VERSION 4.1
JULY 2025
702P09389

Xerox® AltaLink® B8100/C8100 and AltaLink® B8200/C8200 Series Multifunction Printer

System Administrator Guide

xerox™

©2025 Xerox Corporation. All rights reserved.

Xerox®, AltaLink®, SMARTsend®, Xerox Secure Access Unified ID System®, Xerox Extensible Interface Platform®, CentreWare®, and PagePack® are trademarks of Xerox Corporation in the United States and/or other countries.

XMPie® is a trademark of XMPie Inc.

Adobe, Adobe PDF logo, Acrobat, Flash, and PostScript are either registered trademarks or trademarks of Adobe in the United States and/or other countries.

Apache is a trademark of the Apache Software Foundation.

Apple, App Store, AirPrint, Bonjour, iBeacon, iPad, iPhone, iPod, iPod touch, Mac, Macintosh, macOS, and OS X are trademarks of Apple, Inc., registered in the U.S. and other countries and regions.

The Bluetooth® word mark is a registered trademark owned by the Bluetooth SIG, Inc. and any use of such marks by Xerox is under license.

Domino is a trademark of HCL Technologies Limited.

DROPBOX and the Dropbox Logo are trademarks of Dropbox, Inc.

Debian is a registered trademark of Software in the Public Interest, Inc.

Google Drive and Google Chrome are trademarks of Google LLC.

HP®, HP-UX®, JetDirect, and PCL® are trademarks of the Hewlett-Packard Company.

IBM®, AIX®, and PowerPC® are trademarks or registered trademarks of International Business Machines Corporation registered in many jurisdictions worldwide.

IOS is a trademark or registered trademark of Cisco in the U.S. and other countries.

Itanium is a trademark of Intel Corporation or its subsidiaries.

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

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Microsoft Entra ID (formerly know as Azure AD), Microsoft OneDrive, Windows, and Windows Server are trademarks of the Microsoft group of companies.

Mopria is a trademark of Mopria Alliance, Inc.

NetWare® and NDS® are registered trademarks or service marks of Novell, Inc. in the United States and other countries.

SPARC is a registered trademark of SPARC International, Inc. in the United States and other countries.

Sun and Solaris are registered trademarks of Oracle and/or its affiliates.

ThinPrint is a registered trademark of Cortado AG in the United States and other countries.

Trellix, ePolicy Orchestrator, and ePO are trademarks Musarubra US LLC.

UNIX® is a registered trademark of The Open Group.

Wi-Fi® and Wi-Fi Direct® are registered trademarks of Wi-Fi Alliance®.

Wi-Fi Protected Setup™, WPA™, WPA2™, and WPA3™ are trademarks of Wi-Fi Alliance®.

BR41366

Contents

Introduction....17

Overview....18
Configuration Steps....18
More Information....19

Initial Setup....21

Physically Connecting the Printer....22
Installation Wizard....23
Using the Installation Wizard....23
Xerox® Easy Assist App....25
Assigning a Network Address....26
Accessing Administration and Configuration Settings....27
Accessing the Control Panel as a System Administrator....27
Accessing the Embedded Web Server as a System Administrator....28
Using the Search Function in the Embedded Web Server....28
Printing the Configuration Report....29
Initial Setup at the Control Panel....30
Setting the Measurement Units....30
Setting the Date and Time at the Control Panel....30
Configuring Email from App Configuration....30
Configuring the Additional Install Options....31
Configuring Email From Email App....31
Configuring Email From Device App....31
Configuring Email Settings at the Control Panel....32
Installing Optional Software Features....33
Initial Setup in the Embedded Web Server....35
Assigning a Name and Location to the Printer....35
Setting the Date and Time in the Embedded Web Server....35
Using the Configuration Overview Page....36
Restricting Access to the Printer....36
Selecting Apps to Appear on the Touch Screen....38
Installing Optional Software Features....38
Supplies Plan....39
Supplies Plan Activation Code....39
Network Connection Settings....40
Configuring Ethernet Settings....40
Configuring USB Settings....40
Connecting the Device to a Wireless Network....40
Changing the Administrator Password....42
Changing the Administrator Password at the Control Panel....42

Network Connectivity....43

Connecting to a Wireless Network....44

Connecting to a Wireless Network Using the Wireless Wizard....44
Connecting to a Wireless Network in the Embedded Web Server....45
Verifying the Wireless Status and Viewing the Wireless IP Address....47
Configuring Wireless Settings Manually....47
Wireless Troubleshooting....49
Wi-Fi Direct....53
Configuring Wi-Fi Direct....53
Disabling Wi-Fi Direct....53
Dynamic Frequency Selection (DFS)....54
AirPrint....55
Configuring AirPrint....55
Enabling iBeacon for AirPrint Discovery....57
Bonjour....60
Mopria....61
Configuring Mopria....61
Universal Print....63
Universal Print Status....63
Registering a Device for Universal Print....63
Administrator Functions for Universal Print....65
Setting Up Universal Print on macOS....65
Xerox® Workplace Cloud....67
USB Settings....69
Configuring Power in Sleep Mode....69
FTP/SFTP Client....71
Configuring FTP and SFTP Client Settings....71
HTTP....72
Enabling HTTP at the Control Panel....72
Configuring HTTP Settings in the Embedded Web Server....72
Web Browser Certificate Validation Information and Tips....73
Accessing HTTP Web Services....74
HTTP Web Services....74
Accessing HTTP Advanced Settings....75
HTTP Advanced Settings....75
IP....76
Enabling TCP/IP....76
Configuring the Network Address Manually at the Control Panel....76
Configuring DNS Settings at the Control Panel....76
Configuring IP Settings in the Embedded Web Server....77
IPP....83
Configuring IPP....83
LDAP....85
Adding LDAP Server Information....85
Managing LDAP Servers in the Embedded Web Server....85
Configuring LDAP Server Optional Information....85
Configuring a Secure LDAP Connection....86
LDAP Server Contexts....87

Configuring LDAP User Mappings 87
LDAP Custom Filters 88
LPR/LPD 90
NFC 91
NTP 92
POP3 93
Proxy Server 94
Configuring the Proxy Server 94
Raw TCP/IP Printing 96
Configuring Raw TCP/IP Settings 96
Configuring Raw TCP/IP Advanced Settings 96
SLP 98
Configuring SLP 98
ThinPrint Client 99
ThinPrint Client Certificate Requirements 99
Configuring a ThinPrint Client 99
SMB Filing 101
Configuring Kerberos Authentication Options for SMB 101
SMTP Server 102
Configuring SMTP Server Settings 102
Configuring SMTP Authentication Settings 102
Configuring SMTP Connection Encryption Settings 103
Configuring SMTP File Size Management 103
Testing SMTP Configuration Settings 103
SNMP 104
Enabling SNMP 104
Configuring SNMPv1/v2c 104
SNMPv3 105
Configuring SNMP Advanced Settings 106
WSD 107
Enabling WSD 107

Security 109

Setting Access Rights 110
Authentication 111
Setting the Login Method for the Control Panel 112
Setting the Login Method for the Embedded Web Server 113
Configuring Local Authentication Settings 114
Configuring Network Authentication Settings 118
Configuring Convenience Authentication Settings 121
Configuring Xerox Workplace Cloud Authentication Settings 123
Configuring Xerox Secure Access Unified ID System® Authentication Settings 124
Configuring Identity Provider (IdP) - Validate on Cloud Authentication Settings 127
Configuring Smart Card Authentication Settings 130
Configuring Custom Authentication Settings 136
Setting Up Fallback Login 137

Authorization....138
Setting the Authorization Method....138
User Permissions....140
Personalization....148
Enabling Personalization....148
Viewing and Deleting Personalization Profiles....149
Imaging Security....150
Infrared Security....150
Jobs Detected....153
HTTPS (TLS)....155
Using TLS for all HTTP Communication (HTTPS)....155
FIPS 140....156
FIPS 140 Mode....156
FIPS 140 Mode with Common Criteria Compliance....156
FIPS 140 Enablement Workflow and Configuration Checks....157
Enabling FIPS 140 Mode and Checking for Compliance....157
FIPS 140 Configuration Check....158
FIPS 140 Status....158
TLS....160
Stored Data Encryption....162
Enabling Encryption of Stored Data....162
IP Filtering....163
Creating or Editing an IP Filter Rule....163
Editing an IP Filter Rule....163
Arranging the Execution Order of IP Filter Rules....164
Logs....165
Audit Log....165
Authentication Log....167
Network Troubleshooting....168
SIEM....170
Support Logs....172
Trellix® Embedded Control....175
Setting the Security Level....176
Setting the Alert Options....176
Trellix ePolicy Orchestrator Server....177
Downloading the Audit Log....177
Testing Your Alert Configuration....177
Feedback Method Test Results....177
IPsec....178
IPsec Configuration Components....178
Managing Security Policies....178
Managing Host Groups....179
Managing Protocol Groups....179
Managing Actions....180
Enabling IPsec....184
Security Certificates....185

Installing Certificates....185
Creating and Installing a Xerox® Device Certificate....186
Installing the Device Root Certificate Authority....186
Creating a Certificate Signing Request....188
Installing Root Certificates....189
Installing Domain Controller Certificates....190
Viewing, Saving, or Deleting a Certificate....191
Specifying the Minimum Certificate Key Length....191
802.1X....193
Enabling and Configuring 802.1X in the Embedded Web Server....193
System Timeout....196
Setting System Timeout Values....196
USB Port Management....197
USB Port Management at the Control Panel....198
Image Overwrite Security for HDD Storage Devices....200
Immediate Job Overwrite....200
Disk Overwrite....201
Job Data Removal for SSD Storage Devices....205
Removing Job Data Now....205
Scheduling Job Data Removal....206
PostScript® Passwords....208
Enabling or Creating PostScript Passwords....208
Personalized Information....209
Verifying the Software....210
Restricting Print File Software Updates....211
Specifying Email Recipient Restrictions....212
Administrator Password....213
Enabling the Administrator Password Reset....213
Disabling the Administrator Password Reset....213

Printing....215

Paper Management....216
Setting Default Paper Type and Color....216
Enabling Required Paper Policies....216
Setting Paper Size Preference....217
Configuring Tray Settings....218
Selecting Tray 1 Settings....219
Configuring Custom Media Types....220
Saving and Reprinting Jobs....222
Enabling the Reprint Saved Jobs Feature....222
Creating and Managing Saved Jobs Folders....222
Saving and Printing Jobs....223
Backing Up Saved Jobs....223
Restoring Saved Jobs from an FTP Repository....224
Printing Jobs from the Embedded Web Server....225

Configuring General Print Settings 226
Printing an Error Sheet 227
Managing Banner Page Printing Options 228
Enabling Banner Page Printing in the Embedded Web Server 228
Enabling Banner Page Printing at the Control Panel 228
Enabling Banner Page Printing in the V3 Print Driver 228
Configuring Secure Print Settings 230
Configuring Secure Print Device Policies 230
Configuring Secure Print Driver Defaults 230
Hold All Jobs 232
Configuring the Hold all Jobs Feature 232
Showing Printer Font Information 233
Page Description Languages 234
PostScript® 234
PCL 234
PDF 236
TIFF/JPG 238
UNIX, Linux, and AS/400 Printing 240
Xerox® Printer Manager 240
Printing from a Linux Workstation 241
Adding the Printer 241
Printing with CUPS 241
AS/400 242
Configuring Print From 243
Cloud Browsing Enablement 243
Enabling Print From Mailbox 244
Enabling Print From USB 245
Allowing Users to Interrupt Active Print Jobs 246
Specifying Output Settings at the Control Panel 247
Specifying Print Settings Defaults and Policies 248

Copying 251

Copy Overview 252
Specifying Default Copy Settings 253
Setting Copy Feature Defaults at the Control Panel 254
Setting Copy Presets 255
Setting the Color Preset Screen 255
Setting Edge Erase Presets 255
Setting Image Shift Presets 256
Setting Reduce/Enlarge Presets 256
Disabling Automatic Image Rotation 256
Setting ID Card Copy Feature Defaults 258
Specifying Output Settings 259

Scanning 261

Scanning to an Email Address....262
Configuring Email....262
Workflow Scanning....269
Enabling Workflow Scanning....269
Configuring File Repository Settings....269
Configuring the Default Workflow....274
Configuring Workflow Scanning General Settings....275
Configuring Single-Touch App....276
Configuring Custom File Naming....276
Setting Workflow Display Settings for the Control Panel....277
Enabling Remote Scanning Using Remote Scan Start....277
Configuring a Validation Server....278
Configuring Workflow Pool Repository Settings....279
Configuring Unspecified Defaults....279
Managing Scan Workflows....279
Scanning to a Folder on the Device....282
Enabling or Disabling Scan To Mailbox....282
Setting Scan Policies....282
Managing Folders and Scanned Files....283
Scan To USB....286
Enabling Scan To USB....286
Scanning to a User Home Folder....287
Configuring Scan To....289
App Defaults....289
Remote Destinations....290
Print Scanned Document Settings....292
Email Required....293
Metadata....293
Shared Email Settings....300
Address Books....300
Security....301

Faxing....303

Fax Overview....304
Fax....305
Configuring Required Fax Settings at the Control Panel....305
Configuring Embedded Fax Settings....305
Fax Security....306
Setting Fax Defaults....306
Setting Fax Feature Defaults....309
Fax Forwarding....309
Fax Mailboxes....311
Fax Reports....312
Server Fax....315
Configuring a Server Fax Filing Repository....315
Configuring Server Fax General Settings....318
Configuring Server Fax Settings....318

Configuring Server Fax Image-Quality Settings....318
Configuring Layout Adjustment Settings....319
Configuring Server Fax Filing Options....319
LAN Fax....320

Accounting....321

Xerox® Standard Accounting Tool....322
Enabling Xerox Standard Accounting....322
Setting Service Tracking Options....322
General and Group Accounts....322
Adding a User and Setting Usage Limits....323
Managing User Information....324
Assigning Users to an Account....326
Usage Limits....327
Configuring Validation Policies and Print Job Exceptions....328
Network Accounting....330
Enabling Network Accounting....330
Setting Network Accounting Workflow Options....330
Configuring Job Limits Server Settings....330
Disabling the Job Limits Web App....331
Configuring User Prompts....331
Configuring Validation Policies and Print Job Exceptions....332
Accounting Using an Auxiliary Access Device....334
Enabling Accounting Using an Auxiliary Access Device....334
Displaying Your Company Logo on the Blocking Screen....334
Setting the Auxiliary Device Type....335
Selecting Apps to Restrict or Track....335
Setting the Job Timeout....335
Specifying Double Count Large Impressions....335
Premium Select....336
Enabling Accounting in Print Drivers....337
Enabling Accounting in a Windows V3 Print Driver....337
Enabling Accounting in an Apple Macintosh Print Driver....337
Printing a Copy Activity Report....338

Administrator Tools....339

Viewing Device Status and Configuring Apps....341
Display Device Information....343
Quick Access....344
Accessibility....345
Inverting Display Color for the Control Panel....345
Remote Control Panel Speech Output....345
Customizing Device Contact Information....346
Configuring Alerts....347
Control Panel Alerts....347
Email Alerts....348

Status LED and Sounds 348
Energy Saving Settings 351
Setting Energy Saver Mode 351
Smart Proximity Sensor 353
Screen Saver 354
Power in Sleep Mode 355
Remote Control Panel 357
Entry Screen Defaults 358
Setting the Default Walk-up Screen 358
Setting the Default Screen when Originals are Detected 358
Enabling the Auto Start when Originals are Detected Feature 359
Remote Services 360
Configuring Remote Services 360
Policies and Schedule 360
Remote Management Server Setup 362
Configuring a Remote Management Server Connection 362
Security Dashboard 363
Authentication 363
Confidentiality 364
Integrity 364
Availability 364
Quick Links 365
Fleet Orchestrator 366
Automatic File Sharing 366
Cloning 386
Creating and Installing a Clone File in the Embedded Web Server 386
Creating a Clone File on a USB Flash Drive 386
Installing a Clone File from a USB Flash Drive 386
Language and Keyboard 388
Setting Language and Keyboard Options 388
Backup and Restore Settings 390
Setting the Security Installation Policy for Backup and Restore 390
Restoring Settings 390
Creating a Manual Backup File that is Stored on the Device 391
Creating and Downloading a Backup File 391
Deleting a Backup File 391
Supplies 392
Details 392
Order Supplies 392
Billing Impression Mode 393
Changing the Billing Impression Mode 393
Address Books 394
Device Address Book 394
Network Address Book 398
LAN Fax Address Book 399
Font Management Utility 400

Network Logs..... 401
Downloading a Network Log..... 401
Downloading a Network Log to a USB Flash Drive..... 401
Restarting the Device in the Embedded Web Server..... 402
Restarting the Device at the Control Panel..... 403
Taking the Device Offline..... 404
Erase Customer Data..... 405
Resetting the User Interface to Factory Default Settings..... 406
Reverting to Previous Settings..... 407
Updating the Device Software..... 408
Updating the Software in the Embedded Web Server..... 408
Manually Updating the Software Using a USB Flash Drive..... 408
Updating Card Reader Firmware..... 409
Adjusting Color, Image, and Text Detection Settings..... 411
Test Drive..... 412
Enabling Test Drive Features in the Embedded Web Server..... 412
Accessing Test Drive Features at the Control Panel..... 412
Web-Based Configuration Using the Control Panel..... 412
Configuring Lockdown Security Solution..... 414
Configuration Watchdog..... 416
Configuration Watchdog Status..... 416
Configuring Settings for Features to Be Monitored..... 417
Selecting Features to Monitor..... 417
Setting the Check Frequency..... 418
Email Notification..... 419

Customization and Expansion..... 421

Xerox Extensible Interface Platform® (EIP)..... 422
Configuring Extensible Services..... 422
Extensible Service Scan Settings..... 424
Extensible Service Diagnostics..... 424
Extensible Service Setup for Apps..... 424
Extensible Service Advanced Setup..... 425
Auxiliary Interface Kit..... 427
Driver Download Link..... 428
Customizing or Hiding the Driver Download Link..... 428
Customizing the Home Screen in the Embedded Web Server..... 429
App Enablement..... 429
Setting the Display Order for Apps..... 430
Customizing the Home Screen at the Control Panel..... 431
Setting the Default Walk-Up Screen at the Control Panel..... 431
Setting the Default Screen when Originals are Detected at the Control Panel..... 431
Rearranging Apps on the Home Screen..... 431
Displaying or Hiding an App on the Home Screen..... 432
Deleting an App from the Home Screen..... 432

Customizing App Features 433
Customizing App Default Settings 433
Removing App Customization Settings 433
Removing Customization from the Home Screen 434
1-Touch Apps 435
Public 1-Touch Apps 435
Private 1-Touch Apps 435
Creating a 1-Touch App 436
Adaptive Learning 438
Suggest Personalized App Workflows 438
Automatically Set Device Defaults 439
Setting Defaults and Policies for Scan Services 441
Setting the Filename Extension 441
Setting Duplex Color Scanning Options 441
Disabling Multifeed Detection 442
Creating a Custom Scan App 443
Creating a Custom Single-Touch Scan App Overview 443
Creating a Single-Touch Scan App 443
Customizing and Configuring Your App 443
Locking or Hiding Your App from Appearing on the Control Panel 445
Weblet Management 446
Setting the Security Policy for Unencrypted Weblets 446
Enabling Weblet Installation in the Embedded Web Server 447
Enabling Weblet Installation at the Control Panel 447
Installing a Weblet in the Embedded Web Server 447
Installing a Weblet at the Control Panel 447
Troubleshooting a Weblet Installation 447
Configuring Weblet Settings 448
Configuring Xerox® App Gallery Settings 449
Configuring Xerox® XMPie App 449
Configuring an EIP Authentication App 450
Deleting a Weblet 451
Managing Diagnostics and Usage Information 452
Editing Support Settings 453

Audit Log Event Identification Numbers 455

Audit Log Event Identification Numbers 456

External Keyboard 465

External Keyboard Shortcuts 466

Introduction

This chapter contains:

Overview 18
More Information 19

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:

- Not all features are supported on all devices. Some features apply only to a specific device model, configuration, operating system, or driver type.
- 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	Go to www.xerox.com/office/support, then select your specific printer model.
Recommended Media List	United States: www.xerox.com/rmlna Europe: www.xerox.com/rmleu
Technical support information for your printer, including online technical support, Online Support Assistant, and print driver downloads.	Go to www.xerox.com/office/support, then select your specific printer model.
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 documentation	In the Embedded Web Server, click **Help**.
Order supplies for your printer	Go to www.xerox.com/office/supplies, then select your specific printer model.
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/office/register
Xerox® Direct online store	www.direct.xerox.com/
Third party and open source software	To locate third party and open source software disclosure notices and the terms and conditions, go to www.xerox.com/office/support, then select your specific printer model.

Initial Setup

This chapter contains:

Physically Connecting the Printer 22
Installation Wizard 23
Xerox® Easy Assist App 25
Assigning a Network Address 26
Accessing Administration and Configuration Settings 27
Initial Setup at the Control Panel 30
Initial Setup in the Embedded Web Server 35
Network Connection Settings 40
Changing the Administrator Password 42

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.

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

If the Auto-Assembly feature is enabled for your organization in Fleet Orchestrator, in the Installation Wizard, a device can join the Publisher automatically. After a device joins the fleet, the device checks for a clone file automatically. For more information, refer to Fleet Orchestrator.

To use the initial Installation Wizard:

1. To select a language, the date and 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, or Wireless Network Adapter, is connected securely.

2. Complete the Additional Install Options fields.
   - 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 fields later.

3. To complete the configuration using a clone file, follow the steps in this task. To complete the configuration without using a clone file, skip to step 4.

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.

Note: If your clone file contains an administrator password, the password in the clone file replaces the default administrator password.

4. To complete the installation without a clone file:

a. For Paper Size Preference, set the paper size.

b. For Device Information, select a 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 first attempt to log in to the Embedded Web Server with the default administrator password, the device prompts you to change the password. For details, refer to Accessing the Embedded Web Server as a System Administrator.

5. At the Device Setup Complete screen, follow the onscreen instructions, then click **Restart**.

Xerox® Easy Assist App

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

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

The Xerox Easy Assist App has instructions and videos that help you to unpack the printer from its shipping box. You can complete the initial setup of a new printer through the app. To install the Xerox Easy Assist app on your smartphone, scan the QR Code that is provided in the *Installation Guide*. If the printer has Internet connection, then you can connect to the XEA app in your smartphone by typing the IP address of the printer.

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

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

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.

Accessing Administration and Configuration Settings

You can access the administration and configuration settings from the Tools menu at 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 on or power off the device 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.

Note: If there is a power outage, the printer will power on automatically when power is restored without using the **Power/Wake** button. But if the printer was off when the power outage occurred, the printer will remain off and it would require to press the **Power/Wake** button to power on the printer. This is applicable only to ALC82XX and ALB82XX series printers.

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

The administrator password is required to access 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 Tools menu at the control panel.

ACCESSING THE CONTROL PANEL AS A SYSTEM ADMINISTRATOR

If you have not changed the administrator password, you can continue to access the administrator functions at the control panel with the default administrator password. The default administrator password is the device serial number.

Note: You can obtain the serial number from inside the front door of the printer, from the configuration report, and from the home page of the Embedded Web Server.

To access the administrator functions at the control panel:

1. At the control panel touch screen, touch **Log In**.
2. Type **admin**, then touch **Next**.
3. Type the administrator password, then touch **Done**. The password is case-sensitive.

ACCESSING THE EMBEDDED WEB SERVER AS A SYSTEM ADMINISTRATOR

Before you begin:

- Locate your device IP address, or host and domain name, 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 administrator password is the device serial number. The password is case-sensitive.

   Note: You can obtain the serial number from inside the front door of the printer, from the configuration report, and from the home page of the Embedded Web Server.

5. Click **Login**.

   Note: If you did not change the administrator password with the installation wizard, a prompt asks you to change the default administrator password when you first log in as administrator in the Embedded Web Server. If you choose to continue to use the default administrator password, or a password of `1111`, each time you log in as administrator, a prompt reminds you to choose a more secure password for the admin account. 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 many of the important current settings of the printer. A configuration report prints at start-up by default.

There are two configuration reports available, a **Basic Configuration Report**, and a **Detailed Configuration Report**. The configuration reports provide product information, including installed options, network settings, port setup, tray information, and more.

Printing the Configuration Report from the Control Panel

To print the Configuration Report from the device control panel:

1. At the Home screen, touch **Device**, then touch **Information Pages**.
2. Touch **Basic Configuration Report** or **Detailed 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**, then click **Basic Report** or **Detailed Report**.
   - Basic Report: This report provides the basic information of the printer configuration. The Basic Report is printed on a single 2-sided page.
   - Detailed Report: This report provides the detailed information of the printer configuration. The Detailed Report is printed on multiple 2-sided pages.

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 Basic Report at Power on**.
4. To save the new settings, click **Save**.

Initial Setup at the Control Panel

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**.

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**.

CONFIGURING EMAIL FROM APP CONFIGURATION

You can change the printer configuration settings for email or fax using the App Configuration.

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **Device Settings > App Configuration**.
3. To start a wizard, touch **Email** or **Fax Setup**.
   If Email is not configured, then an alert `Email is not configured for this device. Setup email for all users?` message appears. Click **Continue**. For more details, refer to Configuring Email Settings at the Control Panel.
4. Follow the onscreen instructions.

Note: If email is configured to use DNS to identify SMTP server, a `Email is using DNS to identify the SMTP sever` message appears.

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** or **Contact Numbers**, or **Fax Setup**.
4. Follow the onscreen instructions.

CONFIGURING EMAIL FROM EMAIL APP

1. At the control panel touch screen, touch **Email**.
2. Following are the conditions to check the email configuration status:
   - If Email is configured, it allows to navigate into the Email settings.
   - If Email is not configured, then an alert `Email is not configured for this device. Setup email for all users?` message appears. Click **Continue**. For more details, refer to Configuring Email Settings at the Control Panel.
   - If Email is locked and configured, it prompts to enter the login credentials.
   - If Email is locked and not configured, then an alert `Email is not configured for this device. Setup email for all users?` message appears. Click **Continue**.

     Enter the login credentials. For more details, refer to Configuring Email Settings at the Control Panel.
3. If the email configuration is successful and if you do not have permission to access email, then click **Email** App in the Home screen.
   An alert `Email is configured; however, your access is restricted.` message appears.

Note: If email is configured to use DNS to identify SMTP server, a `Email is using DNS to identify the SMTP sever` message appears.

CONFIGURING EMAIL FROM DEVICE APP

1. At the control panel touch screen, touch **Device**, then touch **Tools**.

2. Touch **App Settings > Email App > Email Setup**.
   - If email is configured, the complete Email Setup summary screen is displayed.
   - If email is not configured, then follow the onscreen instructions. For more details, refer to Configuring Email Settings at the Control Panel.

Note: If email is configured to use DNS to identify SMTP server, a `Email is using DNS to identify the SMTP sever` message appears.

CONFIGURING EMAIL SETTINGS AT THE CONTROL PANEL

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **App Settings > Email App > Email Setup**.
3. For Account Provider, select an Email Provider.
   - If the Email Provider is selected as **iCloud**, then check the connection.
     - If the connection is successful, then Send New Messages From screen appears. Follow the onscreen instructions and enter the required email address.
     - If the connection is not successful, an alert `Unable to connect to mail server. Would you like to setup a proxy server?` message appears. To continue, perform any one of the following:
       - **Cancel**: This option allows to navigate to the previous screen to select a different Account Provider.
       - **Setup Proxy Server**: This option allows to setup proxy in Proxy Server screen.
       - **Continue Without Connection**: This option allows to navigate to Send New Messages From screen.

