click **Properties > General Setup**.
2. Click **Configure Driver Links**.
3. To hide the link, for Display Option, select **Hide Link**.
4. To direct users to the location for device drivers on your network, for Software Links, select **Custom Link**, then type a link.
5. To save the new settings, click **Save**. To retain the previous settings, click **Undo**.

Customizing the Home Screen in the Embedded Web Server

In the Embedded Web Server, you can show, hide, or change the display order of apps on the control panel touch screen.

- To customize app features, refer to Customizing the Home Screen at the Control Panel.
- To create a 1–Touch App, refer to Creating a 1-Touch App.

Displaying or Hiding Apps

You can show or hide apps on the control panel touch screen.

Note: You cannot hide apps that are required for basic device operation.

1. In the Embedded Web Server, click **Properties > Apps > Display**.
2. Click **Show/Hide**.
   - To select all apps in the list to appear on the touch screen, click **Show All**.
   - To hide all apps in the list so that no apps appear on the touch screen, click **Hide All**.
   - To select individual apps to appear on the touch screen, for Displayed, select the apps that you want to appear.
3. Click **Apply**.

Setting the Display Order for Apps

You can arrange the order in which apps appear on the control panel touch screen.

1. In the Embedded Web Server, click **Properties > Apps > Display**.
2. Click the **Order** tab.
3. Select, drag, and drop the buttons on the screen until they are in the preferred order.
4. Click **Apply**.

Customizing the Home Screen at the Control Panel

At the Control Panel, to customize the Home screen or app features, log in as an administrator. For details, refer to Accessing the Control Panel as a System Administrator.

Rearranging Apps on the Home Screen

1. At the printer control panel, press the **Home** button.
2. Scroll to the bottom, then touch **Customize**.
3. Touch **Customize Home**.
4. Touch and hold the required app.
5. Drag the app to the new location, then release the app.
6. Touch **Done**.
7. Verify that the apps appear in the correct location on the Home screen.

Displaying or Hiding an App on the Home Screen

1. At the printer control panel, press the **Home** button.
2. Scroll to the bottom, then touch **Customize**.
3. Touch **Customize Home**.
4. To display an installed, but hidden app:
   a. Touch **+**.
   b. Touch the app that you want to appear on the control panel.
   c. Touch **Done**.
5. To hide an installed app:
   a. For the desired app, touch **X**.
   b. At the prompt, touch **Hide**.
   c. Touch **Done**.
6. Verify that only the desired apps appear on the Home screen.

Deleting an App from the Home Screen

1. At the printer control panel, press the **Home** button.
2. Scroll to the bottom, then touch **Customize**.
3. Touch **Customize Home**.
4. To delete an installed app:
   a. For the desired app, touch **X**.

   b. At the prompt, touch **Delete**.

      Note: Deletion is permanent. You cannot restore a deleted app.

   c. Touch **Done**.

5. Verify that only the desired apps appear on the Home screen.

Customizing App Features

To customize the Feature list for an app:

1. At the printer control panel, press the **Home** button.
2. Touch the app required.
3. Scroll to the bottom, then touch **Customize**.
4. Touch **Customize Feature List**.
5. Touch the particular option.
   - To hide a feature, for the required feature, touch the **Eye** icon. To signify that the feature is hidden, the Eye icon appears with a line across it.
   - To show a feature, for the required feature, touch the **Eye** icon. To signify that a feature is visible, the Eye icon appears with no line across it.
6. To reorder the menu features, touch and drag the features into the appropriate order.
7. To save the current configuration, touch **Done**.

Customizing App Default Settings

To customize the default settings for an app:

1. At the printer control panel, press the **Home** button.
2. Touch the app required.
3. Configure the required default settings.
4. Touch **Save**.
5. Touch **Save Settings as Default**. The new settings override the previous default settings.