     If **iCloud** is selected as Account Provider, then SMTP Server and Port details are not displayed in the Email Setup screen.
   - If the email provider is selected as **Other Email Account**, an Email Setup screen appears to customize the email configuration as required.
4. For SMTP Server, perform the following:
   a. For address type, select an option.
      - **IPv4 Address**: Enter the IPv4 address in SMTP Address screen.
      - **IPv6 Address**: Enter the IPv6 address in SMTP Address screen.
      - **Host Name**: Enter the host name in SMTP Address screen.

   b. Type the appropriately formatted address.
   c. Click **OK**.
5. For Port, type the appropriate port number, then click **OK**.

6. For Send Emails, select an option.
   - **No login Credentials**: This option displays only the email address and hides the password in the Email Setup screen.
   - **One login for all messages**: This option displays both the email address and the password in the Email Setup screen. It also prompts for the required credentials to be entered.

   Note: The entered password is always displayed as bullets in the Email Setup screen.

   - **Logged-in user's credentials**: This option displays the already configured email address of the logged-in user in the Email Setup screen.

   Note: If logged-in user is not configured through the Embedded Web Server, then an alert `Logged-in user authentication can only be configured at the Embedded Web Server` message appears.

   - **Login prompt for each message**: This option hides both the email address and the password in the Email Setup screen.
7. For Encryption Connection, select an option.
   - **No Encryption**: This option do not display **Validate Server Certificate** option in the Email Setup screen.
   - **STARTTLS (if available)**: This option displays **Validate Server Certificate** option in the Email Setup screen.
   - **STARTTLS**: This option displays **Validate Server Certificate** option in the Email Setup screen.

   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.
8. Click **Done**.

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.

   Note: Contact a Xerox representative to get a Feature Installation Key.

   There are two types of keys:

   - **Permanent Key**: This key is 12-digit long. You can use dashes or spaces without affecting the entry of the key. For example, 1234-5678-9011.
   - **Expiring Key**: This key is 18-character long. For example, abcj 1234 5678 r12# 7p.

4. Touch **OK**.

Initial Setup in the Embedded Web Server

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. The default Device Name is made with the Manufacturer name, Model name, and partial MAC Address.
   A Host Name is different from the Device Name.
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**.

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.
5. For **Time threshold for triggering device re-sync with NTP**, select a time in seconds. The range is 10–150 seconds. The default value is 110 seconds.

   Note: Changes to these settings cause the printer to restart.
6. 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.
7. For **Time Zone**, select your time zone from the menu.

8. 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.

9. 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.

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**.

SELECTING APPS TO APPEAR ON THE TOUCH SCREEN

Standard apps are installed and enabled on the device by default. Optionally, you can install EIP and weblet apps, which provide extra functionality. For details, refer to Weblet Management.

The Enablement option allows the administrator to disable or enable apps that appear on the control panel touch screen and the Embedded Web Server.

Note: It is not possible to disable the Jobs and Device apps, and apps that are set as entry-screen defaults.

For an app to be available for customization and personalization at the control panel, enable the app. To customize app features, refer to Customizing the Home Screen at the Control Panel.

Enabling Apps

To enable or disable apps:

1. In the Embedded Web Server, click **Properties > Apps > App Enablement**.
2. To enable or disable an app, on the App Enablement page, click the check box next to the app. A check mark indicates that the app is enabled.
3. Click **Apply**.
4. To verify that the required apps are enabled, click the **Home** tab. Enabled apps are listed in the Apps area of the device Home page.

Arranging the Display Order for Apps

To arrange the display order for apps on the control panel touch screen:

1. In the Embedded Web Server, click **Properties > Apps > Order**.
2. Select, drag, then drop the icons on the screen until they are in the preferred order.
3. 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.

   Note: Contact a Xerox representative to get a Feature Installation Key.

   There are two types of keys:

   - **Permanent Key**: This key is 12-digit long. You can use dashes or spaces without affecting the entry of the key. For example, 1234-5678-9011.
   - **Expiring Key**: This key is 18-character long. For example, abcj 1234 5678 r12# 7p.
5. Click **Apply**.

SUPPLIES PLAN

The Supplies Plan page in the Properties tab provides details about the Supplies Plan, Supplier, and Details of ordered supplies.

- In the Supplier Plan area, if a Supply Plan has not been set up and if you have received a key to set one up, to add a plan or install a feature, click **Add Plan/Install Feature**.
- In the Supplier area, to add a supplier, click **Add Supplier**. Enter the supplier details, such as Supplier Name, Contact Information, Phone Number, and Website URL, then click **Add**. If the user needs to delete the existing supplier, click **Edit**, then click **Delete Supplier**.

  To order supplies, go to the Order Supplies page. For more information, refer to Order Supplies.
- In the Details area, details of supplies, such as Serial Number, Impression, and Sequence are displayed.
- For other plan options, click **Other plan options**.

Note: Plan Conversion can be done using Feature Installation Key (FIK) or a Supply Plan Key.

SUPPLIES PLAN ACTIVATION CODE

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

Xerox® PagePack® is a cost-per-page-based program 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**.

You can also activate supplies and service plans from the control panel. To activate PagePack® Supplies Plan from the control panel, touch **Device > Tools > Device Settings > Supplies > Enter PagePack Activation Code**.

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

Network Connection Settings

You can configure wired and wireless network connections for your device. You can manage settings for USB Type A and Type B ports.

For all connectivity settings, refer to Network Connectivity.

CONFIGURING ETHERNET SETTINGS

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. If the device does not recognize your network speed, the device can prevent a connection to the network, and your switch or router can report errors.

If the device does not recognize your network speed, set the rated speed. The rated speed is the maximum speed at which you expect your network to operate.

To verify that the printer detects the correct network speed, refer to the Configuration Report.

1. In the Embedded Web Server, click **Properties > Connectivity > Setup**.
2. In the Profile area, for Wired Connection, click **Edit**.
3. On the Wired Profile page, to configure Ethernet settings, for Ethernet, click **Edit**.
4. On the Ethernet page, for Rated Speed, select a connection speed.

   To return all network settings to factory-default settings, click **Default All**.
5. Click **Save**.

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

CONFIGURING USB SETTINGS

1. In the Embedded Web Server, click **Properties > Connectivity > Setup**.
2. In the USB Settings area, configure settings as needed:
   - To enable or disable USB Type A and Type B ports or to manage USB Type B port policies, for Port Management (A and B), click **>**. For details, refer to USB Port Management.
   - To configure power saver settings, for Power in Sleep Mode, click **>**. For details, refer to Configuring Power in Sleep Mode.

   The Status area displays the current settings for each feature.

CONNECTING THE DEVICE TO A WIRELESS NETWORK

If you have purchased the Xerox® 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. 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.

Changing the Administrator Password

The user name for the administrator account is `admin`.

The default administrator password is the device serial number.

Note: You can obtain the serial number from inside the front door of the printer, from the configuration report, and from the home page of the Embedded Web Server.

If you have not changed the default administrator password, a prompt asks you to change the password when you first log in as administrator in the Embedded Web Server. If you choose to continue to use the default administrator password, or a password of `1111`, each time you log in as administrator, a prompt reminds you to choose a more secure password for the admin account.

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.

To change the administrator password in the Embedded Web Server:

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

CHANGING THE ADMINISTRATOR PASSWORD AT THE CONTROL PANEL

If you have not changed the administrator password, you can continue to access the administrator functions at the control panel using the default administrator password. The default administrator password is the device serial number.

To change the 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. All passwords are case-sensitive.
4. Type the new password, then retype the new password.
5. Touch **OK**.

Network Connectivity

This chapter contains:

Connecting to a Wireless Network 44
Wi-Fi Direct 53
AirPrint 55
Bonjour 60
Mopria 61
Universal Print 63
Xerox® Workplace Cloud 67
USB Settings 69
FTP/SFTP Client 71
HTTP 72
IP 76
IPP 83
LDAP 85
LPR/LPD 90
NFC 91
NTP 92
POP3 93
Proxy Server 94
Raw TCP/IP Printing 96
SLP 98
ThinPrint Client 99
SMB Filing 101
SMTP Server 102
SNMP 104
WSD 107

Connecting to a Wireless Network

If you have purchased the Xerox® 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.

The Xerox® Wireless Network Adapter supports:

- Wi-Fi Bands: Dual Band 2.4 GHz and 5 GHz
- Network Standards:
  - 802.11ac
  - 802.11n
  - 802.11b/a/g
- Wi-Fi Direct

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

Note:

- Not all Xerox® Wireless Network Adapters are compatible with all Xerox® printers. Ensure that you purchase the correct Xerox® Wireless Network Adapter kit for your device. For more information, contact your Xerox representative.
- For more information about installing the wireless network adapter, 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 manually to a wireless network.

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.

Note: For some solutions, Bluetooth functionality is included with the wireless hardware solution.

2. From the Wireless Installation Wizard, 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 as 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 mode requires authentication, enter the credentials, then 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 and configures the security mode for the wireless network as follows:
   - For WPA2 Personal or WPA2 Enterprise, the device optionally supports the Protected Management Frames (PMF) and by default, the device is configured with PMF disabled. For details, refer to Wireless Protected Management Frames.
   - For WPA3 Personal or WPA3 Enterprise, the device supports Protected Management Frames and by default, the device is configured with PMF required. For details, refer to Wireless Protected Management Frames.

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. The Auto option detects the algorithm automatically that your wireless network uses.
   - For Authentication Method, select the authentication method that your wireless network uses.
   - For Server Validation - Validate server using, select the validation server root certificate that you want to use.

   Note: Install the validation server root certificate on the Security Certificates page at **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.

   Note: 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.
10. After you configure the wireless settings, from the Wireless Settings page, click **Close**.
11. From the Wireless Profile page, click **Close**.
12. To activate wireless settings and simultaneously disable the Wired Connection setting, for Xerox Wireless Network Interface, click **Make Active**.
13. On the confirmation screen, select **Activate Wireless**.

Wireless Protected Management Frames

Wireless Protected Management Frames (PMF), also known as 802.11w, provide protection for unicast and multicast management action frames.

- Unicast management action frames are protected from eavesdropping and forging.
- Multicast management action frames are protected from forging.

Note: PMF is not applicable to the device Wi-Fi Direct connection.

For Protected Management Frame (PMF), select an option:

- **Off**: This option indicates that the device does not support PMF.
- **Optional**: This option enables the device to use PMF based on the Access Point (AP) or router configuration. If the AP supports PMF, the device uses PMF. If the AP does not support PMF, the device does not use PMF.
- **Required**: This option instructs the device to use PMF.

Caution: Both the wireless network and the device need to support PMF for the capability to function. Misalignment between the wireless network and the device for this setting can result in communication failures.

Note: For few security modes, PMF is optional, while for others, it is required.

PMF configuration for security modes for the wireless network connections are as follows:

- **WPA2 Personal or WPA2 Enterprise**: For this security mode, the device optionally supports Protected Management Frames and by default, the device is configured with PMF disabled.
- **WPA3 Personal or WPA3 Enterprise**: For this security mode, the device supports Protected Management Frames and by default, the device is configured with PMF required.
- **WPA3 Personal Transition**: For this security mode, the device supports Protected Management Frames and by default, the device is configured with PMF optional.
- **WPA3 Enterprise 192-Bit**: For this security mode, the device supports Protected Management Frames and by default, the device is configured with PMF optional.

Note: WPA3 Enterprise 192-Bit is not supported on all devices.

Limit Wi-Fi Roaming

Use this optional feature to limit Wi-Fi roaming for discovered networks.

Enterprise wireless networks can be configured with multiple Base Station IDs, known as BSSIDs, that can advertise a single network name or SSID. When a device connects to the SSID, the device can connect to an access point (BSSID) that can have a weaker signal or be on a different subnet.

To curtail unexpected roaming, you can define a roaming boundary within the SSID that is determined by a set of specific BSSIDs. To define the boundary, you can specify up to three BSSIDs.

Note:

- During normal operation, the device connects to any available BSSID within the selected SSID.
- To restrict Wi-Fi roaming, you can select up to three preferred BSSIDs within the selected SSID network.

Caution: BSSIDs are location-specific. If you reconfigure the network or move the device, review the settings, then change the settings as needed.

To select preferred BSSIDs:

1. Click **Show Settings**.
2. From the list, select up to three BSSIDs. To refresh the list, click **Refresh List**.
3. Click **Save**.

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, then provide information about your wireless network.

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

If the network that you are connecting to is a hidden, non-advertised network, the hidden network is not discoverable in a network scan. To configure hidden wireless network settings, use the Manual Connections page in the Embedded Web Server.

Note: To connect manually to a hidden network, you need to know the exact network name (SSID) and configuration parameters.

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 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 previously to a wireless network, 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. The Auto option detects the algorithm automatically 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**.

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 (SSID), type the name of your network.
8. For Security Mode, select the security method that your wireless network uses.
9. Select the required security mode configurations for the wireless network connections.
   - For WPA2 Personal or WPA2 Enterprise, the device optionally supports the Protected Management Frames (PMF) and by default, the device is configured with PMF disabled. For details, refer to Wireless Protected Management Frames.
   - For WPA3 Personal or WPA3 Enterprise, the device supports Protected Management Frames and by default, the device is configured with PMF required. For details, refer to Wireless Protected Management Frames.
10. 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. The Auto option detects the algorithm automatically that your wireless network uses.
    - 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.

    Note: To install the validation server root certificate on the Security Certificates page, click **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.

    Note: To install the device certificate on the Security Certificates page, click **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.
11. Click **Save**.
12. To navigate back to the Setup page, click **Properties > Connectivity > Setup**.
13. For Xerox Wireless Network Interface, click **Make Active**.

WIRELESS TROUBLESHOOTING

Wireless performance varies significantly due to many factors that are specific to wireless technology.

To improve performance, you can mitigate the effect of certain factors:

- Improve the wireless signal strength. For details, refer to Wireless Signal Strength.
- Minimize the effects of network usage and access point loading. For details, refer to Network Usage and AP Loading.
- Reduce Radio Frequency interference. For details, refer to Radio Frequency Interference.
- Limit roaming on Enterprise wireless networks. For details, refer to Limit Wi-Fi Roaming.

Wireless Network Adapter

If the wireless network adapter is not recognized by the device:

- Ensure that the USB port to which the Wireless Adapter is connected is enabled. For details, refer to USB Port Management.
- Ensure that the Wireless Adapter and, if applicable, the extension cable connected to the Wireless Adapter, are attached correctly.
- Ensure that the correct Wireless Adapter is installed. The compatibility of the Wireless Adapter is dependent on the device model and software version.

Wireless Signal Strength

Wi-Fi connection speed varies with distance. A wireless client that is further away from the Access Point (AP) obtains a lower signal strength and a slower connection. If the wireless signal between two connected Wi-Fi devices is not strong enough, a degradation in performance occurs. Obstructions between the AP and wireless client can cause interference and affect performance.

To improve signal strength:

- If possible, place the wireless router or AP in a centralized location.
- Remove any physical obstructions between the AP and the Xerox® Wireless Network Adapter.
- If possible, position the Xerox® Wireless Network Adapter closer to the AP.
- Check the wireless signal strength for the Xerox® Wireless Network Adapter. For details, refer to Checking Wireless Signal Strength in the Embedded Web Server.
- To reduce interference with wireless signals from the router, ensure that the router or AP is located away from walls or large metal objects, such as filing cabinets.
- Ensure that the Xerox® Wireless Network Adapter is positioned away from walls or large metal objects.
- If applicable, consider upgrading the router or AP to a high-gain antenna that transmits the wireless signals in one direction only.
- If applicable, position the Wireless Network Adapter on the Xerox device in direct view of the wireless router or AP. To secure the adapter, use the USB extension cable and velcro strips provided with the Xerox® Wireless Network Adapter Kit.

Note: For some solutions, Bluetooth functionality is included with the wireless hardware solution.

Checking Wireless Signal Strength at the Control Panel

1. At the control panel, touch **Device**, then touch **Tools**.
2. Touch **Network Settings > Network Connectivity > Wireless**.

3. In the Wireless information panel, check the Signal Strength indicator.

Note: For optimum performance, the required signal strength for a Xerox® Wireless Network Adapter is 3 bars or more. This level indicates a signal strength of 60–70%.

4. To close the screen, touch **X**.

Checking Wireless Signal Strength in the Embedded Web Server

1. In the Embedded Web Server, click **Properties > Connectivity > Setup**.
2. For Xerox Wireless Network Interface, click **Edit**.
3. On the Wireless Profile page, for Wireless Settings, click **Edit**.
4. On the Wireless Settings page, to check wireless signal strength, do one of the following:
   - In the Limit Wi-Fi Roaming area, click **Show Settings**. The settings table shows the signal strength for the current network.
   - To view the list of available wireless networks, click **Cancel**. In the Wireless Networks list, check the signal level percentage for the selected network.

Note: For optimum performance, the required signal strength for a Xerox® Wireless Network Adapter is 60% or more.

5. Click **Close**.

Network Usage and AP Loading

AP loading relates to the number of client connections to an access point. The number of client connections, and the amount of bandwidth that each client uses, have a direct impact on the performance of the Xerox® Wireless Network Adapter.

To minimize the effects of network usage and AP loading:

- Increase the quality and number of access points.
- Use a wired connection for connected devices that are moved rarely. Reducing the number of wireless connections helps to keep wireless channels free for devices that have to use wireless.
- Remove older clients, such as 802.11b devices, from the network, as they can reduce overall wireless network speed.

Check Access Point for Load Balancing Settings

Some access points have features to help manage load balancing, which can at times result in unintended outcomes. Check your AP for settings that may make 5-GHz frequency bands appear more attractive than 2.4-GHz frequency bands, such as Client Band Select or Band Steering. These settings may end up directing a client toward a 5-GHz band even if the signal in 2.4 GHz is much stronger.

Radio Frequency Interference

Devices that emit an electro-magnetic signal can generate Radio Frequency (RF) interference. Devices include consumer products, such as cordless phones, wireless headsets, microwave ovens, and smart meters. Many of these products use the same 2.4-GHz frequency as 802.11b/g/n. Interference that occurs during transmission can cause

packet loss, which forces Wi-Fi retransmissions. Retransmissions impact throughput, and result in fluctuating wireless performance for all users that share a given access point.

Co-channel interference occurs when devices interfere with each other because they use the same channel or radio frequency to transmit and receive Wi-Fi signals. This type of interference can result in degraded wireless performance.

To reduce interference:

- Avoid the use of older electronic devices that use the 2.4-GHz frequency, or remove these devices, then place them in a separate location.
- Ensure that the wireless channel that is in use does not overlap with another Wi-Fi network.
- Where possible, leverage 802.11n/ac on the 5-GHz frequency band. On this frequency band, the transmission rates are higher and interference is generally lower. However, the range can be lower.

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.

Note: When Wi-Fi Direct is enabled and the wireless interface is operating on a DFS channel concurrently, the Wi-Fi Direct active status displays an error string `Enabled with Errors`.

CONFIGURING WI-FI DIRECT

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

Note: Wi-Fi Direct has compatibility limitations when the wireless interface is enabled using a Dynamic Frequency Selection (DFS) channel. Disable DFS on the wireless access point to which the printer is connected. For details, refer to Dynamic Frequency Selection (DFS).

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 the **Enabled** check box.
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**. The Device 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**.

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**.

DYNAMIC FREQUENCY SELECTION (DFS)

- Dynamic Frequency Selection (DFS) is a wireless channel selection technique that avoids electromagnetic interference with other technologies and services. Because the frequency is shared with other technologies and services, regulations in many countries limit the number of 5-GHz channels available or place additional restrictions on the operation. When operating within limited frequencies, radar detection and avoidance capabilities are required.
  - DFS is a capability of the wireless Access Point (AP). DFS can be enabled or disabled on many APs.
  - If a wireless AP detects a radar system on a DFS enabled channel, the AP broadcasts the switch channel occurrence to the associated client printers and switches the channel to a non-DFS channel.
- If the wireless AP supports DFS channels, the printer supports connecting to DFS channels through the wireless interface.
- When Wi-Fi Direct is enabled, the printer acts as a Software Access Point and manages the Wi-Fi Direct connections and security. Wi-Fi Direct does not support the DFS technique and cannot operate on DFS channels.
- The Wi-Fi Direct inoperability arises when both conditions are true:
  - The printer has Wi-Fi Direct and the wireless interface enabled concurrently.
  - The wireless interface is connected to an AP and operates on a DFS channel.

To resolve Wi-Fi Direct inoperability:

1. When Wi-Fi Direct is inoperable, check the Wi-Fi Direct homepage for the DFS status message.
2. To update the network configuration, perform any of the following:
   - Disable DFS on the wireless network AP. Then DFS frequencies will not be supported.
   - Connect the printer to a 2.4-GHz wireless network. DFS frequencies are not supported on the 2.4-GHz frequency bands.
   - Connect the printer to the Ethernet instead of a wireless network.
   - If the wireless network supports multiple Base Station IDs (BSSIDs), update the wireless connection of the printer and select any of the available non-DFS channels. The BSSIDs of the wireless network can be found in the Limit Wi-Fi Roaming settings. The non-DFS BSSIDs can be determined depending on the frequency range.

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 use AirPrint to scan from a printer to supported Apple devices.

Note:

- Not all applications support AirPrint.
- AirPrint, and the protocols that it requires, are enabled by default.
- When AirPrint is re-enabled:
  - HTTP, IPP, and Multicast DNS are enabled automatically.
  - IPP enablement requires a Web server reset.
- Subnet caveats:

  By default, AirPrint printer discovery is accomplished using Multicast DNS or Bonjour. When Multicast DNS is used, ensure that the client device that submits the AirPrint job is on the same subnet as the printer.

  To allow AirPrint client devices to print from different subnets, try one of the following solutions:

  - Enable iBeacon for AirPrint Discovery. For details, refer to Enabling iBeacon for AirPrint Discovery. This option requires a Bluetooth® device, connected to the printer, that is used for AirPrint printer discovery.
  - Configure your network to pass Multicast DNS traffic across subnets.
  - Use an alternate solution, such as Wide Area Bonjour. For details, refer to Bonjour.
  - Configure a Bonjour Gateway.
- The following are the supported mobile devices. The devices require the latest version of iOS.
  - All models of iPad
  - iPhone 3GS or later
  - Third-generation or later iPod Touch

CONFIGURING AIRPRINT

To configure AirPrint:

1. In the Embedded Web Server, click **Properties > Connectivity > Setup**.
2. In the Mobile Workflows area, for AirPrint, click **Edit**.
3. In the Protocols area, ensure that the required protocols are configured.
   - To configure HTTP/HTTPS, click **Edit**. For details, refer to HTTP.
   - To configure IPP, click **Edit**. For details, refer to IPP.
   - To configure Multicast DNS Registration, click **Edit**. For details, refer to IP.

4. In the iBeacon Settings area, for iBeacon (Bluetooth®) for AirPrint Discovery, click **Edit**. For details, refer to Enabling iBeacon for AirPrint Discovery.

Note: The Status area displays information about the iBeacon Bluetooth® adapter and the iBeacon enablement state.

5. In the Enablement area, 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 Printing/Faxing is enabled by default.
- AirPrint faxing is supported only on devices that have embedded fax enabled and devices that are configured to allow sending faxes.
- When you enable scanning for AirPrint, Mopria is enabled for scanning too.

6. If AirPrint printing is enabled, optionally configure settings for IPP authentication. For details, refer to IPP.
   a. On the IPP page, for Authentication, select **HTTP Basic with Secure IPP (IPPS)**. 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. For sending encrypted login credentials, ensure that the printer is configured to Force Traffic over Secure Connection (HTTPS), which is enabled by default. For details, refer to HTTP.

   b. When HTTP Basic with Secure IPP (IPPS) is enabled, for Validation Location, select an option:
      - **Validate 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.
      - **Validate 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. If scanning is enabled, configure the settings for scanning authentication, if required:
   a. 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. The HTTP Digest option uses encrypted user login credentials over HTTP or HTTPS. HTTP Digest is always encrypted and is the most secure option. HTTP Digest is available when scanning is enabled, and when FIPS 140 is configured as follows:
  - FIPS 140 is disabled.
  - FIPS 140 is enabled with HTTP Digest indicated as an exception. For details, refer to FIPS 140.

Note:

- If you select HTTP Digest authentication, the validation location is configured automatically for validation on the device. This option enables HTTP authentication of user accounts that are configured in the device user database. For details, refer to Device User Database.
- The authentication method for HTTP that is selected here does not affect authentication for other features that use HTTP.

b. If you selected HTTP Basic authentication, for Validation Location, select an option:

- **Validate on the Device**: This option enables HTTP authentication of user accounts that are configured in the device user database. For details, refer to Device User Database.
- **Validate on the Network**: This option enables HTTP 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 or location, for Device Name, Device Location, or Geographic Location, click **Edit**.

Note: Providing a device name can help users identify the device.

9. 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.

ENABLING IBEACON FOR AIRPRINT DISCOVERY

The iBeacon feature simplifies local AirPrint printer discovery, and removes the need for AirPrint clients to be on the same subnet as the printer.

The requirements for using the iBeacon feature are as follows:

- The iBeacon Bluetooth® adapter is installed on the printer.

Note: For some solutions, Bluetooth functionality is included with the wireless hardware solution.

- iBeacon is enabled.
- IPP is enabled.

- A routable, non-link, local unicast IPv4 or IPv6 address is configured for the active network interface of the device. The active interface is Ethernet or wireless.

When the iBeacon feature is configured, the printer advertises basic printer discovery information that includes a routable IP address, using the Bluetooth® low energy beacon. To allow client–printer communication, the AirPrint client needs to reach the printer using the IP address that the iBeacon is broadcasting. If the printer has multiple routable IP addresses, the system administrator can select the IP address for the iBeacon device to use.

Note: The printer can have the following IP address configurations:

- An IPv4 address
- An IPv4 and multiple IPv6 addresses
- Multiple IPv6 addresses

For an introduction to using iBeacon, watch the iBeacon video on the Xerox Support YouTube page. For details, refer to the System Administrator How To Page.

Before you begin, install the iBeacon Bluetooth® adapter into a USB port on the rear of the printer.

Note: Bluetooth is supported through the Xerox® Wireless and Bluetooth Network Adapter.

Note:

- Ensure that the USB port is enabled. For details, refer to USB Port Management.
- When the iBeacon Bluetooth® adapter is installed, a message appears for 7 seconds to indicate the status of iBeacon enablement.

To configure iBeacon:

1. In the Embedded Web Server, click **Properties > Connectivity > Setup**.
2. In the Mobile Workflows area, for AirPrint, click **Edit**.
3. On the AirPrint page, in the iBeacon Settings area, for iBeacon (Bluetooth®) for AirPrint Discovery, click **Edit**.
4. On the iBeacon (Bluetooth®) for AirPrint Discovery page, for iBeacon Enablement, click **Enabled**.

Note: iBeacon is enabled by default.

5. For iBeacon IP Address, review or select the iBeacon IP address. If more than one routable IP address is available, select an address from the list.

Note:

- The Select IP address (routable) feature is disabled until the following conditions are met:
  - The iBeacon Bluetooth® adapter is installed on the printer.
  - iBeacon is enabled.
  - At least one routable IP address is available.
- By default, the printer determines the optimum routable IP address to use in the iBeacon. The optimum routable address is based on the configuration of the printer.

- If more than one routable IP address is available for the active network interface, the system administrator can select an IP address for the iBeacon from the list of addresses, if required. The list of addresses can contain routable IPv4 and IPv6 addresses.

6. To save the settings, click **Save**.

Note: If a mobile Apple client is unable to discover the printer using iBeacon, verify that the client can reach the IP address that the iBeacon is broadcasting.

Bonjour

Bonjour allows the discovery and use of AirPrint devices in a multicast DNS environment. Bonjour requires Multicast DNS Registration enablement.

To expand the service discovery in the local subnet with services available in a wider network domain, you can use Wide Area Bonjour. Wide Area Bonjour removes multicast DNS local network restrictions by using DNS Service Discovery (DNS-SD) information.

Wide Area Bonjour requires:

- Multicast DNS Registration enablement
- A verified host name and domain name

1. In the Embedded Web Server, click **Properties > Connectivity > Setup**.
2. In the Protocol area, for Bonjour, click **Edit**.

   Note: Bonjour Printer Name always displays the device name.

3. In the Bonjour Settings area, for Multicast DNS Registration, click **Edit**. At the IP page, for Multicast DNS Registration, select **Enabled**, then click **Apply**.

   Note: When multicast DNS is enabled, Bonjour is enabled by default.

4. To change the device name, in the Bonjour Settings area, for Device Name, click **Edit**.
5. If needed, configure Wide Area Bonjour settings in the Wide Area Bonjour for AirPrint Settings area.
   a. To view the verified host name and domain name, for Verified Host and Domain Names, click **View**.
   b. To download the DNS-SD record data file, for Manual Wide Area Bonjour (DNS-SD record data), click **Download**. Save the `dns-sd.txt` file to a folder on your computer.

Note: For details and a step-by-step guide on how to use the DNS-SD record data to support AirPrint discovery across subnets, click **DNS-SD Record Data Help**.

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 is disabled. HTTP Digest is also available when FIPS 140 is enabled with HTTP Digest indicated as an exception. For details, refer to FIPS 140.
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**.

Universal Print

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

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

- When Universal Print is enabled, the configuration settings appear. The Universal Print area displays the registration status of your device.
- When Universal Print is disabled, the configuration settings are hidden. The Universal Print area shows the status `Off`. This status is the default.

UNIVERSAL PRINT STATUS

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

- `Not Registered`: This status appears when Universal Print is enabled but the device is not registered.
- `Pending Registration`: This status appears when registration is in process.
- `Registered`: This status appears when Universal Print is enabled and the device is registered.
- `Registration Expired`: This status appears when the Universal Print registration certificate expires.

REGISTERING A DEVICE FOR UNIVERSAL PRINT

Before you register a device for Universal Print, ensure that TLS 1.2 is configured. For details, refer to TLS.

Note: If your organization uses a proxy server, ensure that the proxy server settings are configured for Universal Print. For details, refer to Proxy Server.

1. In the Embedded Web Server, click **Properties > Connectivity > Setup**.
2. For Print and Scan Workflows, for Universal Print, click **Edit**.
3. In the Configuration area, to enable Universal Print, click the toggle button.
4. To set the Job Check Frequency, click in the row. The Job Check Frequency page appears. Select **30 Seconds**, **2 Minutes**, or **4 Minutes**, then click **Save**.
   The job check frequency sets the interval that the device uses to poll the Universal Print service for available print jobs.
5. To update the device name, click in the Device Name row. The Description page appears. Update the device name, then click **Save**.
6. To change the TLS setting, click in the row. The TLS page appears. Ensure that TLS 1.2 is configured, then click **Save**.

   Note: If Universal Print is enabled, and you attempt to change the TLS version to **TLS 1.3 only**, an alert appears. To function correctly, Universal Print requires TLS version 1.2.
7. Click **Register**. The registration process authenticates the device with Microsoft Entra ID. Microsoft Entra ID formerly known as Azure® AD.

Note: Microsoft Entra ID is the new name for Azure AD. The names Azure® Active Directory, Azure AD, and AAD are replaced with Microsoft Entra ID.

a. If authentication fails during the registration process, a message window appears. Respond as needed.

- `Cannot Connect`: If this message shows, verify the network connection, then attempt registration again. To investigate further, view the authentication log.
- `Registration Attempt Failed`: If this message shows, click **View Authentication Log**. For details, refer to Authentication Log.
- `Duplicate Registration`: If this message shows, registration for the device is already in progress.

b. If authentication is successful during the registration process, the Register Device window appears. To copy the registration code, click **Copy**, then click **Register Device with Microsoft**.

Note:

- When registration is in process, you cannot cancel the action.
- The registration process needs to complete before the code expires.
- The registration code expires after 15 minutes.

8. A new Web browser window opens. Do the following:
   a. At the Enter code window, paste the registration code into the Code field, then click **Next**.
   b. At the Pick an account window, select the appropriate Microsoft® account.

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

   c. A Xerox Discovery Universal Print Connector window appears. Close the window.
9. To complete registration, at the Universal Print window, click **Verify Registration Status**. Continue to click **Verify Registration Status** until the status changes to `Registered`.

Note: If verification is in progress, a Verification Still Pending window appears. Close the window.

10. If the code expires or registration fails, a status of `Not Registered` appears in the Universal Print area. Repeat the registration process.
11. If registration is successful, a status of `Registered` appears in the Universal Print area. The device is available as a cloud printer in the Universal Print service.
12. To allow users to access the device, the Azure® administrator needs to share the printer in the Microsoft Entra ID portal. Microsoft Entra ID formerly known as Azure® AD.
    a. In a Web browser, go to https://portal.azure.com/#home.
    b. For Azure services, click **Universal Print**.
    c. In the Manage area, click **Printers**.

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

       The Share printers window appears.

e. To change the default printer name, update the Share name field for the cloud printer. A unique share name allows the users to easily identify the cloud printer in the network.

f. To allow access to the cloud printer for everyone in the organization, click the toggle button.

g. To select the users that you need to share the printer with, in the Select member(s) area, click the names of the users. To locate users, use the search by name option.

h. Click **Share Printer**. When printer sharing is complete, a confirmation message appears.
After the printer is shared, an authorized user can discover the device using the Add Printer feature in Windows 10. The device appears as a cloud printer in the discovered printers list.

To add a cloud printer in Windows 10, click **Settings > Printers & Scanners > Add a printer or scanner**. Select the cloud printer in the list of discovered printers, then click **Add device**.

ADMINISTRATOR FUNCTIONS FOR UNIVERSAL PRINT

When a print job is submitted to Universal Print, it is queued in the cloud until the printer fetches the job. The printer checks for jobs after the polling interval elapses, or when you initiate the **Check For Jobs Now** function.

The following functions are available:

- **Check For Jobs Now**: Use this function to check the cloud for pending print jobs. Available jobs are transferred to the device active jobs queue.

  Note: If a connection failed message appears, verify the network connection, then check for jobs again. If the error persists, refer to the authentication log.

- **Test Connection**: Use this function to test connectivity to the cloud. If the test fails, to investigate further, view the authentication log.
- **Deregister**: Use this function to deregister the device from the Universal Print service. Deregistration requires a deregistration code and follows a similar process to registration.
- **Active Jobs**: Use this function to view jobs in the device active jobs queue. Active print jobs include jobs that are in the queue and jobs that are printing. The active jobs queue does not show completed jobs.

  Note: At the device control panel, in the Jobs App, Universal Print jobs are signified by a cloud print icon.

  Note: Microsoft Entra ID is the new name for Azure AD. The names Azure® Active Directory, Azure AD, and AAD are replaced with Microsoft Entra ID.

Universal Print Secure Release

For Universal Print Secure Release, the Entra ID or Azure® administrator needs to choose a new setting and change the type of the Universal Print queue to Secure Release. At the printer, Secure Release from Universal Print can be performed when the Login Method is set to Identity Provider (IdP) or Smart Cards. For more information, refer to *Xerox® AltaLink® Series Identity Provider Configuration Guide* in Product Support and Drivers – Xerox.

SETTING UP UNIVERSAL PRINT ON MACOS

Universal Print is supported in macOS Ventura 13.3 or later versions. Before you can find and use Universal Print printers from macOS, ensure that you have an active Microsoft Entra ID account and at least one Universal Print eligible license.

Note: Microsoft Entra ID is the new name for Azure AD. The names Azure® Active Directory, Azure AD, and AAD are replaced with Microsoft Entra ID.

1. Install the Universal Print app from the Mac App Store.
2. To open installed applications, click the **Apple** logo, then click **System Settings**.
3. Navigate to **Universal Print** in the left navigation menu. Sign in using your Microsoft Entra ID account credentials.
4. Click **Add Printer**. Select your printer from the list of available printers. You can also search for a specific printer by name or location.
5. Select your printer, then click **Add**. The printer is now available to use from any application on the device.

Note: Installed printers are displayed in the system print dialog for all users on the device. If you do not have permission to use a printer, your print job fails.

6. From any application that supports printing, click **Print** or press **CMD+P** to open the system print dialog.
7. Select your printer that is registered with Universal Print.
8. Set the printing attributes, such as number of copies and pages, then click **Print**.

Xerox® Workplace Cloud

The Xerox® Workplace Cloud (XWC) feature provides a cloud-based print solution that enables a remote service to manage many aspects of your device.

Note: The Xerox® Workplace Cloud service is a separate feature to the Xerox® Workplace Cloud authentication method. Xerox Workplace Cloud authentication options are configured in the Authentication section. For details, refer to Authentication.

Xerox® Workplace Cloud authentication cannot be enabled independently of the Xerox® Workplace Cloud service.

The following scenarios apply:

- Enabling the XWC service does not enable XWC authentication automatically.
- Disabling the XWC service disables XWC authentication, if it is enabled. An alert notifies that disablement of XWC authentication will occur.
- Enabling XWC authentication enables the XWC service at the same time.
- Disabling XWC authentication does not disable the XWC service.

If you are unable to connect to the Xerox Workplace Cloud, click **Retry Connection** to reconnect. Before reconnecting, check your DNS, Firewall, and Proxy Settings.

To enable Xerox Workplace Cloud:

1. In the Embedded Web Server, click **Properties > Connectivity > Setup**.
2. For Remote Management, for Xerox Workplace Cloud, click **Edit**.
3. In the Configuration area, click **Connection**.
4. In the Connection window, configure settings.
   a. Click the check box for **Enable**.

   Note: Xerox Workplace Cloud is enabled by default.

   b. For the XWC server, configure the default host address, port number, and path.
   The default host address is `wdm.services.xerox.com`. The default port number is 443.
   c. Click **Save**.
   d. The Connection window closes. A Connecting to Xerox Workplace Cloud window appears.

   If the initial connection attempt fails, the device performs a retry at the following intervals:

   - 10 seconds after the initial attempt
   - 60 seconds after the first retry sequence
   - 300 seconds after the second retry sequence

   Note: After 5–10 seconds, the **Cancel** option appears. If you click **Cancel** during the initial connection attempt or during a retry sequence, the device cancels the activity.

5. If the connection attempt fails, a Failed to Connect window appears. A message advises you to check the Authentication Log. For details, refer to Authentication Log.

6. If the connection is successful, a status of `Connected` appears in the Xerox Workplace Cloud status area. The XWC statuses include the following:

   - `Disabled`: This status occurs when XWC is not enabled.
   - `Site Cannot Be Reached`: This status occurs when a connection attempt fails. Verify the settings, then retry the connection.
   - `Connection Error`: This status occurs when a connection attempt fails. Verify the settings, then retry the connection.
   - `Connected`: This status occurs when XWC is enabled and a connection is active. The system time stamp indicates the date and time of the latest connection.
   - `Configuration File Received`: This status occurs when a configuration file is received. The system time stamp indicates the date and time of the latest file received.

   Green text indicates a successful connection. Red text indicates a failed connection.

7. To view related Web services, in the Related Pages area, for Web Services, click **Link**. For details, refer to HTTP Web Services.

USB Settings

You can configure the following settings for USB ports:

- Enablement of USB host or Type A ports. For details, refer to USB Port Management.
- Enablement or disablement and Connection Timeout value for the USB device or Type B port. For details, refer to USB Port Management.
- Power saver settings for USB Type A ports. For details, refer to Configuring Power in Sleep Mode.

CONFIGURING POWER IN SLEEP MODE

The Power in Sleep Mode feature controls power usage when the device is in Sleep Mode.

The Standard Savings setting allows USB Type A accessories to operate when the rest of the device is in Sleep Mode. This setting permits Wi-Fi to maintain communication during Sleep Mode, and USB or card reader activity to wake the device, and the device to get ready to print sooner if it has been in Sleep Mode for only a short while.

To configure Power in Sleep Mode in the Embedded Web Server:

1. In the Embedded Web Server, click **Properties > Connectivity > Setup**.
2. In the USB Settings area, for Power in Sleep Mode, select **Edit**.
3. At the Power in Sleep Mode page, select a power savings option:
   - To achieve the highest amount of power savings, select **Maximum Savings**.

   Note:

   - The Maximum Savings option can prevent some USB Type A devices, such as card readers, from waking the device during Sleep Mode.
   - When wireless network adapter hardware is installed, the power state cannot be set to Maximum Savings.

   - To permit USB Type A accessories, such as card readers, to operate during Sleep Mode, select **Standard Savings**.

   Note: Enabling Standard Savings can cause the device to consume more power in Sleep Mode, but can help to avoid issues with the following:

   - Network accessibility, such as network pings and device website access.
   - The ability to wake up from sleep mode or wake on the submission of print jobs.
   - Interoperability with some managed network switches.
4. Click **Save**.

Configuring Power in Sleep Mode at the Control Panel

To configure Power in 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. At the USB Settings screen, touch **Power in Sleep Mode**.
4. For Power State in Sleep Mode, select **Maximum Savings** or **Standard Savings**. For details, refer to Configuring Power in Sleep Mode.

   Note: When a wireless network adapter is installed, the power state cannot be set to Maximum Savings.

5. Touch **OK**.

FTP/SFTP Client

File Transport Protocol (FTP) is a standard network protocol used to send and manipulate files over a TCP/IP network. Secure FTP (SFTP) is a standard network protocol used with the Secure Shell Protocol (SSH) to ensure that data is encrypted and transferred securely. Several services that run on your device can use FTP as a filing service. For example, Workflow Scanning, Backup Saved Jobs, and Software Upgrade.

CONFIGURING FTP AND SFTP CLIENT SETTINGS

To configure the FTP or SFTP client:

1. In the Embedded Web Server, click **Properties > Connectivity > Setup**.
2. For Protocol, for FTP/SFTP Client, click **Edit**.
3. To enable FTP, click the toggle button for **Allow FTP**.

   Note: If you disable FTP, features that rely on FTP may not function as intended, but the Secure FTP will continue to be available.
4. To select the FTP operational mode, 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. This setting is the default.
   - **Active**: This option transfers data over a fixed, known port from a connection made from the server.
5. In the Features area, to configure the FTP or SFTP client, click on the listed services and perform the actions accordingly. The list of services are as follows:
   - Audit Log Transfer
   - Automatic Software Upgrade
   - Device Address Book
   - Backup Saved Jobs
   - Restore Saved Jobs
   - Scan To - Remote Destinations
   - Server Fax - Fax Repository Setup
   - Workflow Scanning
   - Workflow Scanning - File Repository
   - Workflow Scanning - Pool Management
6. Click **OK**.

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**.

WEB BROWSER CERTIFICATE VALIDATION INFORMATION AND TIPS

In the default configuration, the device uses a Xerox certificate authority (Xerox CA) signed device certificate for the Embedded Web Server HTTPS connection. To establish a secure connection, when a client Web browser accesses the Embedded Web Server, it verifies the validity of the HTTPS certificate. Depending on the Web browser, certain characteristics of the certificate need to be accurate. Inaccuracies can cause the browser to issue certificate warnings or errors.

To avoid certificate warnings or errors, refer to Verifying the Validity Date, Verifying the Name and IP Addresses, and Establishing a Chain of Trust.

Verifying the Validity Date

Ensure that the certificate is not expired or otherwise outside of the validity date range. Verify the validity dates on the certificate. For example:

```
Validity
Not Before: May 14 18:39:04 2021 GMT
Not After: Jun 15 18:39:04 2022 GMT
```

If the date known by the Web browser is outside of the validity date range, a certificate warning or error can occur.

Tip: Ensure that the date and time are correct on the Xerox® device and on the client that is running the Web browser.

Verifying the Name and IP Addresses

Verify that the name and IP addresses in the certificate correspond to the values that the Web browser expects for the Embedded Web Server. Verify the certificate details for the Subject Alternative Name. For example:

```
X509v3 Subject Alternative Name:
DNS:printer1.sdsp.mc.xerox.com, DNS:printer1.local,
DirName:/C=US/ST=Connecticut/L=Norwalk/O=Xerox Corporation/OU=Xerox
Corporation/CN=tester/emailAddress=tester@testdomain.com, IP
Address:10.10.10.100, IP Address:1111:0:4321:ABCD:2222:FFFF:ABCD:4321,
othername:<unsupported>
```

If a name or IP address used to access the Embedded Web Server is not present in the certificate, a certificate warning or error can occur.

Tip: The names and IP addresses in the default device certificate reflect the current configuration of the device.

- The names are based on the following, if available:
  - The <requested host name.requested domain name> for the device.
  - The <verified host name.verified domain name> for the device.
  - The <requested host name.local> for the multicast DNS name for the device.
- The IP addresses are based on the following addresses, if available:
  - The IPv4 address for the device.
  - The IPv6 addresses for the device.

Establishing a Chain of Trust

To trust a certificate, a Web browser requires it to come from a trusted certificate authority. To establish a chain of trust for the default device certificate, ensure that the root certificate of the signing CA is installed and trusted within each browser.

To determine the required CA, obtain information about the issuer from the certificate. For example:

```
Issuer: C=US, ST=New York, L=Rochester, O=Xerox Corporation,
OU=Generic Root Certificate Authority,
CN=Xerox Generic Root Certificate Authority
```

If the Web browser cannot establish a chain of trust, a certificate warning or error can occur.

Tip: Download the Xerox Generic Root CA and install it as a trusted CA in your Web browser. Installation of the Xerox Generic Root CA resolves most Web browser certificate-trust errors.

Note: When the Xerox Generic Root CA is installed and trusted for one Xerox® device, all Xerox® devices that leverage this root certificate connect without errors.

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 Xerox Office Products and Solutions - Xerox.

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 and IPv6 are enabled. If you disable IPv4, the device communicates using IPv6 only. Some features are not fully supported in IPv6-only environments.

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 only enable IPv6, the device communicates using IPv6 only. Some features are not fully supported in IPv6-only environments.

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.

   Note: If a network administrator is using IPv6 and if they need to reserve a specific DHCPv6 address on the DHCPv6 server, they need to know the DHCP Unique Identifier (DUID) of the device. The DUID is based on the Link-Layer Address (DUID-LL) and can be found on the configuration report when IPv6 is enabled on the device.

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. To return all network settings to factory-default settings, click **Default All**.

To configure the DNS, perform the following:

Configuring a Host Name

To configure the Host Name, perform the following steps:

1. For the requested Device Host Name (required), type a unique name for your device. If the device can validate that the host name is registered accurately with the DNS server, the host name appears in the Verified Host Name. The default host name is XRXxxx, where xxx is the Mac address of the device.

Note:

- If no host name, or a different host name, appears as the Verified Host Name, the host name is inaccurate on the DNS server. To ensure accurate DNS records, configure your DHCP server to perform updates on behalf of the DHCP clients.
- Slow network connections can impact the speed at which DNS entries are propagated throughout a network.
- For devices with static IP Address Resolution, manually enter DNS information in the DNS server.

2. To acquire a host name via DHCP through the DHCP Client Option 12, perform the following actions in the DHCP area:
   a. To Automatically Acquire Host Name from DHCP, click the toggle button. If a host name is acquired, it displays as the DHCP Host Name. If no host name is acquired, a message `Host Name Not Acquired` appears.
   b. To Prioritize DHCP Host Name as Device Host Name, click the toggle button.

Note:

- Ensure DHCP Client Option 12 is supported and configured on the DHCP server for the device to obtain a value.
- When a host name obtained from DHCP is prioritized as the device host name, it becomes the official Requested Host Name of the device.

3. To save the configuration, click **OK**.

4. To apply the configuration, click **Apply** after completing the remaining configurations. Applying IP changes requires the web server to restart, resulting in a temporary loss of connectivity.

Note: The host name values are updated after selecting **Apply**.

Configuring a Domain Name

To configure a Domain Name, perform the following steps:

1. For the requested Device Domain Name, type the name of the domain to which the device is connected. If the device can validate that the domain name is accurately registered with the DNS server, the domain name appears in the Verified Domain Name.

Note:

- If no domain name, or a different domain name, appears as the Verified Domain Name, the domain name is inaccurate on the DNS server. To ensure accurate DNS records, configure your DHCP server to perform updates on behalf of the DHCP clients.
- Slow network connections can impact the speed at which DNS entries are propagated throughout a network.
- For devices with static IP Address Resolution, manually enter DNS information in the DNS server.

2. To enable Fully Qualify the Domain Name, click the toggle button. This option instructs the device to append a dot (.) to the end of domain names.

Note:

- Fully Qualify the Domain Name to append a dot (.) is enabled by default.
- This setting ensures that domain names are interpreted as absolute domain names, which can improve DNS resolution.

3. To acquire a domain name via DHCP through the DHCP Option 15, perform the following actions in the DHCP area:
   a. To Automatically Acquire Domain Name from DHCP, click the toggle button. If a domain name is acquired, it displays as the DHCP Domain Name. If no domain name acquired, a message `Domain Name Not Acquired` appears.
   b. To Prioritize DHCP Domain Name as Device Domain Name, click the toggle button.

Note:

- Ensure DHCP Client Option 12 is supported and configured on the DHCP server for the device to obtain a value.
- When a domain name obtained from DHCP is prioritized as the device domain name, it becomes the official Requested Domain Name of the device.

4. To save the configuration, click **OK**.
5. To apply the configuration, click **Apply** after completing the remaining configurations. Applying IP changes requires the web server to restart, resulting in a temporary loss of connectivity.

Note: The domain name values are updated after selecting **Apply**.

Adding DNS Servers

To add a DNS Server, perform the following steps:

1. The DNS Server Addresses include both DHCP-obtained addresses and manually configured addresses.
2. DNS Server Addresses obtained from the DHCP server only appear in the DNS servers summary list.
3. To manually add additional DNS Server Addresses, enter addresses into the fields provided.

Note: Manually entered DNS Server Addresses are prioritized over DHCP provided DNS Server Addresses.

4. For DNS Connection Timeout, type a duration between 5 and 60 seconds that the device waits for if it fails to connect to a DNS server. The device tries to connect to any additional DNS servers after the connection timeout.
5. To save the additional DNS servers and DNS connection timeout, click **OK**.
6. To apply the configuration, click **Apply** after completing the remaining configurations. Applying IP changes requires the web server to restart, resulting in a temporary loss of connectivity.

Note: The DNS Server Addresses values are updated after selecting **Apply**.

Configuring Search Domain

To configure the Search Domain, perform the following steps:

1. The device uses Search Domains appended to the host name to resolve unqualified host names.
2. The Search Domains include DHCP obtained domains, manually configured domains, and domains generated by optionally appending the device domain name or parent domains.
3. To add the device domain to the Domain Name Search List, for Append Device Domain, click the toggle button.
4. To add the parent domains of the device to the Domain Name Search List, for Append Parent Domains, click the toggle button.
5. To manually add additional Search Domains, enter domains into the fields provided.

Note: Depending on the configuration, domain names are prioritized based on the device domain, parent domain, and manually entered Search Domains following DHCP provided Search Domains.

6. To save the configuration, click **OK**.
7. To apply the configuration, click **Apply** after completing the remaining configurations. Applying IP changes requires the web server to restart, resulting in a temporary loss of connectivity.

Note: The Search Domain values are updated after selecting **Apply**.

Configuring Additional DNS Configuration

To configure the Additional DNS Configuration, perform the following steps:

1. To enable Multicast DNS Registration, click the toggle button.

Note: Multicast DNS is used to support Bonjour, AirPrint, Mopria, and other device capabilities.

2. For Release DHCP leases and DNS registrations (via DHCP), click the toggle button. This option allows the device to send a release request to the DHCP and DNS servers. If the servers grant the request, the current IP address and any dynamic DNS names are released. IP addresses and DNS names are released and renewed immediately, and when the device is powered off.
3. To use an IPv6 address before an IPv4 address, select **Prefer IPv6 Address over IPv4**.

   Note: This setting is only applicable if both IPv4 and IPv6 are enabled.
4. To save the configuration, click **OK**.
5. To apply the configuration, click **Apply** after completing the remaining configurations. Applying IP changes requires the web server to restart, resulting in a temporary loss of connectivity.

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 Status LED and Sounds.
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 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 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 in close range. 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. The NFC feature requires installation of the Xerox Print Service app on the mobile device.

Printers can communicate using NFC when they are within your mobile device range.

Note: The actual range can vary depending on mobile 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. The default port number is 123.
   - **Host Name**: For Host Name: Port, and Alternate Host Name: Port, type the host names and port numbers. The default port number is 123.
5. For **Time threshold for triggering device re-sync with NTP**, select a time in seconds. The range is 10–150 seconds. The default value is 110 seconds.

   Note: Changes to these settings cause the printer to restart.
6. For synchronizing the time manually, click **Manual Time Sync**. The Manual Time Sync page appears with a message `Device will restart if correction is required`. To synchronize the time, click **Continue**. To implement the time change, the printer restarts automatically.
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.
8. Click **Save**.

   Changes to these settings can cause the printer to restart.

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 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 that seek services and the servers that provide the services. The proxy server filters client requests and if the requests meet the proxy server filtering rules, the proxy server 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. For some features, you can configure login credentials to enable communication between the client and the proxy server.

The following features use proxy server settings:

- Remote Services
- HTTP and HTTPS Workflow Scanning destinations
- HTTP and HTTPS Workflow Pool repositories
- Extensible Services
- Job Limits Server

Note:

- Not all printer models support all features that use the proxy server.
- Workflow pool repositories and Extensible Services do not support proxy authentication.

CONFIGURING THE PROXY SERVER

If you are using proxy authentication, ensure that you have created a user account and password for the device to use to access the proxy server. Note the user name and password. Also follow the procedure on how to setup the Proxy Server manually.

1. In the Embedded Web Server, click **Properties > Connectivity > Setup**.
2. In the Protocol area, for Proxy Server, click **Edit**.
3. For HTTP Proxy Server, select **Automatic Detection**, **Manual Setup**, or **Disabled**.

   Note: The default configuration for the Proxy Server is **Automatic Detection**.

   a. If the network supports Web Proxy Auto Discovery (WPAD) and when the device is setup for **Automatic Detection**, the device will attempt to automatically detect the HTTP Proxy Server IPv4 communication settings using WPAD.

   b. When Automatic Proxy Detection (APD) succeeds, the device will use the detected address for the Proxy Server and will display the address in use.
4. To setup the HTTP Proxy Server manually, perform the following:

   a. Select **Manual Setup**.

   b. Select the HTTP Proxy Server address type. The options are **IPv4 Address**, **IPv6 Address**, or **Host Name**.

c. Type the appropriately formatted proxy server address and port number.

d. If your proxy server requires a password:

1. Select **Proxy server requires password**.
2. Type the proxy server login name and password.

Note: Use the login credentials that are configured on the proxy server for the device.

e. Click **Save**.

5. To prevent the device from using the HTTP Proxy Server, perform the following:

a. Select **Disabled**.

b. 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**.

ThinPrint Client

For the ThinPrint workflow, a ThinPrint server compresses your ThinPrint print job. If you select the encryption option, the server encrypts the ThinPrint job. Your Xerox device is a ThinPrint client printer that receives, decompresses, and decrypts the print data, then prints the job. ThinPrint is disabled by default. For information on ThinPrint servers, refer to *ThinPrint Engine on Print Servers* at ThinPrint Manuals & Guides.

THINPRINT CLIENT CERTIFICATE REQUIREMENTS

For ThinPrint TLS channel encryption, certificates are required on both the ThinPrint Server and the Xerox device. The certificates can be created by an individual certificate authority server at the customer site, or by an official certificate source. Refer to Security Certificates and *Creating Certificates* at ThinPrint Manuals & Guides.