Removing App Customization Settings

To remove the current app customization settings:

1. At the printer control panel, press the **Home** button.
2. Touch the app required.
3. Scroll to the bottom, then touch **Customize**.
4. Touch **Remove App Customizations**.
5. At the prompt, touch **Remove**.

Removing Customization from the Home Screen

To remove customization from the Home screen:

1. At the printer control panel, press the **Home** button.
2. Scroll to the bottom, then touch **Customize**.
3. Select an option:
   - **Remove Home Customization**: This option removes all customization from the Home screen.

     Note: This option can cause deletion of 1-Touch, EIP, Single Touch, and Weblet apps.

   - **Remove All Customizations**: This option removes all customizations for the device.

     Caution: The Remove Home Customization option removes customization from the Home screen, and other customized device settings.
4. At the prompt, touch **Remove**.

   Apps appear in their default location on the Home screen.
5. Touch **Done**.

1-Touch Apps

You can use 1-Touch Apps to create individual apps for completing frequent jobs or tasks. After you create a 1-Touch App, the app appears on the printer Home screen.

Note: To create or modify a 1-Touch App, log in as an administrator. For details, refer to Accessing the Control Panel as a System Administrator.

- To create a 1-Touch App, refer to Creating a 1-Touch App.
- To change the order of 1-Touch Apps on the Home screen, refer to Rearranging Apps on the Home Screen.
- To display or hide a 1-Touch App, refer to Displaying or Hiding an App on the Home Screen.
- To delete a 1-Touch App, refer to Deleting an App from the Home Screen.

Creating a 1-Touch App

To create a 1-Touch App:

1. At the printer control panel, press the **Home** button.
2. Touch the app required.
3. Select the job settings.
4. Scroll to the bottom, then touch **Create 1-Touch App**.
5. Touch the **Enter App Name** entry field, then use the keypad to enter a name. Touch **Next**.
6. Touch a color scheme option for your 1-Touch App, then touch **Next**.
7. Touch an icon that best suits the 1-Touch App that you are creating, then touch **Next**.
8. Touch the **Enter App Instructions** entry field, then use the keypad to enter instructions for the user. Touch **Next**.

   When the 1-Touch App is selected, the instructions appear at the top of the screen.
9. Touch the app settings required.
   - **Allow Editing Quantity**: Use this option to allow users to view and update the quantity.
   - **Show Feature Settings**: Use this option to display a summary of the features programmed for the 1-Touch App.
10. Touch **Done**.

    The 1-Touch App appears on the Home screen.

Setting Defaults and Policies for Scan Services

You can select the case of the default file name extensions for scan services. Some operating systems are case-sensitive. For example, a case-sensitive system treats myscan.PDF and myscan.pdf as two different files.

You can select a duplex color scanning option based on your requirements for scan speed and image quality.

Note: Not all options listed are supported on all devices. Some options apply only to a specific device model, configuration, operating system, or driver type.

Setting the Filename Extension

To set the case for filename extensions:

1. In the Embedded Web Server, click **Properties > Apps**.
2. Click **Scan Services > Defaults & Policies**.
3. For Filename Extension, select **Lower Case** or **Upper Case**.
4. Click **Save**.

Setting Duplex Color Scanning Options

To set the duplex color scanning option:

1. In the Embedded Web Server, click **Properties > Apps**.
2. Click **Scan Services > Defaults & Policies**.
3. For Duplex Color Scanning Options, select an option:
   - **Select fastest scanning speed**: This option allows scanning at maximum speed.
   - **Select best auto-color detection accuracy**: This option can affect scanning speed in 2-sided auto-color scanning for resolutions of 300 dpi and below.
   - **Select best auto-color detection accuracy and color image quality**: This option can affect scanning speed in 2-sided auto-color scanning and full-color scanning for resolutions of 300 dpi and below.
4. Click **Save**.

   Note: Not all options listed are supported on all devices. Some options apply only to a specific device model, configuration, operating system, or driver type.