- The ThinPrint Server requires a Server Authentication Certificate and the corresponding Certificate Authority Root Certificate. The Certificate Authority Root Certificate is the certificate of the Certificate Authority that signed the Server Authentication Certificate.
- The Xerox device requires a ThinPrint Server Authentication Certificate that is signed by the same Root Certificate Authority that signed the ThinPrint Server Authentication Certificate of the ThinPrint Server.
- To upload certificates from the certificate management page, system administrator credentials are required. As the system administrator, after you upload a certificate, from the ThinPrint page for your Xerox device, select and assign the certificate for ThinPrint Encryption.

Note: The ThinPrint Server Authentication Certificate on the device and the ThinPrint Server Authentication Certificate on the server can be the same or different certificates. It is recommended that each device has a unique certificate.

CONFIGURING A THINPRINT CLIENT

To configure your printer as a ThinPrint Client:

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

   Note: The Printer Name is a read-only field, based on the Device Name.
4. To add printers to a named group, type the group name in the Printer Class field. You can enter up to seven ASCII characters or special characters in the Printer Class field.
5. The packet size determines the size of the unit for transferring the printing data. To set the packet size, choose an option:
   - To allow the ThinPrint Server to determine the packet size, select **Auto-Allow ThinPrint Server to Choose**.
   - To change the default setting, clear **Auto-Allow ThinPrint Server to Choose**. Type a value from 200–64000.
6. The default TCP Port is 4000. To use a different port, in the TCP Port field, type a port number.
7. To enable encryption for your ThinPrint print job, select **Activate TLS**.

8. For Select ThinPrint Certificate, select a certificate for your Xerox device.
   - If you choose to use TLS, you cannot print a ThinPrint job unless a ThinPrint certificate is installed on your Xerox device.
   - If the ThinPrint Certificate is not installed on your Xerox device, upload the certificate. For ThinPrint Certificate upload instructions, in the ThinPrint Encryption section, click the **I** icon.
   - To upload a ThinPrint Certificate, click the **View Xerox Device Certificates** link. For details, refer to Creating and Installing a Xerox® Device Certificate.
   - After a ThinPrint Certificate has been installed successfully, the certificate is available in the Select ThinPrint Certificate menu.

Note: ThinPrint encryption requires that your Xerox device and the ThinPrint server have identical configuration. If both systems are not configured the same, job submissions fail.

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. For Protocol, for SMB Filing, click **Edit**.
3. For With Kerberos Tickets, for 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. 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 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 **512–122880** 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. In the Protocol area, for SNMP, click **Edit**.
3. For SNMPv1/v2c, select **Enable SNMP v1/v2c Protocols**, then select an option:
   - To enable SNMPv1/v2c for read and write access, select the check box for **Allow SNMP v1/v2c Set**.
   - To enable SNMPv1/v2c for read-only access, clear the check box for **Allow SNMP v1/v2c Set**.
4. To configure SNMPv1/v2c, click **Edit SNMP v1/v2c Properties**. For details, refer to Configuring SNMPv1/v2c.
5. For SNMPv3, select **Enable SNMP v3 Protocol**, then select an option.
   - To enable SNMPv3 for read and write access, select the check box for **Allow SNMP v3 Set**.
   - To enable SNMPv3 for read-only access, clear the check box for **Allow SNMP v3 Set**.
6. To configure SNMPv3, click **Edit SNMP v3 Properties**. For details, refer to SNMPv3.
7. To prompt the printer to generate a trap for every SNMP request that is processed with an invalid community name, for Authentication Failure Generic Traps, select **Enabled**.
8. 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 SNMPv2c uses the simple community-based security scheme of SNMPv1.

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

   Note:

   - On first access to the printer, the SET Community Name is set to the device serial number. After the initial admin password reset by the system administrator, the SET Community Name is set to the typical default.
   - Changes made to the GET or SET community names for this device require corresponding changes to the GET or SET community names for applications that use SNMP.

6. For Confirm SET Community Name, re-enter the SET Community Name.
7. To save the SET Community Name, select the check box for **Select to save new 'SET Community Name'**.
8. For TRAP Community Name, type a name.

   Note: Use the Default TRAP Community Name to specify the default community name for all traps that the printer generates. Individual TRAP community names specified for each trap destination address can override the community name. Ensure that each TRAP community name is unique.

9. To apply the new settings, click **Save**, or to retain the previous settings, click **Undo**.
10. To return to the previous page, click **Cancel**.

SNMPV3

SNMPv3 is the current standard version of SNMP defined by the Internet Engineering Task Force (IETF). SNMPv3 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

On the first access to the printer, the SNMPv3 passwords are set to the device serial number. After the initial admin password reset by the system administrator, the SNMPv3 passwords are set to the typical defaults.

Configuring SNMPv3

1. In the Embedded Web Server, click **Properties > Connectivity > Setup**.
2. In the Protocol area, for SNMP, click **Edit**.
3. Click **Edit SNMPv3 Properties**.
4. For Security, select an Authentication/Encryption protocol pair for SNMPv3.
5. To configure the Administrator Account:
   a. For Administrator Account, select **Account Enabled**.
   b. Type the user name for the administrator account.
   c. Type, then confirm the authentication password.
   d. Type, then confirm the privacy password.

Note:

- Ensure that the passwords are at least 8 characters in length.
- To set the account credentials to factory-default values, select **Default All**.

6. To allow Xerox clients and print drivers limited access to objects on the device, for Print Drivers/Remote Clients Account, select the configuration settings:
   a. For Print Drivers/Remote Clients Account, select **Account Enabled**.
   b. For Drivers Account, type the user name for the account. Drivers account name cannot be the same as the Administrator account name.
   c. For Authentication Password, type, then confirm the password.
   d. For Privacy Password, type, then confirm the password.

Note:

- Ensure that the passwords are at least 8 characters in length.
- To set the account credentials to factory-default values, select **Default All**.

7. To apply the new settings, click **Save**, or to retain the previous settings, click **Undo**.
8. To return to the previous page, click **Cancel**.

CONFIGURING SNMP ADVANCED SETTINGS

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

To configure advanced settings:

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

Security

This chapter contains:

Setting Access Rights 110
Authentication 111
Authorization 138
Personalization 148
Imaging Security 150
HTTPS (TLS) 155
FIPS 140 156
TLS 160
Stored Data Encryption 162
IP Filtering 163
Logs 165
Trellix® Embedded Control 175
IPsec 178
Security Certificates 185
802.1X 193
System Timeout 196
USB Port Management 197
Image Overwrite Security for HDD Storage Devices 200
Job Data Removal for SSD Storage Devices 205
PostScript® Passwords 208
Personalized Information 209
Verifying the Software 210
Restricting Print File Software Updates 211
Specifying Email Recipient Restrictions 212
Administrator Password 213

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.

The Login Methods page in the Embedded Web Server provides links to authentication and personalization configuration settings. 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 user name and password at the control panel or in the Embedded Web Server. The printer compares the user credentials to the information that is 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. For details, refer to Configuring Local Authentication Settings.
- **User Name / Password - Validate on the Network**: This option enables network authentication. Users prove their identity by typing 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. For details, refer to Configuring Network Authentication Settings.

  Note: The printer can use one of the following authentication server types: Kerberos, LDAP, or SMB.
- **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. For details, refer to Configuring Convenience Authentication Settings.
- **Xerox Workplace Cloud**: This option enables cloud-based authentication. The printer connects directly to the Xerox® Workplace Cloud solution. This method provides multiple options for authentication. To prove their identity, users can use mobile authentication methods, such as NFC or QR Codes, use an identification card, or type a user name and password at the control panel or in the Embedded Web Server. For details, refer to Configuring Xerox Workplace Cloud Authentication Settings.
- **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 authentication method, purchase and install the Xerox Secure Access Unified ID System®. For details, refer to Configuring Xerox Secure Access Unified ID System® Authentication Settings.
- **Identity Provider (IdP) - Validate on Cloud**: This option enables cloud-based authentication through an identity provider (IdP). The device establishes a secure connection with the IdP, then passes the user credentials to the IdP for authentication. For details, refer to Configuring Identity Provider (IdP) - Validate on Cloud Authentication Settings.
- **Smart Cards**: This option enables authentication for a smart card reader. Users swipe a pre-programmed identification card at the control panel. To use this authentication method, purchase and install a smart card reader system, for example, the Xerox Common Access Card Enablement Kit. For details, refer to Configuring Smart Card Authentication Settings.

  Note: New identification cards and card reader systems are launched constantly. To ensure that your printer supports the latest identification cards and devices that are available, software patches are provided on the Xerox website. Before you configure smart card authentication, ensure that the latest software patches are installed on your device.

- **Custom Authentication**: This authentication method requires a feature installation key. After you enter the feature installation key, the Custom Authentication option is available for configuration. For details, refer to Configuring Custom Authentication Settings.

Note: For IdP and Smart Cards login methods, the Xerox Mandatory Multiport USB Hub Kit is required to log in with the USB Authentication Token. For more information, go to www.xerox.com.

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 select Convenience Authentication, Xerox Workplace Cloud, Identity Provider (IdP) - Validate on Cloud, Smart Cards, or Custom Authentication as the authentication method, you can allow users to log in at the control panel. For Alternate Control Panel Login, select **User Name / Password - Validate on the Network**.

Note: The Alternate Control Panel Login method enables users to log in without using a smart card. This option is useful if users lose their smart cards, but need to access the printer.

6. Click **Save**.

Note: The first time that you select Smart Cards as the authentication method, you are prompted for a feature enablement key. The feature enablement key is included in the purchased smart card reader system, for example, the Xerox Common Access Card Enablement Kit.

After you set the login method, the Configuration Settings table on the Login Methods page shows the settings that are available for the authentication method that you selected. Configure the settings as required.

Additional Login Options and Xerox® Easy Assist (XEA) App

You can log in to the printer using your ID card or mobile phone. For Additional Login Options, enable the toggle button to log in at the printer using cards and mobile phones.

The ID card and mobile phone options allow you to log in using the following methods:

- Local accounts, such as administrator account
- Network accounts, such as those connected through LDAP or Kerberos authentication
- IdP (Identity Provider), such as Microsoft Entra user account.

To register and login using an ID card or mobile phone, you will be required to enter a valid user credential. The registration will be complete after the user credential is authenticated successfully. However, they require you to enter the credentials only once.

Subsequent logins use the registered credentials that are stored in the printer to authenticate and log you in. If your password changes, you will be prompted to re-register at the printer.

You can register only one mobile phone or ID card per account. If you are using a Local Authentication and want more than one administrator to log in with their mobile phone or ID card, create additional users with administrative rights.

1. Under Prompts area, select one of the following login options to display at the control panel:
   - **Standard Prompt**: To log in using cards and mobile phones, select **Standard Prompt**, then select one of the following login options from the drop-down menu, as needed:
     - Keyboard and Mobile Phone
     - Keyboard and Card
     - Keyboard, Mobile Phone, and Card

   Note: These options control what is displayed for the user. However, all three login methods, such as cards (if a card reader is attached), mobile phones (if NFC is enabled), and the keyboard will function regardless of the Prompts setting.

   - **Custom Prompt**: To change the window title, instructional text, background image, and logo placement, click **Edit Custom Login Prompt**. For more information, refer to Customize Blocking Screen.
2. Enable **Require Periodic Registration Renewal** to renew the registered profiles periodically. The renewal period can range from 1 through 365 days.

   Note: It is optional and recommended to add Device User Accounts.
3. To enable log in with your mobile phone, download and install Xerox Easy Assist app for Android or iOS mobile phones. For more information about Xerox Easy Assist app, refer to the *User Guide* of your printer.

Additional Login Registration Profiles

You can review a list of ID cards or mobile phones that have been recently registered or used on a printer. A System Administrator can delete any or all of the registrations, which will require the users to re-register.

If the **Require Periodic Registration Renewal** option is enabled, you can view the registrations that have expired.

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: The Website Login option is available when you enable one of the following login methods for the control panel:
   - Convenience Authentication
   - Xerox Workplace Cloud
   - Xerox Secure Access - Unified ID System
   - Identity Provider (IdP) - Validate on Cloud
   - Smart Cards
   - Custom Authentication
5. Click **Save**.

After you set the login method, the Configuration Settings table on the Login Methods page shows the settings that are available for the authentication method that you selected. Configure the settings as required.

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 that is stored in the user database. If you have a limited number of users, or do not have access to an authentication server, use the local authentication method.

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 > Login Methods**.
2. Set the login method to **User Name / Password - Validate on the Device**. For details, refer to Setting the Login Method for the Control Panel.
3. In the Configuration Settings table, configure options for local authentication:
   - To add user information to the device user database, for Device User Database, click **Edit**. For details, refer to Adding, Editing, or Viewing User Information in the User Database.
   - To specify the account and password requirements for a locally authenticated user, for Device Account Requirements, click **Edit**. For details, refer to Specifying User Password and Account Requirements.
   - To enable personalization for logged-in users, for Personalization, click **Edit**. For details, refer to Enabling Personalization.
   - To view or delete personalization profiles, for Personalization Profiles, click **Edit**. For details, refer to View and Deleting Personalization Profiles.
   - To provide information about your LDAP server for personalization, for LDAP Servers, click **Edit**. For details, refer to Configuring LDAP Server Optional Information.
   - To enable or disable the logout prompt at the control panel, for Log Out Confirmation, click **Edit**. For details, refer to Disabling the Logout Confirmation Prompt.
   - To enable and configure an EIP authentication app, for EIP Authentication, click **Edit**. For details, refer to Configuring an EIP Authentication App.
   - To configure card reader policies or to install a card reader firmware update, for Card Reader Setup, click **Edit**. For details, refer to Configuring the USB Card Reader Disconnection Policy.
   - To customize the title and instruction text that appears on the blocking screen, for Customize Blocking Screen, click **Edit**. For details, refer to Customize Blocking Screen.
   - To enable and configure the login options, for Additional Login Options, click **Edit**. For details, refer to Additional Login Options and Xerox® Easy Assist (XEA) App.
   - To view or configure any actions on registered profiles for a user, for Additional Login Registration Profiles, click **Edit**. For details, refer to Additional Login Registration Profiles.

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, Editing, or Viewing User Information in the User 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. For each user, type a user name and a friendly name.

   Note: After you add a user name and friendly name, you can edit the Friendly Name field, but you cannot edit the User Name field.
3. Type a password for the user. To verify the password, retype it.

   Note: The Password field appears only if the selected authentication method is Local Authentication.
4. To add a 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.

   If you have created any user roles, the roles appear in the list.
5. To edit a custom user role, for the role, click **Edit**.
6. Click **Save**.
7. To view a permission summary, for a listed user, click **Permissions**.
   - To view the Print Time Summary, for the Time feature, in the Result column, click the **I** icon.
   - To view and edit the permission roles, for any category, click the **user role** link.

   For details, refer to User Permissions.

Importing the User Database

You can import a user database from a `.csv` file. To import user credentials:

1. In the Embedded Web Server, click **Properties > Login/Permissions/Accounting > Device User Database**.
2. From Management Actions, click **Import**.
3. Click **Choose File**, then select the `.csv` file that you want to import.
4. For Delimiting Character, select an option.
5. For Language, select the language of the text in your `.csv` file.
6. Click **Next**.
7. Enter information in the required fields.
8. Click **Import**.

Downloading a Sample .csv File

To download an example of a formatted `.csv` file for import:

1. In the Embedded Web Server, click **Properties > Login/Permissions/Accounting > Device User Database**.
2. From Management Actions, click **Download Sample**.
3. For Delimiting Character, select an option.
4. For Language, select the language of the text in your `.csv` file.
5. Click **Generate**.
6. When the sample file generates successfully, click **Download File Now**, then open or save the file.

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 non-administrator system accounts from logging in to the device.

Note: When the Restrict System Account Access feature is enabled, you cannot log in to the Diagnostics, Customer Service Engineer, and Force OnBox Login accounts. This feature does not impact other authentication and accounting 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-System Admin Accounts, click the toggle button.
4. Click **Save**.

CONFIGURING NETWORK AUTHENTICATION SETTINGS

When you configure network authentication, to prove their identity, users type their user name and password 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, the IPP Authentication Policy window appears. The IPP Authentication Policy is used to determine which server to use for IPP 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 > Login Methods**.
2. Set the login method to **User Name / Password - Validate on the Network**. For details, refer to Setting the Login Method for the Control Panel.

3. In the Configuration Settings table, configure options for network authentication:
   - To configure authentication server settings, for Authentication Servers, click **Edit**.
     - For Kerberos authentication, refer to Configuring Authentication Server Settings for Kerberos.
     - For LDAP authentication, refer to Configuring Authentication Server Settings for LDAP.
     - For SMB authentication, refer to Configuring Authentication Server Settings for SMB.
   - To enable personalization for logged-in users, for Personalization, click **Edit**. For details, refer to Enabling Personalization.
   - To view or delete personalization profiles, for Personalization Profiles, click **Edit**. For details, refer to View and Deleting Personalization Profiles.
   - To provide information about your LDAP server for personalization, for LDAP Servers, click **Edit**. For details, refer to Configuring LDAP Server Optional Information.
   - To enable or disable the logout prompt at the control panel, for Log Out Confirmation, click **Edit**. For details, refer to Disabling the Logout Confirmation Prompt.
   - To enable and configure an EIP authentication app, for EIP Authentication, click **Edit**. For details, refer to Configuring an EIP Authentication App.
   - To enable and configure a Single Sign On Identity Provider app, for Single Sign On Identity Provider, click **Edit**. For details, refer to Single Sign On Identity Provider.
   - To enable DNS canonicalize hostname in Kerberos Settings, for Device-Wide Kerberos Settings, click **Edit**.

     In the Device-Wide Kerberos Settings window, select any one option to configure the DNS canonical name, then click **OK**.
   - To configure card reader policies or to install a card reader firmware update, for Card Reader Setup, click **Edit**. For details, refer to Configuring the USB Card Reader Disconnection Policy.
   - To customize the title and the instruction text that appears on the blocking screen, for Customize Blocking Screen, click **Edit**. For details, refer to Customize Blocking Screen.
   - To enable and configure the login options, for Additional Login Options, click **Edit**. For details, refer to Additional Login Options and Xerox® Easy Assist (XEA) App.
   - To view or configure any actions on registered profiles for a user, for Additional Login Registration Profiles, click **Edit**. For details, refer to Additional Login Registration Profiles.

Authentication Servers

Use the Authentication Servers page to provide information about your authentication server.

1. In the Authentication Type area, select an authentication server type.
2. To provide information about your server, click **Add New**.
3. To copy the settings from another server, select a server from the list, then click **Copy From**.
4. To specify server settings for an alternate authentication server, click **Add New**.
5. To edit server settings, for the server, click **Edit**.
6. To delete all server information, click **Delete All**.

7. If the IPP authentication window appears, select the number of the default server, then click **Save**.

Note: If IPP Authentication is configured and 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.

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 CONVENIENCE AUTHENTICATION SETTINGS

When convenience authentication is enabled, users swipe a preprogrammed identification card through a proximity card reader at the control panel. To use this method of authentication, purchase and install a USB card reader and an authentication server that supports the Xerox® Convenience Authentication API.

Note: To ensure that the remote server solution works with your printer, you need to add the printer to the remote server solution. As part of this workflow, the remote server configures the printer using SNMP or Web services. For more information, refer to the solutions setup guide for your remote server.

Before you begin:

- Format and configure identification cards.
- Ensure that USB ports are enabled. For details, refer to USB Port Management.
- Connect your card reader to the USB port.

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 > Login Methods**.
2. Set the login method to **Convenience Authentication**. For details, refer to Setting the Login Method for the Control Panel.

3. In the Configuration Settings table, configure options for convenience authentication:
   - To provide information about your authentication server, for Convenience Authentication Setup, click **Edit**. For details, refer to Configuring an Authentication Server for Convenience Authentication.
   - To enable the Xerox Secure Access Web service, for Web Service Enablement (Xerox Secure Access), click **Edit**. For details, refer to HTTP Web Services.
   - To configure card reader policies or to install a card reader firmware update, for Card Reader Setup, click **Edit**. For details, refer to Configuring the USB Card Reader Disconnection Policy.
   - To customize the title and instruction text that appears on the blocking screen, for Customize Blocking Screen, click **Edit**. For details, refer to Customize Blocking Screen.
   - To enable personalization for logged-in users, for Personalization, click **Edit**. For details, refer to Enabling Personalization.
   - To view or delete personalization profiles, for Personalization Profiles, click **Edit**. For details, refer to View and Deleting Personalization Profiles.
   - If you selected an alternate login method that requires a network authentication server, provide information about the server. For Authentication Servers, click **Edit**. For details, refer to Configuring Network Authentication Settings.
   - To provide information about your LDAP server for personalization, for LDAP Servers, click **Edit**. For details, refer to Configuring LDAP Server Optional Information.
   - To enable or disable the logout prompt at the control panel, for Log Out Confirmation, click **Edit**. For details, refer to Disabling the Logout Confirmation Prompt.
   - To enable and configure an EIP authentication app, for EIP Authentication, click **Edit**. For details, refer to Configuring an EIP Authentication App.
   - To enable or disable the device authentication, for On-Device Authentication, click **Edit**.

     In the On-Device Authentication window, to enable or disable On-Device Authentication option, click the toggle button, then click **OK**.

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 XEROX WORKPLACE CLOUD AUTHENTICATION SETTINGS

When Xerox Workplace Cloud authentication is enabled, the printer connects directly to the Xerox® Workplace Cloud solution. This method provides multiple options for authentication. To prove their identity, users can use mobile authentication methods, such as NFC or QR Codes, use an identification card, or type a user name and password.

The configuration options for Xerox Workplace Cloud authentication are similar to the options for convenience authentication with an additional option to configure a proxy server if needed.

Note: To ensure that the remote server solution works with your printer, you need to add the printer to the remote server solution. As part of this workflow, the remote server configures the printer using SNMP or Web services. For more information, refer to the solutions setup guide for your remote server.

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 > Login Methods**.
2. Set the login method to **Xerox Workplace Cloud**. For details, refer to Setting the Login Method for the Control Panel.
3. In the Configuration Settings table, configure the options for Xerox Workplace Cloud:
   - To provide information about your authentication server, for Convenience Authentication Setup, click **Edit**. For details, refer to Configuring an Authentication Server for Convenience Authentication.
   - To enable the Xerox Secure Access Web service, for Web Service Enablement, click **Edit**. For details, refer to HTTP Web Services.
   - To configure card reader policies or to install a card reader firmware update, for Card Reader Setup, click **Edit**. For details, refer to Configuring the USB Card Reader Disconnection Policy.
   - To customize the title and instruction text that appears on the blocking screen, for Customize Blocking Screen, click **Edit**. For details, refer to Customize Blocking Screen.
   - To enable personalization for logged-in users, for Personalization, click **Edit**. For details, refer to Enabling Personalization.
   - To view or delete personalization profiles, for Personalization Profiles, click **Edit**. For details, refer to View and Deleting Personalization Profiles.
   - If you selected an alternate login method that requires a network authentication server, provide information about the server. For Authentication Servers, click **Edit**. For details, refer to Configuring Network Authentication Settings.
   - To provide information about your LDAP server for personalization, for LDAP Servers, click **Edit**. For details, refer to Configuring LDAP Server Optional Information.
   - To enable or disable the logout prompt at the control panel, for Log Out Confirmation, click **Edit**. For details, refer to Disabling the Logout Confirmation Prompt.
   - To configure proxy server settings, for Proxy Server, click **Edit**. For details, refer to Proxy Server.
   - To enable and configure an EIP authentication app, for EIP Authentication, click **Edit**. For details, refer to Configuring an EIP Authentication App.

CONFIGURING XEROX SECURE ACCESS UNIFIED ID SYSTEM® AUTHENTICATION SETTINGS

When Xerox Secure Access authentication is configured, users present a preprogrammed 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 Xerox Secure Access, purchase and install the Xerox Secure Access Unified ID System®.

Note: To ensure that the remote server solution works with your printer, you need to add the printer to the remote server solution. As part of this workflow, the remote server configures the printer using SNMP or Web services. For more information, refer to the solutions setup guide for your remote server.

Before you begin:

- Install the Xerox Secure Access authentication server software, then configure 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.
- Ensure that USB ports are enabled. For details, refer to USB Port Management.
- Connect your card reader to the USB port.

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 > Login Methods**.
2. Set the login method to **Xerox Secure Access - Unified ID System**. For details, refer to Setting the Login Method for the Control Panel.

3. In the Configuration Settings table, configure options for Xerox Secure Access Unified ID System® authentication:
   - To configure the Xerox Secure Access server, for Xerox Secure Access Setup, click **Edit**. For details, refer to Configuring Xerox Secure Access.
   - To enable the Xerox Secure Access Web service, for Web Service Enablement, click **Edit**. For details, refer to HTTP Web Services.
   - To customize the title and instruction text that appears on the blocking screen, for Customize Blocking Screen, click **Edit**. For details, refer to Customize Blocking Screen.
   - If you selected local authentication as the website login authentication method, add user information to the user information database. For Device User Database, click **Edit**. For details, refer to Adding, Editing, or Viewing User Information in the User Database.
   - If you selected an alternate login method that requires a network authentication server, provide information about your server. For Authentication Servers, click **Edit**.For details, refer to Configuring Network Authentication Settings.
   - To enable personalization for logged-in users, for Personalization, click **Edit**. For details, refer to Enabling Personalization.
   - To view or delete personalization profiles, for Personalization Profiles, click **Edit**. For details, refer to View and Deleting Personalization Profiles.
   - To provide information about your LDAP server for personalization, for LDAP Servers, click **Edit**. For details, refer to Configuring LDAP Server Optional Information.
   - To enable or disable the logout prompt at the control panel, for Log Out Confirmation, click **Edit**. For details, refer to Disabling the Logout Confirmation Prompt.
   - To enable and configure an EIP authentication app, for EIP Authentication, click **Edit**. For details, refer to Configuring an EIP Authentication App.

Configuring Xerox Secure Access

1. In the Embedded Web Server, click **Properties > Login/ Permissions/ Accounting > Login Methods**.
2. In the Configuration Settings table, for Xerox Secure Access Setup, click **Edit**.
3. Configure the remote server. For details, refer to the instructions that are provided with your server hardware. After the server is configured, it communicates with the printer and completes the configuration process automatically.
4. To configure communication manually, personalize instructional windows, and review accounting options, click **Manually Configure**. For details, refer to Manually Configuring Xerox Secure Access Settings.
5. To return to the Login Methods page, click **Pending Remote Server Setup**.
6. To configure any settings that are marked in red text as **Required; Not Configured**, in the Configuration Settings table, click **Edit**.

Manually Configuring Xerox Secure Access Settings

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

Before you begin:

Configure the Xerox Secure Access authentication server.

1. In the Embedded Web Server, click **Properties > Login/ Permissions/ Accounting > Login Methods**.
2. In the Configuration Settings area, for Xerox Secure Access Setup, click **Edit**.
3. Click **Manually Configure**.
4. For Server Communication, select the address type and port number.
5. Type the appropriately formatted address and port number.
6. In the Path field, type the following HTTP path: `public/dce/xeroxvalidation/convauth`.
7. For Embedded, select **Enabled**.
8. For Device Log-In Methods, select an option:
   - **Xerox Secure Access Device Only**: This option allows users to access the printer only using the card reader.
   - **Xerox Secure Access Device + alternate onscreen authentication method**: This option allows users to access the printer by logging in at the control panel.
9. When the Network Accounting feature 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**.
10. To create login instructions for users, in the Device Instructional Blocking Window, type the text that you want to appear on the touch screen:
    a. In the Window Title field, type the text that you want to appear as a title at the top of the touch screen.
    b. In the Instructional Text field, type the instructions that you want to 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.
11. Click **Save**.

CONFIGURING IDENTITY PROVIDER (IDP) - VALIDATE ON CLOUD AUTHENTICATION SETTINGS

When you configure Identity Provider (IdP) authentication, users prove their identity by typing a user name and choosing one of the sign-in options allowed by the IdP, such as password. The printer supports several modern authentication sign-on options, such as using an authenticator app, certificate-based authentication, and FIDO2 security keys. These modern authentication technologies offer Single-Factor Authentication (SFA), Multi-Factor Authentication (MFA), and password-less workflows to login to the control panel UI of the printer.

Certificate-based Authentication

- The IdP administrator must set up the CBA sign-in option for their tenant.
- Ensure that the Smart Card interface of the USB security key is enabled and contain a valid smart card logon certificate.
- A USB CCID reader must be connected to the printer to use a smart card like a PIV card.
- The printer administrator must set the First Priority Client Cert Validation Pool setting to Smart Card.
- The printer administrator should set the Acquire email address from user certificate to auto-populate IdP login option to **Yes**.

FIDO2

- Ensure that the IdP administrator has set up the FIDO2 sign-in option for their tenant.
- FIDO2 interface of the USB security key must be enabled and configured.
- Ensure that the USB security key is registered with IdP before using it on the printer.

USB Security Key

If using a USB security key for CBA or FIDO2, then you must have a USB hub installed. For more information, go to www.xerox.com.

USB Security Key with Several Interfaces Enabled

The printer can use the FIDO2 and smart card (PIV) interface of the USB security key. However, if both are enabled, then the printer will not know which interfaces to use without additional user interaction. If smart card (PIV) is the preferred interface, then set the Pre-Capture Smart Card with FIDO2 Support setting of the printer to **Yes**.

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 > Login Methods**.
2. Set the login method to **Identity Provider (IdP) - Validate on Cloud**. For details, refer to Setting the Login Method for the Control Panel.

3. In the Configuration Settings table, configure options for local authentication:
   - To configure identity provider settings, for Identity Provider Endpoint, click **Edit**. For details, refer to Identity Provider Endpoint.
   - To auto-populate IdP login from user certificate, for Auto-Populate IdP Login, click **Edit**.

     In the Auto-Populate IdP Login window, to enable or disable Acquire email address from user certificate to auto-populate IdP login option, click the toggle button, then click **OK**.
   - To add user information to the device user database, for Device User Database, click **Edit**. For details, refer to Adding, Editing, or Viewing User Information in the User Database.
   - To specify the account and password requirements for a locally authenticated user, for Device Account Requirements, click **Edit**. For details, refer to Specifying User Password and Account Requirements.
   - To configure card reader policies, for Card Reader Setup, click **Edit**. For details, refer to Configuring the USB Card Reader Disconnection Policy.
   - To select the trusted client certificates to validate login first, for First Priority Client Cert Validation Pool, click **Edit**.

     In the Edit Client Certificate Priority window, select Smart Card option to login with a Smart Card Authentication using the Certificate Based Authentication sign-in option, then click **OK**.
   - If needed, specify the method that the printer uses to acquire the email address of users. For Acquiring Logged in User's Email Address, click **Edit**. For details, refer to Specifying the Method the Printer Uses to Acquire Email Address of Users.
   - To customize the title text and the instruction text that appears on the blocking screen, for Customize Blocking Screen, click **Edit**. For details, refer to Customize Blocking Screen.
   - To enable the USB device reset from the control panel, for USB Reset Policy, click **Edit**.

     To enable or disable Allow the USB reset from the Touch Control Panel option, click the toggle button in the USB Reset Policy window, then click **OK**.
   - To enable or disable the device authentication, for On-Device Authentication, click **Edit**.

     In the On-Device Authentication window, to enable or disable On-Device Authentication option, click the toggle button, then click **OK**.
   - To enable personalization for logged-in users, for Personalization, click **Edit**. For details, refer to Enabling Personalization.
   - To view or delete personalization profiles, for Personalization Profiles, click **Edit**. For details, refer to View and Deleting Personalization Profiles.
   - To provide information about your LDAP server for personalization, for LDAP Servers, click **Edit**. For details, refer to Configuring LDAP Server Optional Information.
   - To enable or disable the logout prompt at the control panel, for Log Out Confirmation, click **Edit**. For details, refer to Disabling the Logout Confirmation Prompt.
   - To enable and configure proxy server settings, for Proxy Server, click **Edit**. For details, refer to Proxy Server.
   - To enable and configure an EIP authentication app, for EIP Authentication, click **Edit**. For details, refer to Configuring an EIP Authentication App.

- To enable and configure the login options, for Additional Login Options, click **Edit**. For details, refer to Additional Login Options and Xerox® Easy Assist (XEA) App.
- To view or configure any actions on registered profiles for a user, for Additional Login Registration Profiles, click **Edit**. For details, refer to Additional Login Registration Profiles.

Identity Provider Endpoint

Use the Identity Provider Endpoint page to configure cloud-based authentication through a third-party identity provider (IdP). This method of authentication does not require any local server-based components or extra applications on the local network.

For IdP authentication, the administrator establishes a trust relationship between a Xerox® device and an IdP endpoint. When the trust relationship is established, the device passes user credentials to the IdP for authentication. For an authenticated user, the IdP manages access to authorized applications and workflows on the Xerox® device.

Note: If your organization uses a proxy server, communications between the Xerox® device and the IdP endpoint include proxy server authentication.

When the login method is set to IdP authentication, the following configuration settings are required:

- The IdP endpoint settings, including the IdP Web service URL. These settings are contained in an IdP metadata file that the administrator creates and downloads from the identity provider. For detailed instructions, refer to the *IdP Authentication Configuration Guide* at www.support.xerox.com.
- IdP security certificates, including the IdP root certificate and chain of trust certificates. These certificates are installed on the Xerox® device when the administrator downloads the IdP metadata file. To view the certificates installed on your device, refer to Security Certificates.
- A Xerox® device metadata file. The administrator downloads this file during the initial configuration process. The file contains the device settings required to set up the trust relationship between the Xerox® device and an IdP endpoint. The file includes the Xerox root certificate.

The Identity Provider Endpoint area shows the IdP configuration status. The statuses of the Identity Provider Endpoint area appear include:

- `No IdP File Configured`: This status appears when no IdP endpoint is configured. This status is the default.
- `Connection Not Complete`: This status appears on a Xerox® device that has not validated the IdP metadata file.
- `Identity Provider (IdP) Configured`: This status signifies that a secure connection is established between the Xerox® device and the IdP endpoint.

First Time IdP Creation

To create a connection between your Xerox® device and a new IdP endpoint, establish a trust relationship between the two endpoints.

To create a first-time connection:

1. In the First Time IdP Creation area, for Download Device Metadata File to Configure IdP, click **Download File**. A file named `Xerox_mfp_saml_metadata.xml` downloads to the device.

Note: The Xerox® device metadata file is not specific to an individual device. This file is valid for other Xerox® devices.

2. In the Connecting to Existing IdP area, for Upload IdP SAML Metadata File, click **Browse**. Browse to the IdP metadata file downloaded from the IdP endpoint. For example, `IDP_metadata_forXerox.xml`.
3. Select the file, then click **Validate File**. A message, `Connecting to Identity Provider`, appears.
4. If validation is successful, the message, `Successfully validated Identity Provider file`, appears. Click **Close**.
5. The status of the Identity Provider Endpoint area appears as `Identity Provider (IdP) Configured`.
6. If validation fails, the following error message appears:
   - `Could not connect to Identity Provider`: This message appears when the connection fails.
   - `Could not validate Identity Provider file`: This message appears when the metadata file is not valid.
7. Click **Close**. The status of the Identity Provider Endpoint area appears as `No IdP File Configured`.

Test Connection

To test the connection between your Xerox® device and the IdP endpoint, click **Test Connection**. A message, `Connecting to Identity Provider`, appears. Do one of the following:

- To abandon the test, click **Cancel**.
- If the connection is successful, the message, `Successfully connected to Identity Provider`, appears. Click **Close**.
- If the connection fails, the message, `Could not connect to Identity Provider`, appears. Click **Close**.

Note: The connection test obtains the IdP endpoint URL from the IdP metadata file. Run this test only when the IdP metadata file is downloaded.

After you verify the connection, you can clone the IdP settings for use on other Xerox® devices. The clone file includes the device metadata file, the IdP metadata file, and the IdP configuration settings. When a device is configured from cloned IdP settings, a secure connection to the IdP endpoint is established.

CONFIGURING SMART CARD AUTHENTICATION SETTINGS

When the Smart Card Authentication feature is configured, users swipe a preprogrammed identification card at the control panel.

Before you configure the Smart Card Authentication feature, purchase and install a smart card reader system. For more information, refer to *Xerox® AltaLink® Series Smart Card Installation and Configuration Guide*.

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 > Login Methods**.
2. Set the login method to **Smart Cards**. For details, refer to Setting the Login Method for the Control Panel.

3. For Smart Card Type, select one of the following:
   - All Supported Smart Cards
   - CAC & PIV Cards
   - IDPrime MD Cards
4. To customize the supported smart card list, click **Customize Supported Smart Card List**, then click **Download** in the Customize Supported Smart Card List window.

   The supported smart card list package is downloaded. For more details, refer to `Readme.txt` file in the downloaded package.

5. In the Configuration Settings table, configure the options for Smart Card Authentication:
   - To provide information about your domain controller servers, and to configure domain controller and NTP settings, for Domain Controllers, click **Edit**. For details, refer to Domain Controller.
   - To configure certificate validation options and to provide information about your OCSP server, for Certificate Validation, click **Edit**. For details, refer to Configuring OCSP Validation Server Settings.
   - To configure the inactive time limit, for Smart Card Inactivity Timer, click **Edit**. For details, refer to Setting the Inactive Time Limit.
   - To configure card reader policies, for Card Reader Setup, click **Edit**. For details, refer to Configuring the USB Card Reader Disconnection Policy.
   - To customize the title and instruction text that appears on the blocking screen, for Customize Blocking Screen, click **Edit**. For details, refer to Customize Blocking Screen.
   - If needed, specify the method that the printer uses to acquire the email address of users. For Acquiring Logged in User's Email Address, click **Edit**. For details, refer to Specifying the Method the Printer Uses to Acquire Email Address of Users.
   - To display your company logo on the blocking screen, for Import Customer Logo, 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**. For details, refer to Configuring Network Authentication Settings.
   - To allow personalization for logged-in users, for Personalization, click **Edit**. For details, refer to Enabling Personalization.
   - To view or delete a personalization profile for a user, for Personalization Profiles, click **Edit**. For details, refer to Viewing and Deleting Personalization Profiles.
   - To provide information about your LDAP server for personalization, for LDAP Servers, click **Edit**. For details, refer to Configuring LDAP Server Optional Information.
   - To enable or disable the logout prompt at the local user interface, for Log Out Confirmation, click **Edit**. For details, refer to Disabling the Logout Confirmation Prompt.
   - To enable and configure an EIP authentication app, for EIP Authentication, click **Edit**. For details, refer to Configuring an EIP Authentication App.
   - To enable and configure an Single Sign On Identity Provider app, for Single Sign On Identity Provider, click **Edit**. For details, refer to Single Sign On Identity Provider.
   - To enable DNS canonicalize hostname in Kerberos Settings, for Device-Wide Kerberos Settings, click **Edit**.

     In the Device-Wide Kerberos Settings window, select any one option to configure the DNS canonical name, then click **OK**.
   - To enable the USB device reset from the control panel, for USB Reset Policy, click **Edit**.

     To enable or disable Allow the USB reset from the Touch Control Panel option, click the toggle button in the USB Reset Policy window, then click **OK**.
   - To enable or disable the device authentication, for On-Device Authentication, click **Edit**.

     In the On-Device Authentication window, to enable or disable On-Device Authentication option, click the toggle button, then click **OK**.

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. To install domain controller certificates, refer to 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: To ensure time synchronization, Xerox recommends that you enable NTP.

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

To associate an LDAP server with your Domain Controller for authorization or personalization, under 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.

1. On the Login Methods page, next to Certificate Validation, click **Edit**.
2. Select a validation method and 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, under 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, next to 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**.

Single Sign On Identity Provider

A Single Sign On Identity provider is a user authentication service that allows users to maintain multiple user names and passwords with a single set of user credentials. The service authenticates the user for various applications to which they have been granted access, preventing future password prompts for individual applications within the same session and reducing the need for multiple passwords for diverse uses.

The system administrator uses the Single Sign On Identity Provider window to configure the printer to use AD FS as an Identity Provider (IdP), which allows the apps to support a Single Sign On (SSO) workflows.

To configure the Single Sign On Identity Provider app:

1. To enable or disable Single Sign On Identity Provider, click the toggle button.
2. In the Setup area, perform the following:
   a. Enter the complete path of the AD FS endpoint.
   The printer uses this path to communicate with AD FS.
   b. To validate the AD FS Server Certificate, click the toggle button for **Enable**.
   To view the content of the device certificates, click on **View Xerox Device Certificates**. For more details, refer to Security Certificates.
   c. In SAML Token Access Code, enter the code that you received during the installation.

Note: If the number of characters entered for the SAML Token Access Code is less than 14 or more than 64, and if you select **OK**, an error message appears as `The number of characters entered is outside of the approved range. 14 - 64 characters` in the SAML Token Access Code Failed window.

3. To save the settings, click **OK**.

Note: If one or more required fields are left empty, and if you select **OK**, an error message appears as `One or more required fields have not been entered. Enter the required data and select 'OK'` in the Required Entry Required window.

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**.

Configuring the USB Card Reader Disconnection Policy

You can configure the device to display a message when it detects that a USB card reader is disconnected.

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

2. For Card Reader Setup, click **Edit**, then select the **Detection Policy** tab.

Note: If no updatable card reader is detected, the Firmware Update and Detection Policy tabs are not displayed.

3. For Prevent use of device when USB Card Reader is disconnected, click the check box.
4. For Alert walkup user when CCID card reader is not detected or Alert walkup user when Keyboard Emulation reader is not detected, click one or all of the toggle buttons.

Note: These two options are only applicable to particular Login Methods.

5. Click **Save**.

Customize Blocking Screen

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. You can customize the message to provide specific instructions for users, or to remind users to swipe an identification card to access the feature.

To change the window title and instructional text:

1. In the Title field, type the text that you want to appear as a title.
2. For Instructional Text, type instructions for users that appear below the title. For example, type **Swipe your employee badge over the card reader to log in**.
3. Click **Save**.

To change the background image or logo placement:

1. For Background Image Placement or Logo Placement, click **Browse** or **Choose File**.
2. Select the file, then click **Open**.
3. Click **Import**. The new image appears on the blocking screen.
4. To ensure that the changes take effect, click **Restart Device**.

To delete the background image or logo placement:

1. Click **Delete Image**, then click **OK**.
2. To ensure that the changes take effect, click **Restart Device**.

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

1. On the Login Methods page, next to Acquired Logged-in User's Email Address, click **Edit**.
2. Under 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, next to Network Address Book (LDAP), click **Edit**.
4. To enable or disable Personalization, under Feature Enablement, next to Acquire Email from Network Address Book, click **Enable Personalization** or **Disable Personalization**.
5. Click **Save**.

CONFIGURING CUSTOM AUTHENTICATION SETTINGS

Custom authentication requires a feature installation key. After you enter the feature installation key, the Custom Authentication method is available for configuration.

For information about entering feature installation keys, refer to Installing Optional Software Features.

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 > Login Methods**.
2. Set the login method to **Custom Authentication**. For details, refer to Setting the Login Method for the Control Panel.
3. In the Configuration Settings table, configure options for custom authentication:
   - To provide information about your authentication server, for Custom Authentication Setup, click **Edit**. For details, refer to Configuring the Custom Authentication Server.
   - If you require an additional login method to allow users to log in if the custom authentication server is unavailable, for Fallback Login, click **Edit**. For details, refer to Setting Up Fallback Login.
   - To configure card reader policies or to install a card reader firmware update, for Card Reader Setup, click **Edit**. For details, refer to Configuring the USB Card Reader Disconnection Policy.
   - To customize the title and instruction text that appears on the blocking screen, for Customize Blocking Screen, click **Edit**. For details, refer to Customize Blocking Screen.
   - If you enabled Fallback Login or selected an alternate login method that requires a network authentication server, provide information about your server. For Authentication Servers, click **Edit**.
   - To add user information to the user database, for Device User Database, click **Edit**. For details, refer to Adding, Editing, or Viewing User Information in the User Database.
   - To configure the account and password requirements for local authenticated users, for Device Account Requirements, click **Edit**.
   - To enable personalization for logged-in users, for Personalization, click **Edit**. For details, refer to Enabling Personalization.
   - To view or delete personalization profiles, for Personalization Profiles, click **Edit**. For details, refer to View and Deleting Personalization Profiles.
   - To provide information about your LDAP server for personalization, for LDAP Servers, click **Edit**. For details, refer to Configuring LDAP Server Optional Information.
   - To enable or disable the log out prompt at the control panel, for Log Out Confirmation, click **Edit**.
   - To enable and configure an EIP authentication app, for EIP Authentication, click **Edit**. For details, refer to Configuring an EIP Authentication App.

Configuring the Custom Authentication Server

When custom authentication is configured, users swipe a pre-programmed identification card at the control panel.

Before you configure custom authentication, purchase and install a card-reader system.

Custom authentication requires a feature installation key. For information about entering feature installation keys, refer to Installing Optional Software Features.

To configure custom authentication servers:

1. In the Embedded Web Server, click **Properties > Login/Permissions/Accounting > Login Methods**.
2. In the Configuration Settings table, for Custom Authentication Setup, click **Edit**.
3. For Primary Server, select the address type. Options are **IPv4 Address** or **Host Name**.
4. For IP Address: Port, or Host Name: Port, type the appropriately formatted address and port number, as required. For HTTP, the default port number is 80. For HTTPS, the default is 443.
5. For Path, type the server location and directory. The format for an HTTP Web service path is `/directory/directory`.
6. For Secondary Server, select the address type. Options are **IPv4 Address** or **Host Name**.
7. For IP Address: Port, or Host Name: Port, type the appropriately formatted address and port number as required. For HTTP, the default port number is 80. For HTTPS, the default is 443.
8. For Path, type the server location and directory. The format for an HTTP Web service path is `/directory/directory`.
9. The device requires access to the server destination. For Security Credentials, enter the user name and password, then reenter the password. To save the new password, click **Select to save new password**.
10. For Timeout, type a time from 1–120 seconds.
11. Click **Apply**.

SETTING UP FALLBACK LOGIN

If the primary login fails because the authentication server becomes unavailable, users can log in with a user name and password. As a fallback option, the device uses network authentication to validate users.

To enable control panel login if the custom authentication server fails:

1. In the Embedded Web Server, click **Properties > Login/ Permissions/ Accounting > Login Methods**.
2. On the Login Methods page, for Fallback Login, click **Edit**.
3. For Fallback Login, select **User Name/Password – Validate on the Network**.
4. Click **Save**.

After you enable the Fallback Login feature, the Configuration Settings table shows the Authentication Servers option. Configure the Authentication Servers settings required. For instructions, refer to Configuring Network Authentication Settings.

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.

SETTING THE AUTHORIZATION METHOD

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**.
3. To change the User Permissions Method, for Control Panel & Website Login Methods, click **Edit**.
4. At the Edit Methods page, for User Permissions Method, select an option:
   - **Locally on the Device (Internal Database)**: This option verifies user information in the device user database. For details, refer to Configuring Local Authorization Settings.
   - **Remotely on the Network using LDAP**: This option verifies user information in an LDAP server directory. For details, refer to Configuring Network Authorization Settings.
   - **Remotely on the Network using SMB**: This option verifies user information on an SMB server. For details, refer to Configuring Network Authorization Settings.
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 device user database.
- Configure user permissions. For information about user permissions, refer to User Permissions.

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

1. In the Embedded Web Server, click **Properties > Login/ Permissions/ Accounting**.
2. Click **User Permissions**.
3. To view or edit user information, for Device User Database, click **Edit**. For details, refer to User Database.
4. To configure user permission roles, for User Permission Roles, click **Edit**. For details, refer to User Roles.

5. To configure color printing and 1sided printing policies, for Job Override Policies, click **Edit**. For details, refer to Specifying Job Override Policies.

Configuring Network Authorization Settings

When you configure network authorization, the printer references a network 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. For information about user permissions, refer to User Permissions.

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

1. In the Embedded Web Server, click **Properties > Login/ Permissions/ Accounting**.
2. Click **User Permissions**.
3. In the Configuration Settings table, for LDAP Server or SMB Server, click **Edit**. For details, refer to Configuring Network Authorization Server Settings.
4. To configure user permission roles, for User Permission Roles, click **Edit**. For details, refer to User Roles.
5. To configure color printing and 1sided printing policies, for Job Override Policies, click **Edit**. For details, refer to Specifying Job Override Policies.

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**.
   a. For Merge With the Application Group, select an application from the list.
   b. Click **Save**.
3. To create an Application Group from a custom Application ID, for the custom application ID, click **Make This A Group**.
   a. For Application Group Name, type a name for the group.
   b. 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**.
   a. To remove the Application ID, click **Un-merge**. To delete the Application ID, click **Delete**.
   b. Click **Close**.
7. To create a custom Application ID, click **Add Manually**.
   a. For Application ID, type an Application ID.
   b. Click **Save**.
8. To return to the Applications page, click **Close**.

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

Use the Apps & Tools permissions page in the Embedded Web Server to control access to features or configuration settings for a specific user role.

To configure Apps and Tools permissions for the Non-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 **Non-Logged-In Users** tab.
5. For Non-Logged-In User, click **Edit**.
6. Click the **Apps & Tools** tab.
7. To select a preset permission, for Presets, select an option.

   Note: When a preset option is set, a lock icon appears for any app that is not accessible to the user role.

8. If you selected Custom presets, for each app, select a Role State:
   - **Allowed**: The app is visible and accessible to the user.
   - **Not Allowed**: The app is visible, but appears gray. The app is not accessible to the user.
   - **Not Allowed & Hidden**: The app is not visible and not accessible to the user.

9. To allow or restrict access to all apps, select an option:
   - To lock all apps, click the **Lock All** icon.
   - To unlock all apps, click the **Unlock All** icon.
10. To allow or restrict users from setting device-feature defaults, for Customization, select an option:

    Note: If customization is allowed, the user role can set app display preferences at the device user interface. Display preferences include showing or hiding apps, and changing the display order for apps on the home screen. The user role can configure default settings within the Email, Scan To, Copy, Embedded Fax, and ID Card Copy Apps. After customization, the app default settings apply to walk-up users who have not personalized the device for their own use.

    - To restrict users from setting device-feature defaults, select **Not Allowed**.
    - To allow users to set device-feature defaults, select **Allowed**.
11. Click **Apply**.

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. At the Manage user permissions page, configure the needed settings:
   - To assign users to the role, click the **Assign Users to Role** tab. For details, refer to Assigning Users to a Role for Local Authorization or Assigning User Groups to a Role for Network Authorization.
   - To configure print permissions, click the **Print** tab. For details, refer to Editing Print Permissions for the Non-Logged-In Users Role.
   - To control access to features, click the **Apps & Tools** tab. For details, refer to 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.

7. To save your selections, click **Apply**.

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 allows logged-in users to personalize the device home screen to suit the demands of their workflows. Users can select which apps are displayed on the home screen, and the order in which they appear. A logged-in user can create personalized 1-Touch Apps for individual use. Personalized 1-Touch Apps are available only to the logged-in users.

Personalization for logged-in users is enabled by default. Personalization allows a logged-in user to configure the following settings:

- Personalized walk-up screen: When a user logs in, the device launches their preferred app instead of the default walk-up screen.
- Personalized home screen: A user can select their preferred apps to display in a preferred order on the home screen.
- Personalized default settings for the Copy, Email, Fax, Scan To, and ID Card Copy Apps.
- Personalized 1-Touch Apps.
- Personalized app to launch when originals are detected: At the home screen, when a logged-in user loads original documents in the duplex automatic document feeder, the device launches their preferred app.
- Personalized auto start settings for the Copy, Email, Fax, Scan To, and 1-Touch Apps.

Personalization settings are stored in personalization profiles associated with users that have an entry in the user database. For a logged-in user, all personalized settings override the device defaults.

Note: The personalization options that are available to a logged-in user are defined by you as the administrator. For example, if you have chosen to limit permissions for the use of an app, the individual user cannot override those permissions.

ENABLING PERSONALIZATION

To enable logged-in users to personalize the device home screen and app settings:

1. In the Embedded Web Server, click **Properties > Login/ Permissions/ Accounting > Login Methods**.
2. In the Configuration Settings table, for Personalization, click **Edit**.
3. In the Device Personalization area, for Allow logged-in users to personalize workflows & settings, select the toggle button. A check mark indicates that the feature is enabled.
4. To manage the settings for Adaptive Learning, for Use Adaptive Learning to make personalized suggestions for logged-in users, click in the row. For details, refer to Adaptive Learning.
5. To enable the device to retrieve remote customized settings from LDAP, in the LDAP Personalization area, for Retrieve remote customization from LDAP for logged-in users, select the toggle button. A check mark indicates that the feature is enabled.
6. Click **Save**.

VIEWING AND DELETING PERSONALIZATION PROFILES

A personalization profile is associated with a specific logged-in user and is available only to that user. When a user leaves a group, or no longer uses a device, the system administrator can delete the personalization profile for that user.

Note: When the login method is changed, all personalization profiles are deleted automatically.

1. In the Embedded Web Server, click **Properties > Login/ Permissions/ Accounting > Login Methods**.
2. In the Configuration Settings table, for Personalization Profiles, click **Edit**.
3. To delete a personalization profile for an individual user, select the check box for the user, then click **Delete Selected**.
4. At the confirmation prompt, click **Delete**.
5. Click **Close**.

Imaging Security

Security Imaging with Infrared (IR) marking can help with the tracking and management of sensitive documents. IR marking prints a concealed mark that is detected with Infrared technology only. This method of marking can prevent the accidental disclosure of sensitive documents.

Use Imaging Security to enable IR mark application and IR mark detection. The Apply Mark feature is available on color printers only. The Detect Mark feature is available on color and black and white printers.

Note: Not all printer models support the Infrared marking and detection features.

You can enable IR mark application for copy and print jobs. For print jobs, you can restrict IR marking to Secure Print jobs only. When **Apply Mark** is enabled, the device places a predetermined mark in a predetermined place on the job output.

You can enable IR mark detection for copy and scan jobs. When **Detect Mark** is enabled, the device can detect IR marks on documents that are copied or scanned. When an IR mark is detected, the device can stop the job and send email alerts. When an IR mark is detected, the device adds an entry to the Audit Log.

INFRARED SECURITY

To activate the Infrared Security feature:

1. In the Embedded Web Server, click **Properties > Security > Imaging Security**.
2. In the Infrared area, click the toggle button for **Infrared Security**.
   - When **Infrared Security** is enabled:
     - On a color device, Apply Mark and Detect Mark are enabled automatically.
     - On a black and white device, Detect Mark is enabled automatically.
   - When **Infrared Security** is disabled, the configuration settings are hidden. This status is the default.

To configure the **Infrared Security** settings, refer to Mark Configuration Settings, Apply Mark Settings, and Detect Mark Settings.

Mark Configuration Settings

Use Mark Configuration to define IR mark characteristics and to determine an action associated with mark detection.

The IR mark consists of a symbol and dynamic content that relates to the job.

Note: The dynamic content comprises the date and time, the device serial number, and the logged-in user name, if available. If no user is logged in, the default user name for the specific job type is used. For example, `Guest`, `Local User`, `Mobile`.

1. In the Embedded Web Server, click **Properties > Security > Imaging Security**.
2. In the Infrared area, click the toggle button for **Infrared Security**.
3. To configure IR marking, click in the Mark Configuration row.

   The Mark Configuration window appears.