Creating a Custom Scan App

You can create a custom scan app and associate the service with a scan workflow. You can also customize the icons and text that appears on the device touch screen.

Note:

- After you create an app, you can edit the description but not the name of the app.
- You can create up to 10 apps.
- The app does not appear on the control panel touch screen until you design your app and select a scan workflow for your app.

Creating a Custom Single-Touch Scan App Overview

- Create the app.
- Customize the appearance of your app. Refer to Customizing the Appearance of Your App.
- Associate a scan workflow with your app. Refer to Associating a Scan Workflow with Your App.
- Lock or hide the app on the control panel as needed. Refer to Setting Access Permissions for Your App.
- Set the app as the default screen that appears on the touch screen as needed. Refer to Setting Your App as the Default Screen on the Device Touch Screen.

Creating a Single-Touch Scan App

1. In the Embedded Web Server, click **Properties > Apps**.
2. Click **Workflow Scanning > Single-Touch App**.
3. Click **Create**.
4. On the New Service page, type a name and description for the app.
5. Click **Create**.

Customizing and Configuring Your App

Customizing the Appearance of Your App

1. In the Embedded Web Server, click **Properties > Apps**.
2. Click **Workflow Scanning > Single-Touch App**.
3. In the App Configuration area, for Design Your App, click **Edit**.
4. On the Design Your App page, click the **Service Design** tab.
5. For Theme, select a color.
6. For App Display Name, type the text that you want to appear in the header.

7. For Instructional Text, type instructions for users.

   Note: Line breaks are supported. For example, you can type:

   Load documents and press Start.

   File original documents in the file cabinet in Room 423.

   Scanned files are sent to the following destinations:

   ServerA:/business_records

   ServerB:/scan_archives

8. Click **Apply**.
9. Continue to Customizing Additional Features.

Customizing Additional Features

1. On the Design Your App page, click the **Additional Features** tab.
2. To allow users to use the Build Job option, select **Display Build Job**.
   - To enable Build Job by default, select **On by default**.

     Note: The On by default setting overrides the default setting specified in the scan workflow that you associate with the app.
   - For Feature Label / Instructional Text, type instructions for users.
3. To allow users to configure Output Color, 2-Sided Scanning, Original Type, or File Name settings, select **Display Image Settings**.

   Note: The scan workflow specifies the default image settings associated with the service.
4. Click **Apply**.

   Note: Not all options listed are supported on all devices. Some options apply only to a specific device model, configuration, operating system, or driver type.
5. Continue to Specifying the Image File for the Custom App Icon.

Specifying the Image File for the Custom App Icon

You can specify the icon image file that you want to represent the app on the Apps Home page.

1. On the Design Your App page, click the **App Icon** tab.
2. For App Icon, click **Browse** or **Choose File**.
3. Select a 160 x 120 pixel **.png** file that represents the app on the control panel touch screen.
4. Click **Open** or **Choose**.
5. Click **Apply**.
6. Click **Close**.

Associating a Scan Workflow with Your App

1. In the App Configuration area, for Choose Scan Workflow, click **Edit**.
2. From the list, select a Scan Workflow.

   Note: If you select Default Workflow, configure the default workflow, then add at least one file destination to the workflow. Refer to Configuring the Default Workflow. For information on creating and editing scan workflows, refer to Managing Scan Workflows.

3. Click **Save**.

Setting Access Permissions for Your App

1. In the App Configuration area, for Define App Access Permissions, click **Edit**.
2. Click the **Non-Logged-In Users** tab.
3. For Permission Role, for Non-Logged-In User, click **Edit**.
4. Click the **Apps & Tools** tab.
5. For your custom app, select an option:
   - To allow users to use the app, select **Allowed**.
   - To restrict users from using the app, select **Not Allowed**.
   - To restrict users from using the app and hide the app from the control panel touch screen, select **Not Allowed and Hidden**.
6. Click **Apply**.
7. Click **Close**.