4. To specify a text classification for the mark, for Label, type up to 18 characters. You cannot leave this field blank.
   The label text is included on entries in the Audit Log and email alerts.
5. For Detected Action, select an action associated with the detection of an IR mark. You can select from the following options:
   - **Inhibit Job**: This option instructs the device to stop the copy or scan job as soon as a mark is detected. This setting is the default.

   Note: If **Inhibit Job** is enabled, and a mark is detected, an alert appears at the device control panel. The job is deleted from the job queue.

   - **Email Alerts**: This option instructs the device to send an email alert. The device sends an alert to contacts configured on the Email Alerts page. Only one email alert is sent for each job with a detected mark or marks.
   - **Inhibit Job and Email Alert**: This option instructs the device to stop the copy or scan job, and to send an email alert.
   - **Audit Log Only**: This option instructs the device to record the job in the Audit Log and take no other action. The device records the event in the SIEM log also.

   Note: All jobs with a detected mark are recorded in the Audit Log.
6. When you select an action that includes an email alert, the Email Notifications settings appear.

   Note: If SMTP is not configured, or no email contacts are specified, an error message appears. To configure SMTP, refer to SMTP Server. To specify email recipients, refer to Email Alerts. Ensure that the email recipient is not the same as the email address of the printer.

   a. To view the device notification settings, click in the Email Notifications row. The Email Alerts page opens. Update settings as needed, then click **Apply**.
   b. To include the user name of the logged-in user in the email notification, enable **Include Username**. This setting is disabled by default.
   c. To include the job name in the email notification, enable **Include Job Name**. This setting is disabled by default.

   Device information from the Description page is included in the notification.
7. To save the Mark Configuration settings, click **Save**.

Apply Mark Settings

To configure the **Apply Mark** settings, do the following:

1. In the Embedded Web Server, click **Properties > Security > Imaging Security**.
2. In the Infrared area, click the toggle button for **Infrared Security**.

3. To apply IR marking, click in the **Apply Mark** row. The Apply Mark window appears. **Apply Mark** is enabled by default.
   - When **Apply Mark** is enabled, IR mark settings appear.
   - When **Apply Mark** is disabled, IR mark settings are hidden.

   Note:
   - When **Detect Mark** is disabled, you cannot disable **Apply Mark**.
   - When **Apply Mark** is disabled, the mark settings are saved.
4. In the Marking Apps area, select IR marking options for the Copy and Print Apps. You cannot select **None** for both options.
   - For Copy, select **Mark All Jobs** or **None**. The default setting is **Mark All Jobs**.
   - For Print, select **Only Secure Print Jobs**, **Mark All Jobs**, or **None**. **Mark All Jobs** includes network and mobile print jobs, Secure Print jobs, and jobs initiated through the Print From App. This setting includes jobs submitted from remote repositories such as Microsoft OneDrive and Google Drive also. The default setting is **Only Secure Print Jobs**.

   Note: When black and white output settings are specified, the following applies:
   - For copy jobs, if the output color is set to black and white, the job is printed in black and white and the IR mark is printed in color.
   - For print jobs, if the black and white only feature is enabled in the print driver, the job is printed in black and white and the IR mark is printed in color.
   - For billing purposes, any black and white pages with IR marks are charged as black impressions.
5. To specify the IR mark location, for Location On Page, select **Top - Right** or **Bottom - Right**. The default location is **Top - Right**.

   Note: When **Apply Mark** is enabled, the following applies:
   - Any original content that lies within the bounds of the IR mark is replaced by the IR mark in the job output.
   - IR mark settings override annotation settings defined in the Copy App. If you select **Top - Right**, the entire top row is not available for copy annotations. If you select **Bottom - Right**, the entire bottom row is not available for copy annotations.
6. To save the settings, click **Save**.

When **Apply Mark** is enabled, the app enablement status for IR mark application appears in the Imaging Security area.

Detect Mark Settings

To configure the **Detect Mark** settings, do the following:

1. In the Embedded Web Server, click **Properties > Security > Imaging Security**.
2. In the Infrared area, click the toggle button for **Infrared Security**.

3. To configure IR mark detection, click in the **Detect Mark** row. The Detect Mark window appears. **Detect Mark** is enabled by default.
   - When **Detect Mark** is enabled, IR mark detection settings appear.
   - When **Detect Mark** is disabled, IR mark detection settings are hidden.

   Note:
   - If **Apply Mark** is disabled, you cannot disable **Detect Mark**.
   - When **Detect Mark** is disabled, the mark detection settings are saved.
4. In the Detection Apps area, enable IR mark detection for the Copy and Scan Apps. Enable one or both options.
   - To enable IR mark detection on copy jobs, enable **Copy**. The default setting is enabled.

   Note: If the device detects an IR mark in a copy job, and the device policy allows the job to continue, the following applies:
   - For a color printer, the device applies a new IR mark to the copies. The new mark includes the updated date and time, the device serial number, and a user name.
   - For a black and white printer, the device replaces the IR mark with a generic mark on the copies. The generic mark includes the mark label and the date and time. The text is visible to the human eye.
   - To enable IR mark detection on scan jobs, enable **Scan Apps**. The default setting is enabled. Mark detection does not apply to jobs generated by the Fax and Server Fax Apps.

   Note: If the device detects an IR mark in a scan job, and the job is allowed to continue, the device replaces the IR mark with a generic mark on the scanned document. The generic mark includes the mark label, and the date and time.
5. When **Detect Mark** is enabled, IR mark detection occurs before normal processing for a copy or scan job begins.

   Note:
   - To ensure accurate IR mark detection, adjust the paper guides to fit snugly against original documents loaded in the duplex automatic document feeder.
   - When detection is in process, a `Security Inspection` message appears at the device control panel.
   - The detection function can impact the performance of the Copy and Scan Apps.
6. To save the settings, click **Save**.

When **Detect Mark** is enabled, the app enablement status for IR mark detection appears in the Imaging Security area.

JOBS DETECTED

The **Jobs Detected** feature displays a list of jobs with a detected IR mark. The list is an extract from the Audit Log.

- When **Infrared Security** is disabled and no jobs are available, the Jobs Detected option is hidden.
- When **Infrared Security** is disabled and at least one job is logged, the Jobs Detected option appears.

- When **Infrared Security** is enabled, the Jobs Detected option is available.

To access the Jobs Detected feature, do the following:

1. In the Embedded Web Server, click **Properties > Security > Imaging Security**.
2. In the Infrared area, click the toggle button for **Infrared Security**.
3. In the Imaging Security area, click **Jobs Detected**.
   - If no jobs are available, the Jobs Detected window displays the message `No Jobs Detected`.
   - If at least one job is available, the Jobs Detected window displays the detected jobs log. You can search and filter the list of jobs.
4. To download the report, click the **Download Jobs Detected Report** link, then save the file to your computer.
5. To close the window, click **Close**.

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

The United States Federal Information Processing Standard (FIPS) 140, is a series of government security standards that specify requirements for computer-based encryption algorithms. You can enable FIPS 140 mode, and check the printer for compliance.

Note: The FIPS 140 Security setting on the Xerox® device applies only to the security of the Xerox® device itself. External cryptographic sources, such as servers, clients, smart cards, and other peripheral devices, are outside of the scope of the FIPS 140 boundary for the Xerox® device. The Xerox® device does not assure the FIPS 140 validation of any external cryptographic source.

For interoperability purposes, if a Xerox® device is FIPS 140 enabled, ensure that external entities are minimally FIPS 140 compatible. That is, ensure that the external entities support cryptographic hashes and algorithms that align with those hashes and algorithms required by FIPS 140, regardless of the FIPS 140 validation of the external source.

For security information about your Xerox® device, refer to the *Security Guide* on Information Assurance for your product at Information Security - Xerox. For specific information about FIPS 140, refer to FIPS 140 Compliance Validation.

FIPS 140 MODE

If FIPS 140 encryption is required, all computers, servers, browser software, security certificates, and applications must comply with the standard or operate in FIPS 140 compliant mode. Transmitted and stored data must be encrypted as specified in United States Federal Information Processing Standard (FIPS) 140, 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 140 compliant encryption algorithms. To allow non-FIPS 140 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 140 compliant protocols after FIPS 140 mode is enabled, a message appears that indicates that the protocols use non-FIPS 140 compliant encryption algorithms. Examples of non-FIPS 140 compliant protocols include SMB, Digest HTTP authentication for AirPrint scanning and Mopria™ scanning, and wireless networking.

FIPS 140 MODE WITH COMMON CRITERIA COMPLIANCE

The Common Criteria for Information Technology Security Evaluation, abbreviated as Common Criteria or CC, is an international standard for computer security certification: ISO/IEC 15408.

For CC compliance, where applicable, enhanced security requirements are applied to a FIPS 140 enabled printer to satisfy the CC security evaluation. FIPS 140 with Common Criteria (CC) compliance mode is a more restrictive configuration. The CC mode can limit interoperability with other network devices that do not communicate with the more stringent CC-defined algorithms.

Note: When FIPS 140 in Common Criteria (CC) compliance mode:

- The certificate checking protocol, OCSP, is automatically enabled. Certificates received from TLS connecting servers will be checked through OCSP, when OCSP is indicated in the certificates.
- In the server certificates received from TLS connecting servers, the IP address in the Common Name (CN) in the subject field of the certificate or Subject Alternative Name (SAN) extension of the certificate, or the Fully Qualified Domain Name (FQDN) in the SAN will need to match the configured server value. Some server certificates may require modifications to comply with this.
- For IPsec, in configurations where peer certificates are required in setting up IPsec communications, the IP address in the SAN will need to match the configured peer value. Some peer certificates may require modifications to comply with this.

FIPS 140 ENABLEMENT WORKFLOW AND CONFIGURATION CHECKS

When you enable FIPS 140 only mode or FIPS 140 with Common Criteria (CC) compliance mode, the printer performs a series of checks to validate the current printer configuration. The FIPS 140 Configuration Check page displays a pass or fail message as a result of the FIPS 140 configuration check. To complete the FIPS 140 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.

For details, refer to Enabling FIPS 140 Mode and Checking for Compliance, and FIPS 140 Configuration Check.

ENABLING FIPS 140 MODE AND CHECKING FOR COMPLIANCE

1. In the Embedded Web Server, click **Properties > Security > Encryption**.
2. Click **FIPS 140**.
3. Click **Enable FIPS 140 only**, or **Enable FIPS 140 with Common Criteria (CC) compliance**. For information, click the **i** icon.
4. Click **Run Configuration Check and Apply**.
5. Complete the iterative FIPS 140 configuration checks. For details, refer to FIPS 140 Configuration Check.

Note:

- When FIPS 140 Mode is enabled, only FIPS 140 compliant certificates can be installed on the device.
- Some FIPS 140 compliance actions require you to move from the FIPS 140 Configuration Check page to other feature or protocol Embedded Web Server pages. After you complete the action, to continue the validation, return to the FIPS 140 (Level 1) page, re-enable FIPS 140, then rerun the configuration check.
- When the validation completes, you receive notification that the configuration check passed. After you restart the device, the FIPS 140 status details update.

6. To enable FIPS 140 when the FIPS 140 configuration checks are complete, restart the device.

FIPS 140 CONFIGURATION CHECK

When you enable FIPS 140 only or FIPS 140 with Common Criteria compliance mode, the printer performs a series of checks to validate the current printer configuration. For enablement to complete, the printer configuration is required to pass all the validation checks, then you receive notification to restart the printer.

Validation involves a series of iterative checks on the device configuration. 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 140 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 that is acting as a server, and a peer device that is acting as a client

  – Establishing a secure connection between the device that is acting as a client, and a peer device that is 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 140 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 140 is not enabled until you receive notification that all configuration checks are complete and the device is restarted.
- Some configuration actions require you to move from the FIPS 140 page to other Embedded Web Server pages. After completing these actions, to continue the FIPS 140 validation checks and enablement, restart the FIPS 140 checks.

FIPS 140 STATUS

When FIPS 140 is enabled, the FIPS 140 (Level 1) page provides an enablement status for the feature. The status indicates that FIPS 140 is enabled, with or without exceptions, or that the feature requires attention.

- For FIPS 140 only mode, statuses include:

  - FIPS On: The device is compliant with no exceptions acknowledged.
  - FIPS On With Exceptions: The device is compliant with exceptions acknowledged. A summary table lists the exceptions.
  - Feature Needs Attention: Changes may have occurred that impact FIPS compliance: To ensure compliance, disable, then re-enable **FIPS 140 only** mode.
- For FIPS 140 with Common Criteria (CC) compliance mode, statuses include:
  - FIPS + Common Criteria On: The device is compliant with no exceptions acknowledged.
  - FIPS + Common Criteria On With Exceptions: The device is compliant with exceptions acknowledged. A summary table lists the exceptions.
  - Feature Needs Attention: Changes may have occurred that impact FIPS / Common Criteria compliance: To ensure compliance, disable, then re-enable **FIPS 140 with Common Criteria compliance** mode.

TLS

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

TLS settings apply to the device features that use TLS. For example, connection to the device Embedded Web Server, IPPS, HTTPS, and email.

Note:

- TLS settings have no impact on features that do not use TLS. For example, Kerberos, SNMPv3, SFTP, and IPsec.
- TLS hash algorithm settings do not apply to the Scan To Cloud and Print From Cloud features other than for authentication.

To configure TLS:

1. In the Embedded Web Server, click **Properties > Security > TLS**.
2. For TLS Version for Secure Device Communication over a Network, do the following:
   a. To include support for TLS 1.3, select the check box for **Include TLS 1.3**. Select an option:
      - **TLS 1.3 only**: This setting is the most secure option.
      - To support older network protocols, select one of the following options:
        – **TLS 1.2 and TLS 1.3**
        – **TLS 1.1, TLS 1.2, and TLS 1.3**
        – **TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3**

Caution: TLS 1.3 does not support Remote Services. If any servers do not support TLS 1.3, this setting can affect the operation of certain features.

   b. If **Include TLS 1.3** is not enabled, select one of the following options:
      - **TLS 1.2 only**
      - **TLS 1.1 and TLS 1.2**
      - **TLS 1.0, TLS 1.1, and TLS 1.2**

Note:

- The older TLS versions are available for interoperability with older products and environments, but are less secure. Xerox recommends that you choose the most secure option that is interoperable with your environment.
- Changes to the TLS version require a device restart.
- If FIPS 140 with Common Criteria compliance is enabled completely, options less than TLS 1.2 are not available.

Caution: If a chosen more secure setting is not supported by all other network clients and servers, significant network interoperability issues can occur. Network interoperability issues can occur in any device feature that uses TLS, including workflow scanning over HTTPS, SMTP over TLS, POP3 over TLS, and IPPS.

To mitigate network interoperability issues, upgrade the other network clients and servers to higher TLS versions and hash algorithms. Alternatively, use the TLS page to configure support for lower TLS versions and hash algorithms on your Xerox device.

3. For TLS Hash Algorithm, select an option.
   - **SHA-256 and above**: To support current network protocols, select this option. This is the recommended value. When TLS 1.0 or TLS 1.1 is selected, this setting is not available.
   - **SHA-1, SHA-256 and above**: To support older network protocols, select this option.

Note:

- The older TLS hash algorithms are available for interoperability with older products and environments, but are less secure. Xerox recommends that you choose the most secure option that is interoperable with your environment.
- Changes to the TLS hash algorithm setting do not affect digital certificates that are installed on the device. Ensure that any certificates used for TLS connections meet the TLS hash algorithm criteria.

Caution: If a chosen more secure setting is not supported by all other network clients and servers, significant network interoperability issues can occur. Network interoperability issues can occur in any device feature that uses TLS, including workflow scanning over HTTPS, SMTP over TLS, POP3 over TLS, and IPPS.

To mitigate network interoperability issues, upgrade the other network clients and servers to higher TLS versions and hash algorithms. Alternatively, use the TLS page to configure support for lower TLS versions and hash algorithms on your Xerox device.

4. Click **Apply**.

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**.

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

Secure 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**.

   A PII/CII Acknowledgement messages appears as `You are about to download an authentication log that may contain Personally Identifiable Information (PII) or Customer Identifiable Information (CII). By proceeding, you acknowledge your responsibility to comply with all applicable company and government policies regarding the handling, storage, and protection of PII/CII.` To proceed, click **OK** or click **Cancel**.
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 for the troubleshooting session stops when either of the following limits is reached:
  - The allotted amount of time.
  - The maximum file size.
- After 72 hours, the data are removed securely from the device.

For an immediate Network Troubleshooting session, select **Start Now** for the Delayed Start option. Configure session attributes as needed, click **Start**, then click **OK** in the Start Session window to troubleshoot. For details, refer to Set Up a Network Troubleshooting Session.

Delayed Start Network Troubleshooting

Note: The Network Troubleshooting session can be delayed to start at a future time or after the next device restart.

For Delay Start of Network Troubleshooting Session until a future time:

1. For Delayed Start, select **Start Specific Day/Time**.
2. Select the required **Start Day** and **Start Time**.

   Note: The delay start time can be set between 15 minutes and 72 hours.
3. Configure the network troubleshooting session attributes as needed. For details, refer to Set Up a Network Troubleshooting Session.
4. Click **Start**.

The network troubleshooting session starts as scheduled.

Note: Once the Delayed Start status appears, the Start Day and Start Time cannot be modified. To change the Start Day and Start Time, stop the ongoing session and reschedule if required.

For Delay Start of Network Troubleshooting Session until the next device Restart:

1. For Delayed Start, select **Start After Next Restart**.
2. Configure the network troubleshooting session attributes as needed. For details, refer to Set Up a Network Troubleshooting Session.
3. Click **Start**.
4. If needed, select **Restart Now**.

Note: Once the Delayed Start status appears, the Start Day and Start Time cannot be modified. To change the Start Day and Start Time, stop the ongoing session and reschedule if required.

Set Up a Network Troubleshooting Session

To set up a network troubleshooting session:

1. For session duration, select the length of time in hours.

   Note: The capture stops automatically after the time duration.

2. Enter a value between 1 and 50 megabytes to set the maximum file size.
   To optionally configure Session Filters:

   a. If required, you can set the Data Packet Size of the capture. For packet size, type a value between 96 and 65,535 bytes.

   b. To select specific ports for the troubleshooting session, click **Port Filters**.

   Note: All ports are included by default.

      1. If needed, click the toggle button for **Do Not Record Remote Control Panel Data** to exclude network traffic from TCP ports 5905 through 5999.
      2. To include only data from specific ports, click the toggle button for **Record Data from Specific Ports**.
      3. For the ports you want to include, select **Enable**.
      4. To change the properties of a port, click **Edit**. For details, refer to Edit Port Filters.

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

3. To begin the network troubleshooting capture session immediately, click **Start**, then click **OK**.
4. To delay the start of the network troubleshooting session, enable the **Delay Start**. For details, refer to Delayed Start Network Troubleshooting.

   a. To end an ongoing session before the allocated time, click **Stop**, then click **OK**.

   b. To delete the captured session, click **Clear Log**, then click **OK**.

5. To save a copy of the captured session, click **Download Data Log**.
6. To restore the network troubleshooting values to default, click **Reset to Default**, then click **OK** in Reset to Default window.
7.

   Note: Use the **Permanent Removal** option with extreme caution.

   For permanent removal of the Network Troubleshooting function, click **Permanent Removal**, then click **OK** in the confirmation window.
   To restore the Network Troubleshooting function, contact the customer support.

Edit Port Filters

You can use this page to include the selected service in the network troubleshooting session. You can change the service name or add a service name and associated port. Perform the following steps:

1. To edit a service, perform the following steps:

   a. To rename the service, for Service, type a name. Click **Edit**.

b. To include the service in the network troubleshooting session, select **Enable**.

c. To change the port number used for the service, type a port number or select the Plus icon (**+**) or the Minus icon (**-**).

d. Click **Save**.

2. To add a service, perform the following steps:

a. Click **Add**.

Add Port Filters window appears.

b. By default, **Enable** option is selected.

c. For Service, type a name.

d. To add a new port number used for the service, type a port number or select the Plus icon (**+**) or the Minus icon (**-**).

e. Click **Save**.

SIEM

The Security Information and Event Management (SIEM) feature enables your Xerox device to send audit log events directly to compatible SIEM systems using the syslog protocol.

Syslog messages that are generated by your Xerox device can be sent automatically to SIEM destinations for analysis and reporting. In a SIEM system, an administrator can view the events that occurred over a specific time period, for example, to investigate a security breach.

Events are sent as they occur. Events are transmitted in Common Event Format (CEF), which a SIEM system can interpret.

You can configure up to three SIEM destinations and control the events that are sent to each destination, based on the level of severity. The severity levels correspond to the syslog severity codes.

Configuration Overview

To configure the Security Information and Event Management (SIEM) feature:

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

Note: Alternatively, to access the SIEM page from the Connectivity setup page, click **Properties > Connectivity > Setup**. For SIEM, click **Edit**.

At the SIEM page, the status area displays the time stamp of the last device event and shows the enablement state of SIEM destinations.

2. To view the stored events log, click **View Events**.

The latest syslog events appear in reverse order. The event log can display up to 20,000 events. To download the events log, click **Download Events**, then save the `syslog.txt` file to a folder on your computer.

3. The Share Events area shows the status of SIEM destinations. The statuses include the following:
   - `event range; host name settings`: The SIEM destination is configured and is enabled to receive events in the specified range.
   - `Configured; Not Sharing`: The SIEM destination is configured, but not enabled to receive events.
   - `Not Configured`: The SIEM destination is not configured.
4. To send a test message to the SIEM destinations, click **Send Sample Event**. At the prompt, click **Send**. A sample event is sent to all destinations that are configured and enabled.

Note: If no destinations are configured, the Send Sample Event function is not available.

Configuring a SIEM Destination

To configure a Security Information and Event Management (SIEM) destination:

1. In the Embedded Web Server, click **Properties > Security > Logs > SIEM**.
2. In the Share Events area, click the row for the destination that you need to configure. The destination settings window appears.
3. To enable the destination to receive events, for Enable Sharing, click the toggle button.
4. In the Destination Name field, type a name for the SIEM destination.
5. In the Connection area, configure the settings.
   a. To select a protocol for transporting events to the configured destinations, for Transport Protocol, select an option:
      - **TCP/TLS (Secure/Recommended)**: This is a reliable protocol. This option is the default and is the most secure.
      - **TCP**: This is a reliable protocol.
      - **UDP**

Note: Transmission Control Protocol (TCP) is a reliable protocol that performs well with networks that are linked physically and with hosts that are stationary. TCP checks that all data packets are delivered to the receiving host, and retransmits any lost packets. This process ensures that all transmitted data is received eventually.

   b. For Host (Syslog Server), specify a destination by host name, IPv4, or IPv6 address.

Note:

- The device supports destination port numbers from 1–65535.
- If you select TCP/TLS, the default port number is 6514.
- If you select TCP or UDP, the default port number is 514.

6. To test the connection:
   a. Ensure that sharing is enabled.
   b. Click **Test Connection**.
   c. If the ping to the destination fails, verify the configuration, then retest the connection.

7. In the Event Policies area, click **Event Range**. In the Event Range window, select a logging severity level, then click **Save**. The default is severity level 4.

   Note: When you select a severity level, messages for that level and more critical levels are sent to the SIEM destination.

8. Click **Save**.
9. To send a test message to the SIEM destinations, click **Send Sample Event**. At the prompt, click **Send**. A sample event is sent to all destinations that are configured and enabled. Check with the SIEM Administrator to confirm that their SIEM system received the Xerox device event.

   Note: If no destinations are configured, the Send Sample Event function is not available.

Editing a SIEM Destination

To edit a Security Information and Event Management (SIEM) destination:

1. In the Embedded Web Server, click **Properties > Security > Logs > SIEM**.
2. In the Share Events area, click the row for the destination that you need to edit.
3. At the prompt, select an option:
   - To view or modify the destination settings, click **Edit**. For details, refer to Configuring a SIEM Destination.
   - To clear the destination settings, click **Reset**. At the confirmation prompt, click **Reset**.

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, perform the following:
   a. For Increase log levels for selected logs features, click **Configure**. Then, configure settings as needed:

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

   1. In the Feature 1 area, for **Feature**, select a feature from the list. Then, for **Log Level**, select **None**, **Low**, **Medium**, or **High**.
   2. To enable enhanced logging for a second feature, in the Feature 2 area, repeat step 7a.
   3. To enable enhanced logging for a third feature, in the Feature 3 area, repeat step 7a.
   4. In the Additional Logs area, to include SOAP logs, click the check box for **SOAP Logs**.
   5. In the Additional Logs area, to include SMB logs, click the check box for **SMB Logs**.
   6. In the Additional Logs area, to include Stunnel logs, click the check box for **Stunnel Logs**.
   7. 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.
   8. 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.

b. For Increased Data Analysis, click **Configure**. Then, configure settings as needed:

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

1. Select **Enable**.
2. In the **Auto stop** area, set the duration for enhanced logging in days. The range is 1–3 days. The default value is 1 day. Set the time of day for the logging to stop.
3. Click **Start**.

Trellix® Embedded Control

Note: Trellix® formerly known as McAfee®.

Trellix 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.

Security Alerts

Security alerts result from the following events:

- An unauthorized attempt to add or modify a file in a write-protected area
- An unauthorized attempt to read from a read-protected area
- Enablement or disablement of Enhanced Security
- Enablement or disablement of Integrity Control
- An attempt to execute an unauthorized file when Integrity Control is enabled

Note: The device records all security events in the audit log.

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 Trellix ePolicy Orchestrator (Trellix ePO), Xerox® CentreWare® Web, or Xerox® Device Manager. For details about Trellix ePO and Trellix Embedded Control, visit www.Trellix.com.

Note: Trellix ePolicy Orchestrator formerly known as McAfee ePolicy Orchestrator.

To configure Trellix Embedded Control:

- To configure email alerts, for Email Alerts, 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 Trellix 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 **Trellix Embedded Control**.

SETTING THE SECURITY LEVEL

Trellix Embedded Control has two security levels:

- Enhanced Security
- Integrity Control

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

   Note: Trellix Embedded Control formerly known as McAfee Embedded Control.
3. To enable Trellix 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**.

   Note: You cannot disable Trellix Embedded Control. Trellix Embedded Control formerly known as McAfee Embedded Control.
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 **Trellix Embedded Control**.

   Note: Trellix Embedded Control formerly known as 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 Trellix 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.
   - 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: By default, Trellix Embedded Control features are always enabled, and the device records security events in the Audit Log. Trellix Embedded Control formerly known as McAfee Embedded Control.

TRELLIX EPOLICY ORCHESTRATOR SERVER

Use this page to provide authentication data for communicating with your Trellix ePolicy Orchestrator (Trellix ePO) server.

To provide authentication data for your Trellix ePO server:

1. Select an address type. Type the appropriately formatted IP address or host name of your server. Change the default port number as needed.
2. For User Name, type the name that the device uses to access the server.
3. Type the password, then retype the password.
4. Click **Save**.

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 Trellix 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, Trellix® 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.

Note: When FIPS 140 mode is enabled on the device, it is possible to configure IPsec with FIPS 140 complaint options only.

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.

The policy list order is important. The policies are applied in order of priority. Traffic that meets the criteria of a higher priority policy is handled according to that policy, ignoring any lower priority policy that governs the same traffic.

Caution: Ensure that the IPsec security selections for your device match precisely to those on the IPsec security end-point client devices. Mismatches result in communication failures.

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

Use the **Actions** page to create and manage actions. Use the New Action Step 1 of 2 page to name an action and select the keying method.

1. Click **Actions** at the top of the IPsec page.
2. Click **Add New Action**.
3. For IP Action Details, in the Name field, type a name for the action.
4. In the Description field, type a description for the action, if needed.

5. For Keying Method, select an option.
   - **Internet Key Exchange (IKEv1)**. For details, refer to Configuring Internet Key Exchange Settings.
   - **Manual Keying**. For details, refer to Configuring Manual Keying Settings.