Setting Your App as the Default Screen on the Device Touch Screen

1. In the App Configuration area, for Set Entry Screen Default, click **Edit**.
2. Click the **Non-Logged-In Users** tab.
3. For Default Walkup Screen, from the list, select your custom app.
4. Click **Save**.

Locking or Hiding Your App from Appearing on the Control Panel

To lock or hide the app from appearing on the control panel, configure Apps and Tools user permissions for the role of non-logged-in users. On the Configure Your App page, for Define App Access Permissions, click **Edit**. For details, refer to User Permissions.

Weblet Management

Weblets are small HTML-based and JavaScript-based applications that you can install on the printer to customize the touch screen. You can download weblets from www.office.xerox.com.

Setting the Security Policy for Unencrypted Weblets

You can set a security policy for weblet encryption. Enable this setting to allow installation of unencrypted weblets on the device. Disable this setting to require encryption for installation of all weblets on the device.

To set the security installation policy for weblet installation:

1. In the Embedded Web Server, click **Properties > Apps > Custom Apps > Weblet Management**.
2. For Weblet Settings, select an option:
   - To allow installation of unencrypted weblets on the device, select the **Allow unencrypted Weblets to be installed on this device** check box.
   - To restrict weblet installation on the device to encrypted weblets only, clear the **Allow unencrypted Weblets to be installed on this device** check box.
3. Click **Apply**.

Installing a Weblet

1. In the Embedded Web Server, click**Properties > Apps > Custom Apps > Weblet Management**.
2. Click **Choose File** or **Browse**, navigate to a **.weblet** file, then click **Choose** or **Open**.
3. Click **Install Weblet**.

Enabling Weblet Installation at the Control Panel

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **App Settings > Weblet Settings**.
3. Touch **Weblet Install Policy**.
4. Touch **Allow Installation**.
5. Touch **OK**.

Enabling Weblet Installation in the Embedded Web Server

1. In the Embedded Web Server, click **Apps > Custom Apps > Weblet Management**.
2. Click **Security Installation Policy**.
3. For Weblet, select **Allow Weblet Installation**.
4. Click **Apply**.

Installing a Weblet at the Control Panel

Before you begin, save the **.weblet** file to a USB Flash drive.

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **App Settings > Weblet Settings**.
3. Touch **Weblet Management**.
4. Touch **Install from USB**.
5. Insert the USB Flash drive. Follow the instructions on the touch screen.
6. Browse to the appropriate file folder on the USB Flash drive, then touch the **.weblet** file that you want to install.

Configuring Weblet Settings

1. In the Embedded Web Server, click **Apps > Custom Apps > Weblet Management**.
2. In the Installed Weblets area, for a weblet, click **Edit**.
3. To hide or display the weblet icon on the control panel Apps screen, for Displayed on Touch Interface, click **Edit**.
4. To configure the weblet application as the default control panel entry screen, for Default Walk-Up Screen, click **Edit**.
5. To configure user access to the weblet application, for User Permissions, click **Edit**.

Configuring Xerox® App Gallery Settings

You can download weblets from the Xerox Home Page.

To configure Xerox® App Gallery settings:

1. In the Embedded Web Server, click **Apps > Custom Apps > Weblet Management**.
2. In the Installed Weblets area, for Xerox® App Gallery, click **Edit**.
3. To hide or display the Xerox® App Gallery icon on the control panel Apps screen:
   - For Displayed on Touch Interface, click **Edit**.
   - For Xerox® App Gallery, select the check box.
   - Click **Save**.
4. To configure the Xerox® App Gallery as the default control panel entry screen:
   - For Default Walk-Up Screen, click **Edit**.
   - For Default Walkup Screen, from the list, select **Xerox® App Gallery**.
   - Click **Save**.
5. To configure user access to the Xerox® App Gallery:
   - For User Permissions, click **Edit**.
   - On the Non-Logged-In Users tab, in the Permission Role area, for Non-Logged-In User, click **Edit**.
   - Select the Apps and Tools tab.
   - For AppGallery/AppEncrypted, select an option:
     - **Allowed**: This option permits Xerox® App Gallery usage.
     - **Not Allowed**: This option restricts Xerox® App Gallery usage, but its icon appears on the control panel touch screen.

- **Not Allowed & Hidden**: This option restricts Xerox® App Gallery usage and its icon does not appear on the control panel touch screen.

6. Click **Apply**.

Managing Diagnostics and Usage Information

You can send diagnostic information to Xerox or start an online troubleshooting session to help you solve any device issues.

Note: Before you send diagnostic information to Xerox, ensure that you configure Remote Services. For details, refer to Remote Services or Xerox Smart eSolutions.

To manage diagnostics and usage information:

In the Embedded Web Server, click **Support > General**.

- To send diagnostic information to Xerox, click **Send diagnostic Information to Xerox**.
- To send device diagnostics information to Xerox for analysis of detected issues and to match with current solutions, click **Start an Online Troubleshooting Session at www.xerox.com**.
- To download usage information to your local computer, click **Download File to Your Computer**.

Editing Support Settings

You can customize the device support information with your company information. You can use this information to locate assistance or contact your system administrator. You can send diagnostic information to Xerox or start an online troubleshooting session to help you solve any device issues.

1. In the Embedded Web Server, click **Support > General**.
2. Click **Edit Settings**.
3. For Device Administrator, type contact information for your administrator.
4. For Xerox® Support, type information for your Technical Customer Support contact, service contact, and supplies contact. You can include internal locations, telephone contacts, or other information.
5. Click **Apply**.
6. When completed, click **Close**.

A

Audit Log Event Identification Numbers

This appendix contains:

Audit Log Event Identification Numbers

Event Identification Number	Description
1	System startup
2	System shutdown
3	Manual On-Demand Image Overwrite (ODIO) Standard started
4	Manual ODIO Standard (complete)
5	Print job
6	Network scan job
7	Server fax job
8	Internet fax job
9	Email job
10	Audit Log disabled
11	Audit Log enabled
12	Copy job
13	Embedded fax
14	LAN Fax job
15	Data encryption enabled
16	Manual ODIO Full (start)
17	Manual ODIO Full (complete)
18	Data encryption disabled
20	Scan to Mailbox job
21	Delete File/Dir
23	Scan to Home

Event Identification Number	Description
24	Scan to Home job
26	PagePack login
27	PostScript passwords
29	Network user login
30	System admin login
31	User login
32	Service login diagnostics
33	Audit Log download
34	IIO feature status
35	System admin pin changed
36	Audit Log file saved
37	SSL
38	X509 certificate
39	IPsec (enable/disable/configure)
40	SNMPv3
41	IP Filtering rules
42	Network Authentication (enable/disable/configure)
43	Device clock
44	Software upgrade
45	Cloning
46	Scan metadata validation
47	Xerox ® Secure Authentication (enable/disable/ configure)

Event Identification Number	Description
48	Service login copy mode
49	Smartcard access
50	Process terminated
51	ODIO scheduled
53	CPSR backup
54	CPSR restore
55	System Administrator Tools admin access
57	Session Timer log out
58	Session Timer interval change
59	Feature Access Control (configure)
60	Device clock NTP (enable/disable)
61	Grant/revoke admin rights
62	Smartcard (enable/disable/configure)
63	IPv6 (enable/disable/configure)
64	802.1X (enable/disable/configure)
65	Abnormal system termination
66	Local Authentication (enable/disable)
67	Web User Interface Authentication (Enable Network or Local)
68	FIPS 140 mode (enable/disable/configure)
69	Xerox ® Secure Access login
70	Print from USB (enable/disable)
71	USB port (enable/disable)