   Note: If client devices are not configured for or do not support IKE, select **Manual Keying**.

6. If you selected IKE, select an authentication mode:
   - **Pre-shared Key**: This option instructs the device to authenticate with a pre-shared key. For this method of authentication, each peer device needs to be configured with the same key. Type the key in the Pre-shared Key field.

   Note: For improved security, use a complex and long key:

   - To meet updated security requirements, the minimum key length required is 14 bytes. For example, 14 ASCII characters.
   - The key length can have a maximum length of 248 bytes.
   - You can enter characters from the Latin-1 or UTF-8 character sets.

   - **Digital Certificates**: This option instructs the device to authenticate with digital certificates.

     For this method of authentication, each peer device obtains a unique digital identity certificate from a Certificate Authority (CA) for authentication. The CA issues a digital certificate that contains the public key of the applicant and other identification information. The CA makes its own public key available through the CA certificate. The recipient of the IKE message uses the public key from the CA to verify the digital identity certificate of the peer device. To verify that the digital identity certificate of the peer device is the one that is issued by the CA, the printer verifies the signature of the certificate.

     Important: To authenticate each other successfully, it is necessary for each peer device in the IPsec connection to possess a device certificate signed by a CA that the other peer device trusts.

     When the required certificates are installed, do the following:

     - For Device Authentication Certificate, select a certificate from the list.
     - For Server Validation Certificate, select a certificate from the list.

   Note: Before you can configure the IPsec Action, install the certificates for IKE digital authentication through the Security Certificates page. For more information, refer to Security Certificates.

   Before you save the configuration, to view certificates do the following:

   a. To view the Xerox Device Certificate, click **View Xerox Device Certificates**.
   b. At the View/Save Certificates page, to export the certificate, click **Export (Base-64 Encoded - PEM)**.
   c. To exit the View/Save Certificates page, click **Close**.
   d. To view a Server Validation Certificate, click **View Server Certificates**. Repeat steps b and c, as needed.

7. Click **Next**.

Configuring Internet Key Exchange Settings

Use the Step 2 of 2 (IKEv1 Settings) page to configure Internet Key Exchange settings.

Internet Key Exchange (IKE) is a keying protocol that allows automatic negotiation and authentication, anti-replay services, and Certificate Authority support. IKE can change encryption keys during an IPsec session also. 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 Security Associations to set up the IPsec tunnel.

The device supports the following IKE Phase 1 values by default:

- DH Groups:
  - DH Group 20 (EC P-384)
  - DH Group 19 (EC P-256)
  - DH Group 14 (2048-bit MODP)
- Hashes:
  - SHA-384
  - SHA-256
- Encryptions:
  - AES-CBC-256
  - AES-CBC-128

Note: The System Administrator cannot configure the IKE Phase 1 default values.

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 Security Association is renegotiated and the key is regenerated or refreshed.
2. In the IKE Phase 2 area, for IPsec Mode, select an option.
   - **Transport Mode**: This option encrypts the IP payload only.
   - **Tunnel Mode**: This option encrypts the IP header and the IP payload.

   Note: Tunnel mode treats the entire IP packet as an Authentication Header (AH) or Encapsulating Security Payload (ESP), which provides protection for the entire packet.
3. If you selected **Tunnel Mode**, for Enable Security End Point Address, select an address type. Options are **Disabled**, **IPv4 Address**, or **IPv6 Address**.
4. For IPsec Security, select **ESP**, **AH**, or **BOTH**.
5. For Perfect Forward Secrecy (PFS), select an option. Options are **Group 20 (EC P-384)**, **Group 19 (EC P-256)**, **Group 14 (2048-bit MODP)**, or **None**.

   Note: If FIPS 140 is enabled, you cannot select **None** for PFS.
6. For Hash, select an option. Options are **SHA-256**, **SHA-1**, or **None**.

7. If you selected **ESP** or **BOTH** for the IPsec Security type, for Encryption, select **AES-CBC-128/256** or **None**.

   Note: If FIPS 140 is enabled, you cannot select **None** for Encryption.

8. For Key Lifetime, type the length of time until the key expires in Seconds, Minutes, or Hours. When a key reaches this lifetime, the Security Association is renegotiated and the key is regenerated or refreshed.
9. Click **Save**.

Configuring Manual Keying Settings

Use the Step 2 of 2 (Manual Settings) page to configure manual keys.

Use Manual Keying when client systems either do not support Internet Key Exchange (IKE) or are not configured for IKE.

1. In the Mode Selections area, for IPsec Mode, select an option.
   - **Transport Mode**: This option encrypts the IP payload only.
   - **Tunnel Mode**: This option encrypts the IP header and the IP payload.

   Note: Tunnel mode treats the entire IP packet as an Authentication Header (AH) or Encapsulating Security Payload (ESP), which provides protection for the entire packet.

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. In the Security Selections area, for IPsec Security, select **ESP**, **AH**, or **BOTH**.
4. Depending on the IPsec Security setting, do the following:
   a. To define the inbound Security Association, enter the Security Parameter Index (SPI) inbound value for ESP or AH, or both. For ESP Security Parameter Index: IN or AH Security Parameter Index: IN, type a 32-bit number greater than or equal to 256.
   b. To define the outbound Security Association, enter the Security Parameter Index (SPI) outbound value for ESP or AH, or both. For ESP Security Parameter Index: OUT or AH Security Parameter Index: OUT, type a 32-bit number greater than or equal to 256.
5. For Hash, select an option. Options are **SHA-256**, **SHA-1**, or **None**.
6. For Enter Keys as, select **ASCII format** or **Hexadecimal number**.
7. For Hash Key: IN and Hash Key: OUT, type keys in the appropriate format. Ensure that string lengths meet requirements detailed on the page.
8. If you selected ESP or BOTH for the IPsec Security type, for Encryption, select an option. Options are **AES-CBC-128/256**, or **None**.

   Note: If FIPS 140 is enabled, you cannot select **None** for Encryption.

9. For Encryption Key: IN and Encryption Key: OUT, type keys in the appropriate format. Ensure that string lengths meet requirements detailed on the page.
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, based on the X.509 standard, 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 that defines how the certificate and public key can be used
- A key usage that defines the cryptographic uses of the public key of the certificate

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 that is 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: A Xerox® Device Certificate is less secure than a certificate signed by a trusted certificate authority.

1. In the Embedded Web Server, click **Properties > Security**.
2. Click **Certificates > Security Certificates**.
3. Click the **Xerox Device Certificate** tab.
4. Select **Create New Xerox Device Certificate**.
5. Complete the fields for 2 Letter Country Code, State/Province Name, Locality Name, Organization Name, Organization Unit, Common Name, and Email Address.
6. For MS Universal Principal Name, type a user name as needed.

   Note: The MS Universal Principal Name is required when using 802.1X EAP-TLS for Windows clients or servers.
7. Type the number of days of validity.
8. 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 > Security Certificates**.
3. Click the **CA-Signed Device Certificate(s)** tab.
4. Select **Create Certificate Signing Request (CSR)**.
5. Complete the fields for 2 Letter Country Code, State/Province Name, Locality Name, Organization Name, Organization Unit, Common Name, and Email Address.
6. For MS Universal Principal Name, type a user name as needed.

   Note: The MS Universal Principal Name is required when using 802.1X EAP-TLS for Windows clients or servers.

7. Enter an optional **Challenge Password** for cases where you are using a Certificate Authority (CA) that supports enforcing of a **Challenge Password** during the CSR process.
8. For Key Algorithm, select an option.
9. In the Subject Alternative Name area, select values to include in the security certificate attributes:
   - **Distinguished Name**
   - **IPv4 Address**
   - **IPv6 Address(es)**
   - **Fully Qualified Domain Name**
   - **Multicast DNS Name**

- **Microsoft Universal Principle Name**

Note:

- By default, all Subject Alternative Name (SAN) attributes are included.
- If no SAN attributes are selected, the SAN extension is not included in the generated certificate.

10. To generate the new CSR, 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

Use the View/Save Certificates page to view or save security certificates that are installed on your Xerox® device. To help prevent certificate errors and warnings, review certificate properties for accuracy. Some common property attributes include the following:

- Chain of trust: To determine the CA that can establish a chain of trust for the certificate, view the issuer information.
- Validity date: To ensure that the certificate is not expired, or otherwise outside of the validity date range, verify the validity dates.
- Name and IP addresses: To ensure that the name and IP addresses correspond to the expected values, verify the details for Subject and Subject Alternative Name.
- Security attributes: To ensure that the certificate meets the security requirements for its intended use, verify the details for Signature Algorithm and Subject Public Key Info.
- Certificate purpose and usage: To ensure that the potential uses of the certificate can be supported, verify the details for Key Usage and Extended Key Usage.

To view, save, or delete a certificate, do the following:

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.
   a. To save the certificate file to your computer, click **Export (Base-64 encoded-PEM)**.
   b. 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.

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 for all users, install the Device Root Certificate Authority.

SPECIFYING THE MINIMUM CERTIFICATE KEY LENGTH

All RSA and ECDSA certificates that your Xerox® device uses for encryption need to meet the minimum key-length requirements for the device.

Note: The Elliptic Curve Data Signature Algorithm (ECDSA) and RSA are independent algorithms used in encryption. If you install a certificate that uses ECDSA, it is validated against the ECDSA key-length requirements. If you install a certificate that uses RSA, it is validated against the RSA key-length requirements.

The minimum key lengths apply to the following certificates:

- Existing security certificates installed on your device. For details, refer to Security Certificates.
- Security certificates imported to your device at a future time.

- Security certificates that originate from other sources. For example, certificates used by smart card and email encryption.

Note:

- When you import new certificates to your device, the certificate key lengths are validated against the minimum requirements. Certificates with key lengths that are less than the minimum key-length requirements are not installed.
- If you attempt to change a minimum key-length setting to a value that invalidates an installed certificate, the change is rejected.
- Before you change the key-length setting, remove any noncompliant certificates.

To set certificate key lengths:

1. In the Embedded Web Server, click **Properties > Security**.
2. Click **Certificates > Certificate Key Length**.
3. For Minimum RSA Encryption Key Length, select an option:
   - **No Minimum**
   - **1024-bit**
   - **2048-bit***: This option is the default setting. This setting is FIPS 140 with Common Criteria compliant.
   - **4096-bit**

   Note: If FIPS 140 with Common Criteria compliance is enabled completely, options less than 2048 bits are not available.
4. For Minimum ECDSA Encryption Key Length, select **256-bit*** or **384-bit***. The default setting is **256-bit***. Both settings are FIPS 140 with Common Criteria compliant.
5. 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 and the relevant authentication credentials, such as user name, password, authentication certificate, and server validation certificate.
- Determine if the network supports an 802.1X failover VLAN. If supported, a failover VLAN provides an alternate, potentially limited, non-802.1X VLAN for clients that fail 802.1X Authentication, allowing for 802.1X configuration remediation.

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. Select the device behavior in the event of an 802.1X **Authentication Failure**.
    - Selecting **Block Network Access** prevents the device from connecting to the network in the event of an 802.1X Authentication Failure. The 802.1X settings should be reset from the front panel of the device, if a failure occurs when remote access is not possible. This is the default selection and recommended option for security.
    - Selecting **Connect Anyway** allows the device to connect to an alternate, non-802.1X network (if it is available and configured on the network) in the event of an 802.1X Authentication Failure. This option allows for flexibility in managing the device, when remote access is still possible after a failure.

6. For Authentication Method, select the method used on your network and provide the associated authentication information.

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

   You could require the printer to validate certificates used to encrypt 802.1X only if you select PEAPv0/EAP-MS-CHAPv2 or EAP-TLS as an authentication method.

   TLS authentication and server verification both require X.509 certificates. To use the features, before configuring 802.1X, install the necessary certificates on the Security Certificates page.

   - For PEAPv0/EAP-MS-CHAPv2:

     1. For Server Validation - Validate server using, select a certificate from the drop-down menu.

        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: Install the necessary certificates from the Security Certificates page before configuring 802.1X.

     2. For User Name (Device Name), type the user name.
     3. For Password, type and confirm a password.
     4. To save the new password, click **Select to save new password**.

   - For EAP-MS-CHAPv2:

     1. For User Name (Device Name), type the user name.
     2. For Password, type and confirm a password.
     3. To save the new password, click **Select to save new password**.

   - EAP-TLS:

     1. For Server Validation - Validate server using, select a certificate from the drop-down menu.

        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: Install the necessary certificates from the Security Certificates page before configuring 802.1X.

     2. For Device Certificate (TLS) - Authentication Certificate, select a certificate from the drop-down menu.

     Note: Install the necessary certificates from the Security Certificates page before configuring 802.1X.

     3. For User Name (Device Name), type the user name.

     Note: A password is not required for EAP-TLS as certificate exchange is used for authentication.

     Note: 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. Click **Save** and **Re-authenticate**.

Note: Re-authentication initiates a network restart, which results in a temporary loss of connectivity. If the connection is lost after the restart, check the following in the device control panel:

1. Print the configuration report at the device and confirm the configuration.
2. Confirm 802.1x configuration.

If 802.1X re-authentication is required irrespective of no change in 802.1X configuration, select **Re-authenticate** from the Xerox Embedded Web Server 802.1X page.

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**.

USB Port Management

Use this page to enable or disable USB host ports and USB device ports, and to manage USB device port policies.

You can prevent unauthorized access to the printer through USB host or Type A and Type B ports by disabling the ports. You can enable or disable each port independently.

Note: If your printer 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 necessary part in the compartment inside Tray 1.

To configure USB Port Management in the Embedded Web Server:

1. In the Embedded Web Server, click **Properties > Security > USB Port Management**.
2. To enable or disable the ports, click the Front (Type A) toggle button or Rear (Type A) toggle button.

Note: If the user disables a port, then an alert in yellow box appears as `Disabling a USB Port may impact features that requires use of the USB ports.`

Caution: Use caution when disabling ports, as this may affect the features and functions currently in use on this device. Although the USB settings can be changed at any time, the device may not recognize these changes until it has been restarted.

DEVICES INSTALLED IN A DISABLED PORT	CONSEQUENCES OF A DISABLED PORT
Wirelesss Adapter	Prevent the use of wireless networking and WiFi-Direct.
Bluetooth Adapter	Prevent the use of Bluetooth functionality, such as iBeacon.
Card Reader	Prevent the use of Smart Card Authentication when utilizing CAC or PIV card readers.
Storage Devices	Prevent the use of any storage device for all functions, such as SW upgrade, clone file installation, printing from or scanning to.
Memory Card Reader	Prevent the use of any memory card for all functions, such as SW upgrade, clone file installation, printing from or scanning to.
Hub	Prevent the use of a Hub for any purpose. USB device connected to the Hub will not be recognized.
Human Interface Devices (HID)	Prevent the use of an HID device (For example, Keyboard, Mouse, or Card Reader) and use of Convenience Authentication when utilizing card readers.
Audio Devices	Prevents the use of audio devices.

3. Click **Apply**.

Note: Few devices may require restart after enabling or disabling the port for changes to take effect.

A message appears as `Device must restart for changes to take effect`. Click **Restart Now** or click **Restart Later**.

Restart Later holds the selections in memory until the next restart. Then the selections take effect.

Restart Now shuts down the device at the next time it is idle (no mid-job shutdowns).

Note:

- Both USB host or Type A and Type B ports can be enabled or disabled. Enabling or Disabling Type A ports does not change the enablement of the Type B port.
- Enabling USB ports does not enable USB-related features:
  - Print From. For details, refer to Enabling Print From USB.
  - Scan To USB. For details, refer to Scan To USB.
- All USB host ports are enabled by default.
- The number of USB ports varies for each printer.

4. To enable or disable Type B port, click the toggle button.
5. In Direct Connection (Type B), you can set the Connection Timeout value for the USB device port.
6. For Connection Timeout, type the number of seconds that the printer waits in an inactive state before it disconnects from a device that is connected to the port. To disable the timeout, type `0`.

Note: The default value for Connection Timeout is 5 seconds.

7. To save changes to USB port settings, click **Save**.
   For changes to take effect, restart the printer.

USB PORT MANAGEMENT AT THE CONTROL PANEL

To configure USB Port Management at the control panel:

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **Security Settings > USB Port Management**.
3. At the USB Port Management screen, in the Front (Type A) area, to enable or disable port, click the toggle button.
4. In the Rear (Type A) area, to enable or disable port, click the toggle button.
5. To enable or disable Type B port, click the toggle button.
6. In Direct Connection (Type B), you can set the Connection Timeout value for the USB device port.
7. For Connection Timeout, type the number of seconds that the printer waits in an inactive state before it disconnects from a device that is connected to the port. To disable the timeout, type `0`.

Note: The default value for Connection Timeout is 5 seconds.

8. To save changes to USB port settings, click **Save**.
   For changes to take effect, restart the printer.

Image Overwrite Security for HDD Storage Devices

To ensure that unauthorized users cannot access image data on the device hard drive, you can delete and overwrite image data. Image data is defined as any in-process or temporary user data on the hard drive.

The Image Overwrite Security feature is available for devices with a traditional magnetic-based, spinning hard disk drive (HDD). For devices with flash-based storage, such as a solid-state drive (SSD), refer to Job Data Removal for SSD Storage Devices.

Note: The administrator password is required to access the Image Overwrite Security feature in the Embedded Web Server or at the control panel.

There are two options for Image Overwrite Security:

- Immediate Job Overwrite: This option 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. Immediate Job Overwrite is the preferred setting for high-security environments and is enabled by default.
- Disk Overwrite: This option allows scheduled or immediate disk overwrite.

There are two modes for overwriting image data:

- Full Overwrite Mode: This mode deletes all user-stored data from the device memory and hard drive. Before you run a full disk overwrite, it is recommended that you create a backup of your saved jobs. For details, refer to Backing Up Saved Jobs. A full disk overwrite takes approximately 60 minutes.
- Standard Overwrite Mode: This mode deletes all user-stored data from the device memory and hard drive, except the following:
  - Jobs and folders stored in the Reprint Saved Jobs feature
  - Jobs stored in the Scan to Mailbox feature
  - Fax Dial Directories, when a fax card is installed
  - Fax Mailbox contents, when a fax card is installed

  A standard disk overwrite takes approximately 20 minutes.

IMMEDIATE JOB OVERWRITE

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

The Immediate Job Overwrite feature is available for devices with a traditional magnetic-based, spinning hard disk drive. For devices with flash-based storage, such as solid-state drives and embedded multimedia cards (eMMC), use the Job Data Removal feature. For details, refer to Job Data Removal for SSD Storage Devices.

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

If Immediate Job Overwrite is not successful, the device prompts you to run the Disk Overwrite feature, which clears the error. To run Disk Overwrite, click the **Disk Overwrite** tab. For details, refer to Disk Overwrite.

Enabling Immediate Job 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**.
   To prevent the device from overwriting each job after it finishes processing, select **Disabled**.
5. To configure the number of passes, for **Number of Overwrite Passes**, select a value. The default is one overwrite pass. The maximum number of passes is three.
6. Click **Apply**.

Enabling Immediate Job Overwrite at the Control Panel

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

DISK OVERWRITE

You can use the Disk Overwrite feature to overwrite user-stored data on the device hard disk drive.

There are two options for Disk Overwrite feature:

- Scheduled: This option allows you to schedule a Standard or Full disk overwrite to occur at a specific time: daily, weekly, or monthly. For details, refer to Scheduling Disk Overwrite.
- Overwrite Now: This option allows you to perform a Standard or Full disk overwrite immediately. For details, refer to Enabling Immediate Disk Overwrite.

The Disk Overwrite feature is available for devices with a traditional magnetic-based, spinning hard disk drive. For devices with flash-based storage, such as solid-state drives and embedded multimedia cards (eMMC), use the Job Data Removal feature. For details, refer to Job Data Removal for SSD Storage Devices.

Any Disk Overwrite action:

- Takes the device offline.
- Cannot be canceled.

Scheduling Disk Overwrite

Note:

- After a disk overwrite action begins, you cannot cancel the operation.
- The disk overwrite action takes the device offline.

- For details on the Scheduled Disk Overwrite feature, in the Overwrite Mode area, click https://www.xerox.com/security.

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:
   - **Monthly**: For this option, select a day of the month, then set the time.
   - **Weekly**: For this option, select a day of the week, then set the time.
   - **Daily**: For this option, set the time.

   To set the time, type the hours and minutes, then select **AM** or **PM**.
7. For Confirmation Report, 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.
8. For Overwrite Mode, select an option:
   - **Standard**: This option deletes all image data from the device memory and hard drive, except the following:
     - Jobs and folders stored in the Reprint Saved Jobs feature
     - Jobs stored in the Scan to Mailbox feature, when this feature is installed
     - Fax Dial Directories, when a fax card is installed
     - Fax Mailbox contents, when a fax card is installed
   - **Full**: This option deletes all image data from the device memory and hard drive. Before you run a full disk overwrite, it is recommended that you create a backup of your saved jobs. For details, refer to Backing Up Saved Jobs.
9. To configure the number of passes, for **Number of Overwrite Passes**, select a value. The default is one overwrite pass. The maximum number of passes is seven.

   Note:

   - A single pass of a standard disk overwrite takes approximately 12 minutes.
   - A single pass of a full disk overwrite takes approximately 16 minutes.
   - Additional passes extend the overwrite time proportionally.
10. Click **Apply**.

Scheduling Disk Overwrite at the Control Panel

1. At the control panel, touch **Device**, then touch **Tools**.
2. Touch **Security Settings > Image Overwrite Security**.

3. Touch the **Disk Overwrite** tab.
4. For Scheduled Overwrite, select a frequency:
   - **Monthly**: For this option, touch **Day of Month**, select a date, then set the time.
   - **Weekly**: For this option, touch **Day of Week**, select a day, then set the time.
   - **Daily**: For this option, set the time.

   To set the time, touch **Overwrite Time**, select the hours and minutes, then select **AM** or **PM**.
5. To change the overwrite mode, touch **Overwrite Mode**, then select **Standard** or **Full**.
6. Touch **Confirmation Report**, then select an option.
7. Touch **OK**.

Enabling Immediate Disk Overwrite

Use the Overwrite Now feature to start a standard or full disk overwrite.

The Overwrite Now feature is available for devices with a traditional magnetic-based, spinning hard disk drive. For devices with flash-based storage, such as solid-state drives and embedded multimedia cards (eMMC), use the Job Data Removal feature. For details, refer to Job Data Removal for SSD Storage Devices.

Note:

- After you initiate a disk overwrite, you cannot cancel the operation.
- The disk overwrite action takes the device offline. When the process completes, the device restarts.
- For details on the Disk Overwrite feature, click **Advanced Settings**. In the Overwrite Mode area, click https://www.xerox.com/security.

1. In the Embedded Web Server, click **Properties > Security**.
2. Click **Image Overwrite Security**.
3. Click the **Disk Overwrite** tab.
4. To start a disk overwrite:
   a. Click the **Overwrite Now** tab.
   b. For Confirmation Report, select an option:
      - **On**: Select this option to print a report after the device removes job data.
      - **Errors Only**: Select this option to print a report only if an error occurs.
      - **Off**: Select this option to disable confirmation report printing.
   c. Click **Advanced Settings**.

d. For Overwrite Mode, select an option:

- **Standard**: 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.
- **Full**: To overwrite all user image data or job data, select **Full**. Full Image Overwrite takes approximately 60 minutes to complete. Before you run a full disk overwrite, it is recommended that you create a backup of your saved jobs. For details, refer to Backing Up Saved Jobs.

e. To configure the number of passes, for **Number of Overwrite Passes**, select a value. The default is one overwrite pass. The maximum number of passes is seven.

Note:

- A single pass of a standard disk overwrite takes approximately 12 minutes.
- A single pass of a full disk overwrite takes approximately 16 minutes.
- Additional passes extend the overwrite time proportionally.

f. Click **Start Disk Overwrite Now**.

g. To acknowledge the warning message, click **OK**.

Enabling Immediate Disk Overwrite at the Control Panel

1. At the control panel, 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 select **Standard** or **Full**.
5. 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**.

Job Data Removal for SSD Storage Devices

To ensure that unauthorized users cannot access image data stored in flash-based storage, you can delete job data. Job data is defined as any in-process or temporary user data stored in flash-based storage.

The Job Data Removal feature is available for devices with non-spinning, flash-based storage, such as a solid-state drive (SSD). For devices that have a traditional hard disk drive (HDD), refer to Image Overwrite Security for HDD Storage Devices.

Note: The administrator password is required to access the Job Data Removal feature in the Embedded Web Server or at the control panel.

There are two modes for Job Data Removal:

- Full Removal: This option deletes all stored job data from the flash-based storage.
- Standard Removal: This option deletes all stored job data from the flash-based storage, except the following:
  - Jobs and folders stored in the Reprint Saved Jobs feature.
  - Jobs stored in the Scan to Mailbox feature.
  - Fax Mailbox contents, when a fax card is installed.

REMOVING JOB DATA NOW

Use the Remove Job Data Now feature to remove job data immediately.

The Full Removal Mode option deletes all job data from the flash-based storage. Before you run a full removal, it is recommended that you create a backup of your saved jobs. For details, refer to Backing Up Saved Jobs.

Note:

- After job data removal begins, you cannot cancel the operation.
- The job data removal action takes the device offline. When the process completes, the device restarts.

To remove job data immediately in the Embedded Web Server:

1. In the Embedded Web Server, click **Properties > Security > Job Data Removal**.
2. Click the **Remove Now** tab.
3. For Confirmation Report, select an option:
   - **On**: Select this option to print a report after the device removes job data.
   - **Errors Only**: Select this option to print a report only if an error occurs.
   - **Off**: Select this option to disable confirmation report printing.
4. To perform a Standard Removal:
   a. Click **Remove Job Data Now**.
   b. To acknowledge the warning message, click **OK**.
5. To perform a Full Removal:
   a. Click **Advanced Settings**.

b. Select **Full**.

c. Click **Remove Job Data Now**.

d. To acknowledge the warning message, click **OK**.

Removing Job Data at the Control Panel

Use the Remove Job Data Now feature to remove job data immediately.

Note:

- After job data removal begins, you cannot cancel the operation.
- The job data removal action takes the device offline. When the process completes, the device restarts.

To remove job data immediately at the control panel:

1. At the control panel, touch **Device**, then touch **Tools**.
2. Touch **Security Settings > Job Data Removal**.
3. Touch the **Remove Now** tab.
4. Touch **Removal Mode**, then select **Standard Removal** or **Full Removal**.
5. Touch **Confirmation Report**, then select an option.
6. Touch **Remove Job Data Now**.
7. At the prompt, touch **Begin Job Data Removal**.

SCHEDULING JOB DATA REMOVAL

You can schedule job data removal to occur at regular intervals.

The Scheduled Removal feature removes user-stored data from the flash-based storage at a specific time.

Note:

- After job data removal begins, you cannot cancel the operation.
- The job data removal action takes the device offline. When the process completes, the device restarts.

The Full Removal Mode option deletes all user-stored data from the flash-based storage. Before you run a full removal, it is recommended that you create a backup of your saved jobs. For details, refer to Backing Up Saved Jobs.

To schedule job data removal in the Embedded Web Server:

1. In the Embedded Web Server, click **Properties > Security > Job Data Removal**.
2. Click the **Scheduled** tab.
3. In the Enablement area, select **Enabled**.

Note: To disable Scheduled Job Data Removal, select **Disabled**.

4. Under Scheduling, for Frequency, select how often the device removes job data.
   - **Monthly**: For this option, select a day of the month, then set the time.
   - **Weekly**: For this option, select a day of the week, then set the time.
   - **Daily**: For this option, set the time.