Event Identification Number	Description
72	Scan to USB (enable/disable)
73	System log download
74	Scan to USB job
75	Remote UI feature
76	Remote UI session
77	Remote Scan feature (TWAIN Driver enable/disable)
78	Remote Scan job submitted
79	Scan to Web Service job completed (TWAIN driver remote scan job)
80	SMTP connection encryption
81	Email Domain Filtering rule
82	Software self test started
83	Software self test completed
84	McAfee Security state
85	McAfee Security event
87	McAfee Agent
88	Digital Certificate import failure
89	User name (add/delete)
90	User name password change
91	Embedded fax job Secure Print passcode
92	Scan to Mailbox folder password change
93	Embedded fax mailbox passcode
94	FTP/SFTP Filing passive mode

Event Identification Number	Description
95	Embedded Fax Forwarding rule
96	Xerox Extensible Interface Platform® Weblets allow install
97	Xerox Extensible Interface Platform® Weblets install
98	Xerox Extensible Interface Platform® Weblets (enable/disable)
99	Network connectivity (enable/disable/configure)
100	Address Book permissions
101	Address Book export
102	SW upgrade (enable/disable)
103	Supplies Plan activation
104	Plan conversion
105	IPv4 (enable/disable/configure)
106	System Administrator password reset
107	Convenience Authentication login
108	Convenience Authentication (enable/disable/configure)
109	Embedded fax passcode length
110	Custom Authentication login
111	Custom Authentication (enable/disable/configure)
112	Billing Impression mode
113	AirPrint (enable/disable/configure)
114	Device Cloning (enable/disable)
115	Save for reprint job

Event Identification Number	Description
116	Web UI Access configure
117	System log push to Xerox
119	Scan to WebDAV job
120	Mopria Print (enable/disable)
121	Point-of-sale credit card API (enable/disable)
122	Point-of-sale data transfer
123	Near Field Communication (enable/disable)
124	Invalid login attempt lockout
125	Protocol audit log (enable/disable)
126	Display device information (configure)
127	Invalid login lockout expires
128	Erase customer data
129	Audit log SFTP scheduled (configure)
130	Audit log SFTP transfer
131	Remote software download (enable/disable)
132	AirPrint & Mopria Scanning (Enable/Disable/ Configure)
133	AirPrint & Mopria Scan Job Submitted
134	AirPrint & Mopria Scan Job Completed
136	Remote Services NVM Write
137	Remote Services FIK Install
138	Remote Services Data Push139
139	Remote Services (Enable/Disable)

Event Identification Number	Description
140	Restore (Enable/Disable)
141	Backup-Restore file downloaded
142	Backup-Restore restore installed
144	User or Group Role Assignment (Added/Removed)
145	User Permission Role (Created/Deleted/Configured)
146	Admin Password Policy Configure
147	Local user account password policy
148	Restricted admin login
149	Grant / revoke restricted admin rights
150	Manual session logout
151	IPP (Enable/Disable/Configure)
152	HTTP Proxy Server (Enable/Disable/Configure)
153	Remote Services Software Download
154	Restricted Admin Permission Role (Created/Deleted/Configured)
155	EIP Weblet Installation Security Policy
156	Lockdown and Remediate Security
157	Lockdown Security Check Complete
159	Send Engineering Logs on Data Push (Enabled/Disabled)

B

External Keyboard

This appendix contains:

You can connect the external keyboard directly to your device using the USB ports. Wi-Fi Direct keyboards are not supported.

Depending on the feature, you can use the external keyboard to navigate fields and manage input.

Note: These keys are not enabled on all screens.

Key	Action
Tab	Moves the cursor from one field to another in the address book
Esc	Cancels input
Enter	Submits input

External Keyboard Shortcuts

You can use shortcuts on the external keyboard instead of buttons on the control panel.

Control Panel Function	Keyboard Shortcut
Home	CTRL+8
Device	CTRL+F3
Reset	CTRL+F5
Log in / Log out	CTRL+F6
Power Saver / Power Off / Restart	CTRL+F7
Language	CTRL+2