   To set the time, type the hours and minutes, then select **AM** or **PM**.
5. For Confirmation Report, select an option:
   - **On**: Select this option to print a report after the device removes job data.
   - **Errors Only**: Select this option to print a report only if an error occurs.
   - **Off**: Select this option to disable confirmation report printing.
6. For Mode, select an option:
   - The Full Removal Mode option deletes all user-stored data from the flash-based storage.
   - The Standard Removal Mode option deletes all job data from the flash-based storage, except the following:
     - Jobs and folders stored in the Reprint Saved Jobs feature
     - Jobs stored in the Scan to Mailbox feature
     - Fax Mailbox contents, when a fax card is installed
7. Click **Save**.

Scheduling Job Data Removal at the Control Panel

To schedule job data removal at the control panel:

1. At the control panel, touch **Device**, then touch **Tools**.
2. Touch **Security Settings > Job Data Removal**.
3. Touch the **Scheduled** tab.
4. For Scheduled Based Removal, select a frequency:
   - **Monthly**: For this option, touch **Day of Month**, select a date, then set the time.
   - **Weekly**: For this option, touch **Day of Week**, select a day, then set the time.
   - **Daily**: For this option, set the time.

   To set the time, touch **Removal Time**, select the hours and minutes, then select **AM** or **PM**.

   Note: To disable Scheduled Job Data Removal, touch **Never**.
5. Touch **Removal Mode**, then select **Standard Removal** or **Full Removal**.
6. Touch **Confirmation Report**, then select an option.
7. 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 password 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**.

Personalized Information

By default, some personally identifiable information for the logged-in user appears on the control panel touch screen.

To suppress the display of login names and completed job details, use the Personally Identifiable Information (PII) page in the Embedded Web Server.

1. In the Embedded Web Server, click **Properties > Security > Personalized Information**.
2. At the Personally Identifiable Information (PII) page, configure settings as needed.
   a. For Login Name, select **Show** or **Hide**.
   b. For Completed Jobs, select **Show** or **Hide**.
3. Click **Apply**.

Verifying the Software

The Software Verification Test checks the software files to confirm that they are not corrupt or have not been modified.

If the printer software appears to function 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 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 to addresses in the address book only, touch **Limit to Address Book Entries**.
4. Touch **OK**.

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.

For administrators, the default password for the admin account is the device serial number. If you do not change the default administrator password using the installation wizard, the printer requires you to change the password when you first log in as administrator in the Embedded Web Server. If you do not change the default administrator password, you cannot access the administrator functions on the device.

If you choose to continue to use the default administrator password or a password of `1111`, each time that you log in as administrator, the device reminds you to choose a more secure password for the admin account. For details on changing the administrator password, refer to Changing the Administrator Password.

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 that you create a number of local accounts with administrator rights.

ENABLING THE ADMINISTRATOR PASSWORD RESET

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

DISABLING THE ADMINISTRATOR PASSWORD RESET

To disable the administrator 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**.

Note: If you disable the administrator 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.

Printing

This chapter contains:

Paper Management 216
Saving and Reprinting Jobs 222
Printing Jobs from the Embedded Web Server 225
Configuring General Print Settings 226
Printing an Error Sheet 227
Managing Banner Page Printing Options 228
Configuring Secure Print Settings 230
Hold All Jobs 232
Showing Printer Font Information 233
Page Description Languages 234
UNIX, Linux, and AS/400 Printing 240
Configuring Print From 243
Allowing Users to Interrupt Active Print Jobs 246
Specifying Output Settings at the Control Panel 247
Specifying Print Settings Defaults and Policies 248

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

You can use the Paper Size Preference feature to set the preferred paper size to imperial or metric. Paper size options that use the selected units setting appear at the top of the Paper Selection list on the Print tab and User Interface.

1. In the Embedded Web Server, click **Properties > General Setup > Paper Management**.
2. Click the **Paper Size Preference** tab.
3. To set the paper size preference, select an option:
   - **Inches**: This option sets the paper size preference to imperial sizes.
   - **Metric**: This option sets the paper size preference to metric sizes.
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**.

Setting Measurements at the Control Panel

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **Device Settings > General > Measurements**.
3. For Units, select an option:
   - **Inches**: This option sets the measurement units to inches.
   - **Metric**: This option sets the measurement units to millimeters.

Note: The named paper sizes are only text and are not impacted by this setting. Measurement units change the units used for the tray and scan custom size settings.

4. For Numeric Separator, select an option:
   - **Comma**: This option separates the units of paper-size with a comma.
   - **Period**: This option separates the units of paper-size with a period.
5. Touch **OK**.

CONFIGURING TRAY SETTINGS

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

You can set the tray mode to Fully Adjustable or Dedicated. When a paper tray is set to Fully Adjustable mode, you can change the paper settings each time that you load the tray. When a paper tray is set to Dedicated mode, the control panel prompts you to load a specific paper size, type, and color.

Note:

- The Bypass Tray is set always as a Fully Adjustable tray.
- For a Dedicated tray, you can set any media size that the tray supports as a dedicated size.

To configure the tray settings:

1. In the Embedded Web Server, access the Paper Management page using one of the following methods:
   - Click **Properties > General Setup > Paper Management**.
   - Click **Home**, then in the Trays area, click **Settings**.
2. Click the **Tray Content & Settings** tab.
3. To edit a specific paper tray, on the row for that tray, click **Edit**.
4. For Tray Type, select an option:
   - **Fully Adjustable**: This option prompts you to confirm the type of paper loaded in the tray.
   - **Dedicated**: This option prompts you to set up a tray to support a specific paper size, type, and color.

     If you select **Dedicated**, to edit the paper size, type, and color for this tray, click the **Edit**.

   Note: An error occurs if a different paper size is loaded into the dedicated tray. But it assumes that the paper you load in the tray is of the specified type and color.
5. For Priority, set the priority for the selected tray. Assign a priority number from 1–99. The lower the number, the higher the priority.

   For example, the printer uses paper from the lowest numbered priority tray first. If that tray is empty, the printer prints using paper from the tray with the next priority in the ranking.
6. To configure the printer to select the tray automatically, for Auto Selection, select **Enabled**.

7. For Bypass Tray, for Empty Tray Alerts, select the **Display Empty Tray Alerts for Bypass Trays and Inserters** check box.

   Note: Empty Tray Alerts option is visible only in Embedded Web Server.

   This option results in Empty Tray Alerts for network jobs for these trays.

   Note: If these trays are typically left empty unless they are actively in use, enabling this option results in frequent empty tray alerts.

8. Click **Save**.

Configuring Tray Settings at the Control Panel

To configure the tray settings at the control panel:

1. At the printer control panel, touch **Device**.
2. Touch **Tools > Device Settings > Paper Management**.
3. Touch **Tray Settings**, then select a tray. Configure settings as needed:
   a. To set the Mode, touch **Fully Adjustable** or **Dedicated**.
   b. To specify the paper settings for a dedicated tray, touch **Edit**. Set the paper size, type, and color, then touch **OK**.
   c. To set the Priority, touch the number field. Assign a priority number from 1–99. The lower the number, the higher the priority.
   d. To configure the printer to select the tray automatically, for Auto Selection, touch **Enabled**.
4. To save the tray settings, touch **OK**.

SELECTING TRAY 1 SETTINGS

The Tray 1 Usage setting notifies the device about the paper Tray 1 configuration type.

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**.

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, 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, .jpg, .txt, .prn, and .tiff 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 Basic Report 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. To reduce the spooling rate for network jobs, for Reduce spooling rate of network jobs (to prevent rejection errors), select **Enabled**.
7. For Held Job Policy, select options as needed.
   - To require active jobs to print in the order that they were received after a held job, for Allow Print Around on Held Jobs, select **No**.
   - To enable users 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**.
8. To set the amount of time that the device holds print jobs before jobs are deleted, for Delete Held Jobs After, enter the number of days, hours, and minutes.
9. 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.
10. To print an error sheet when a print job fails, for Print Error Sheets, select **Enable**.
11. In the Defaults & Policies area, for each setting, select options as needed.
12. 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 V3 PRINT DRIVER

1. With your file open in the application, click the **File** menu, then click **Print**.
2. In the application Print window, from the Printer Name menu, select your printer.
3. To access the print settings for the job, click **Properties**.
4. Click the **Advanced** tab.
5. Click **Job ID**.
6. From the list, select **Print ID on a Banner Page**.

7. 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.

   Note: **Release Secure Print Jobs Upon Confirmation** option prompts the user to resume a job being held. By default, the option is disabled. This option can be enabled or disabled only if **Release Jobs Without Prompting for Passcode** is selected.

   - **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. In the General area, to set the minimum passcode length, for Secure Print Passcode Length, type a number from 4–10.
   Passcode length applies to Secure Print jobs submitted through Embedded Web Server, IPP (AirPrint) and Print Driver submission methods.

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.

   Print drivers need to be specifically configured to acquire settings from the device.

   Note: This option is not applicable for Universal Print.

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**.

Showing Printer Font Information

The printer can print text using PostScript emulation fonts and PCL fonts. Permanent fonts are installed on the printer by default. You cannot delete Permanent fonts. You can install downloaded fonts on the printer using the Xerox® Font Management Utility. You can download the Xerox Font Management Utility from the Xerox website at www.support.xerox.com.

To show font information:

1. In the Embedded Web Server, click **Properties > Apps > Printing > Printer Fonts**.
2. In the Samples area, select a set of fonts.
3. Click **Print Font Samples**.
4. To select the fonts in the printer font list, for View by Font Type, select an option.

Page Description Languages

A Page Description Language (PDL) specifies the arrangement of text, images, and graphics on a printed page using commands that the printer can interpret. PDLs define page elements independently of printer technology, so that the appearance of a printed page is consistent, regardless of the device used.

You can configure the settings for processing print jobs that use a particular PDL. The following PDLs are supported:

- PostScript: For details, refer to PostScript®.
- PCL: For details, refer to PCL.
- PDF: For details, refer to PDF.
- TIFF or JPG: For details, refer to TIFF/JPG.

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.

POSTSCRIPT®

The PostScript® page in the Embedded Web Server displays the Adobe PostScript® emulation PDL level and version that is used for processing print jobs.

To set PostScript output options:

1. In the Embedded Web Server, click **Properties > Apps > Printing**.
2. Click **Page Description Languages > PostScript®**.
3. At the PostScript® page, for Image Quality, select the print quality for PostScript print jobs.

   Note: Higher quality settings improve appearance, but increase the time taken to complete the print job.
4. Click **Save**.

PCL

To view or modify the parameters that control how the printer processes print jobs that use Printer Command Language (PCL), use the PCL General Settings page in the Embedded Web Server.

Note: If the device detects transparent text in a PCL print job, it prints the text as white text.

You cannot configure this setting.

To modify PCL settings:

1. In the Embedded Web Server, click **Properties > Apps > Printing**.
2. Click **Page Description Languages > PCL**.
3. Click the **General Settings** tab.
4. In the Options area, configure the settings as required:
   a. For Pitch Size, type the pitch size for the default font.
   b. For Point Size, type the point size for the default font.

c. For Font Name, select the default font type.

d. For Symbol Set, select the PCL symbol set to use when printing PCL or text files. The printer uses this symbol set when the print driver does not specify the PCL symbol set within the print job.

e. For Lines Per Page, specify how many lines of text fit on a page. This setting determines the line spacing for a printed page. The allowable range is 5–180 lines per page. For a portrait letter-size page, the default setting is 60 lines per page.

f. To change all line feed characters to carriage returns with line feeds, select the check box for **Treat "LF" as "CR" + "LF"**. If the documents do not use the CR+LF combination, use this option.

g. For Default Orientation, select the default page orientation.

h. For Edge-to-Edge Printing, select an option.

- **Normal Print Margins (Recommended)**: Select this option to disable edge-to-edge printing.
- **Edge-to-Edge Printing on All Prints**: Select this option to enable edge-to-edge printing. The device prints with no border for PCL print jobs.

i. To ignore any PCL tray commands, select the check box for **Ignore Tray Commands**.

j. To rotate PCL envelopes, select the check box for **Rotate Envelopes**.

k. To rotate the output for portrait output, select the check box for **Wide A4**, as needed.

l. For Suppress Blank Pages, select an option:

- **Do Not Suppress Blank Pages**: This option allows blank pages sent in a print job to be printed.
- **Suppress All Blank Pages**: This option prevents blank pages in a print job from printing.
- **Suppress Last Page if Blank**: If the last page of a print job is blank, this option prevents the last page from printing.

Note: When you change the **Suppress Blank Pages** setting, after you select **Apply**, a restart of the device is required.

5. Click **Apply**.
6. To restart the printer, click **Reboot Machine**.

Setting PCL Tray Mapping

PCL Tray Mapping customizes the PCL paper source commands to match attributes for paper in the trays, without requiring additional PCL codes. Tray mapping eliminates the need to remap drives in third-party applications that use PCL commands.

Tray mapping enables you to map PCL paper source trays to Xerox device trays for the following tray numbers:

- PCL source tray: 0–8, 20–24, 30–33
- Xerox device trays: 1–6

Note: Depending on the configuration of your Xerox device, and depending on which of the optional trays are installed, the available device trays vary.

To configure tray mapping:

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

2. Click **Page Description Languages > PCL**.
3. Click the **Tray Mapping** tab.
4. The Options area displays the PCL source tray numbers. For the source tray that you need to map, select a device tray from the list.
   - **Auto Select**
   - **Use Currently Selected Tray**
   - Tray number. An option is available for each paper tray in the configuration.
5. Repeat step 4 for each tray mapped in the PCL application.
6. Click **Save**.

Note: To restore the default tray settings for your device, click **Restore Feature Defaults**. Depending on the configuration of the device, the default settings can vary.

PDF

Use the PDF page in the Embedded Web Server to view the PDF version used to process PDF files, and to set default settings for processing PDF files.

Note: The default settings appear as the Automatic settings for the Print from USB feature at the device control panel. You can override these settings at the control panel.

To configure default settings for PDF:

1. In the Embedded Web Server, click **Properties > Apps > Printing**.
2. Click **Page Description Languages > PDF**.

3. In the Default Settings area, for Scale Image, select an option:
   - **None**: Select this option to print the image at its original size. No scaling is applied.
   - **Fit to Page**: Select this option when the image is smaller or larger than the target paper size. The image is scaled to fit the paper size. The image is not cropped and white space can occur. This option is the default.

   Note: The image is scaled so that the longest edge of the image fits on the page. This scaling can result in blank areas on opposite sides of the printed image.

   - **Fill Entire Page**: Select this option when the image is smaller or larger than the target paper size. The image is scaled to fit the paper size so that no white space occurs. Typically, image cropping occurs.

   Note:

     - The image is scaled so that the smallest edge of the image fits on the page.
     - The way in which the image is cropped depends on the image dimensions, the centering option chosen, and whether automatic rotation is applied.

   - **Shrink to Fit**: Select this option when the image is larger than the target paper size. The image is scaled down to fit the paper size. For images that are smaller than or equal to the target paper size, no scaling is applied.
   - **Custom Scale (25–400%)**: Select this option to scale the image to a specific percentage, then enter a reduced or enlarged percentage value. The default is 100%, no scaling applied.

   Note: Scale Image does not work with PostScript files whose images cannot be modified.

4. For Center, select an option:
   - **Center Image**: Select this option to center the scaled or unscaled image on the target output sheet. This option is the default.
   - **Do Not Center**
5. Smart rotation, if enabled, can provide a better fit of the image on the output sheet by maximizing the printed area and minimizing the white space. Depending on the scaling option selected, the Smart Rotate option varies.
   - For Scale Image, if you selected Fit to Page or Shrink to Fit, for Smart Rotate, select an option:
     - **Rotate to Reduce Whitespace**: Select this option for the device to determine if a 90–degree rotation before scaling can improve the fit of the image on the page. An improved fit reduces white space.
     - **Do Not Smart Rotate**
   - For Scale Image, if you selected None, Fill Entire Page, or Custom Scale, for Smart Rotate, select an option:
     - **Rotate to Reduce Cropping**: Select this option for the device to determine if a 90–degree rotation before scaling can improve the fit of the image on the page. An improved fit reduces image cropping.
     - **Do Not Smart Rotate**
6. Click **Apply**.

TIFF/JPG

Use the TIFF/JPG page in the Embedded Web Server to view the Tagged Image File Format (TIFF) version used to process TIFF files, and the JPG version used to process JPG files.

You can use this page to set default settings for processing TIFF and JPG files. The default settings apply to both file formats.

Note: The default settings appear as the Automatic settings for the Print from USB feature at the device control panel. You can override these settings at the control panel.

To configure default settings for TIFF and JPG:

1. In the Embedded Web Server, click **Properties > Apps > Printing**.
2. Click **Page Description Languages > TIFF/JPG**.
3. In the Default Settings area, for Scale Image, select an option:
   - **None**: Select this option to print the image at its original size. No scaling is applied.
   - **Fit to Page**: Select this option when the image is smaller or larger than the target paper size. The image is scaled to fit the paper size. The image is not cropped and white space can occur. This option is the default.

   Note: The image is scaled so that the longest edge of the image fits on the page. This scaling can result in blank areas on opposite sides of the printed image.

   - **Fill Entire Page**: Select this option when the image is smaller or larger than the target paper size. The image is scaled to fit the paper size so that no white space occurs. Typically, image cropping occurs.

   Note:

   - The image is scaled so that the smallest edge of the image fits on the page.
   - The way in which the image is cropped depends on the image dimensions, the centering option chosen, and whether automatic rotation is applied.

   - **Shrink to Fit**: Select this option when the image is larger than the target paper size. The image is scaled down to fit the paper size. For images that are smaller than or equal to the target paper size, no scaling is applied.
   - **Custom Scale (25–400%)**: Select this option to scale the image to a specific percentage, then enter a reduced or enlarged percentage value. The default is 100%, no scaling applied.

   Note: Scale Image does not work with PostScript files whose images cannot be modified.
4. For Center, select an option:
   - **Center Image**: Select this option to center the scaled or unscaled image on the target output sheet. This option is the default.
   - **Do Not Center**

5. Smart rotation, if enabled, can provide a better fit of the image on the output sheet by maximizing the printed area and minimizing the white space. Depending on the scaling option selected, the Smart Rotate option varies.
   - For Scale Image, if you selected Fit to Page or Shrink to Fit, for Smart Rotate, select an option:
     - **Rotate to Reduce Whitespace**: Select this option for the device to determine if a 90–degree rotation before scaling can improve the fit of the image on the page. An improved fit reduces white space.
     - **Do Not Smart Rotate**
   - For Scale Image, if you selected None, Fill Entire Page, or Custom Scale, for Smart Rotate, select an option:
     - **Rotate to Reduce Cropping**: Select this option for the device to determine if a 90–degree rotation before scaling can improve the fit of the image on the page. An improved fit reduces image cropping.
     - **Do Not Smart Rotate**
6. Click **Apply**.

UNIX, Linux, and AS/400 Printing

UNIX-based printing uses LPD/LPR port 515 or lp to port 9100 to provide printer spooling and network print server functionality. 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 the 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. Choose from the available files:
   - 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
   - XeroxOfficev5Pkg-Linuxi686-x.xx.xxx.xxxx.rpm to support RPM-based 32-bit Linux environments
   - XeroxvOffice5Pkg-Linuxi686-x.xx.xxx.xxxx.deb to support Debian-based 32-bit Linux environments
   - XeroxOfficev5Pkg-Linuxx86_64-x.xx.xxx.xxxx.rpm to support RPM-based 64-bit Linux environments
   - XeroxOfficev5Pkg-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 for your environment:
   - AIX: `rpm -U Xeroxv5Pkg-AIXpowerpc-x.xx.xxx.xxxx.rpm`
   - HPUX: `swinstall -s Xeroxv5Pkg-HPUXia64-x.xx.xxx.xxxx.depot.gz \*`
   - 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`.

3. To install the Xerox Office standard driver, log in as root, then type the following command for your environment:
   - Linux (RPM based): `rpm -U XeroxOfficev5Pkg-Linuxi686-x.xx.xxx.xxxx.rpm`
   - Linux (Debian based): `dpkg -i XeroxOfficev5Pkg-Linuxi686-x.xx.xxx.xxxx.deb`

   The installation creates a XeroxOffice directory in `/opt/XeroxOffice/prtsys`.

Launching the Xerox® Printer Manager

To launch the Xerox® Printer Manager, log in as root, type `xeroxofficeprtmgr`, then press **Enter** or **Return**.

PRINTING FROM A LINUX WORKSTATION

To print from a Linux workstation, install a Xerox® print driver for Linux or a CUPS print driver. You do not need both drivers.

It is recommended 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 on the Workstation

1. Download the Xerox® PPD for CUPS from the Drivers and Downloads page on the Xerox Support website.
2. Copy the PPD 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.

ADDING THE PRINTER

1. Verify that the CUPS daemon is running.
2. Open a Web browser and type **http://localhost:631/admin**, then click **Enter** or **Return**.
3. For User ID, type **root**. For password, type the root password.
4. Click **Add Printer** and follow the onscreen prompts to add the printer to the CUPS printer list.

PRINTING WITH CUPS

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 click **Enter**.
2. To print to a specific printer in Berkeley, type: **lpr -Pprinter filename**, then click **Enter**.

AS/400

Xerox provides Work Station Customization Object (WSCO) files to support IBM i V6R1 or later. A Work Station Customization Object is a look-up table that the host print transform (HPT) uses to translate AS/400 commands to the equivalent PCL code that is specific to a particular printer. A WSCO file can modify many print features, including: paper input tray, 2-sided printing, characters per inch, lines per inch, orientation, fonts, and margins.

The XTOOLS library provides a source WSCO file for each supported Xerox® printer or device. The library and installation instructions are available from www.support.xerox.com.

To install the XTOOLS library, select the downloadable files for the IBM AS/400 operating system, unzip the downloaded `XTOOLSxxxx.zip` file, then follow the instructions to install the library. Download and install the library only once.

Note:

- The host print transform works only on AFPDS and SCS files. To use the WSCO for printing, convert IPDS-formatted printer files to AFPDS files.
- Administrator credentials with IOSYSCFG permissions are required 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.

Configuring Print From

The Print From feature allows users to browse and print from enabled locations using the Print From App on the device control panel.

Use the Print From Setup page in the Embedded Web Server to enable browsing and printing from the following locations:

- Cloud service folders: Dropbox, Google Drive, and Microsoft OneDrive. For details, refer to Cloud Browsing Enablement.
- Mailbox folders on the printer hard drive. For details, refer to Enabling Print From Mailbox.
- Folders stored on a USB flash drive that is connected to the USB port on the printer control panel. For details, refer to Enabling Print From USB.

Note: Only USB Flash drives formatted to FAT16, FAT32, and exFAT file systems are supported. exFAT support is a licensed feature that requires a purchased FIK.

Note: To use the Scan To USB or Print From USB app, ensure that at least one USB Type A Port is enabled.

CLOUD BROWSING ENABLEMENT

Use this feature to enable cloud folder browsing in the Print From App.

Note:

- Enabled cloud services appear as cloud locations in the Print From App on the device control panel.
- Cloud locations that are not enabled are hidden from view in the Print From App.

To enable cloud services:

1. In the Embedded Web Server, click **Properties > Apps**.
2. Click **Print From > Setup**.
3. In the Cloud Services area, configure the settings:
   a. For Allow Cloud Browsing, select the check box.

Note:

- Both logged-in and non-logged-in users can use Cloud Authentication. Logged-in users are those who have done initial authentication at the device control panel touch screen. Non-logged-in users are guest users who access the device without any authentication.
- Authentication for cloud services is independent of authentication for login to the device or access to network services.

   b. To set the Cloud Services login session retention policy, for Authenticated users will remain logged-into Cloud Services, select an option:

- **Always**: This option instructs the printer to retain the cloud login session for a non-guest user across device logins.
- **Never**: This option instructs the printer to delete the cloud login session for a non-guest user at the end of a session.

- **Let Each User Choose**: This option instructs the printer to prompt a non-guest user for consent to retain the cloud login session.

Note:

- The default setting for the cloud login session retention policy is **Always**.
- The login session retention policy does not apply to non-logged-in guest users. After the session ends, the device does not retain the cloud login session of a guest user.
- The login session retention policy applies to both Print From and Scan To functions.
- If the device authentication method is changed, any retained cloud login sessions are deleted automatically.
- If cloud sessions are not used for 366 days, the sessions expire. Expired sessions are deleted from the device automatically. Users with expired sessions are required to reenter credentials to access the cloud service.

c. To enable printing from cloud destinations, select options as needed:

- To enable printing from a Dropbox folder, select the check box for **Dropbox**.
- To enable printing from a Google Drive folder, select the check box for **Google Drive**.
- To enable printing from a Microsoft OneDrive folder, select the check box for **Microsoft OneDrive**.

Note:

- When cloud browsing is enabled or disabled in the Print From App, cloud browsing is not enabled or disabled in the Scan To App automatically.
- When a cloud service is enabled and selected in the Print From App, users are prompted for credentials to access the cloud service. On successful authentication, users can access the cloud service and see authorized documents.
- To select a document in the Print From App, users can browse folders in the cloud repository only. Users cannot create or delete folders in the cloud repository.
- To print a document in the Print From App, users can select a print-ready file only. For example, a PDF file.

4. Click **Apply**.

ENABLING PRINT FROM MAILBOX

The Print From Mailbox feature allows you to print a file that is stored in a folder on the printer hard drive.

Before you begin, ensure that Scan To Mailbox is enabled. For details, refer to Enabling or Disabling Scan To Mailbox.

Note: Enable Scan To Mailbox, then enable Print From Mailbox.

1. In the Embedded Web Server, click **Properties > Apps**.
2. Click **Print From > Setup**.
3. In the Mailbox area, select the check box for **Enable Print From Mailbox**.

4. Click **Apply**.

Note: For instructions on using this feature, refer to the *User Guide* for your printer model.

ENABLING PRINT FROM USB

The Print From USB feature allows you to print a file that is stored on a USB flash drive from the USB port on the printer control panel.

Note: Only USB Flash drives formatted to FAT16, FAT32, and exFAT file systems are supported. exFAT support is a licensed feature that requires a purchased FIK.

Before you begin, ensure that the USB port is enabled. For details, refer to USB Port Management.

1. In the Embedded Web Server, click **Properties > Apps**.
2. Click **Print From > Setup**.
3. In the USB area, select the check box for **Enable Print From USB**.
4. Click **Apply**.

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 at the Control Panel

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, then touch **OK**.
   - **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 how the device handles a print job that requires staples when the stapler is empty, select **Out of Staples Options**. Select an option, then touch **OK**.
6. To specify the default output location for jobs that do not have finishing options, select **Output Location**. Select an option, then touch **OK**.
7. To specify where the device applies staples to a print job, select **Staple Productivity Mode**, select an option, then touch **OK**.
8. To specify whether jobs are offset in the output tray, touch **Offset**. As needed, select or clear the check boxes for **Center Tray Offset**, **Offsetting of Sets Within Jobs**, and **Conditional Finisher Offset**. Touch **OK**.

   For more information on **Conditional Finisher Offset**, refer to Specifying Print Settings Defaults and Policies.

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.

Specifying Print Settings Defaults and Policies

To set the Print Settings Defaults and Policies in the Embedded Web Server:

1. In the Embedded Web Server, click **Properties > Apps > Printing > General**.
2. At the Print Settings, go to Defaults & Policies.

   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. To set the number of copies to print by default, for Copies, enter a number.
4. To print jobs in collated sets, for Collate, select **Enabled**.
5. For 2-Sided Printing, select an option:
   - **1-Sided Print**: This option prints on one side of the media. Use this option when you print on transparencies, envelopes, labels, or other media that cannot be printed on both sides.
   - **2-Sided Print**: This option prints the job on both sides of the paper to allow binding on the long edge of the paper.

   Note: 2-Sided Print option is the default setting for 2-Sided Printing.
   - **2-Sided Print, Flip on Short Edge**: This option prints on both sides of the paper to allow binding on the short edge of the paper.
6. For Output Color, select an option.
7. To set the print job for normal printing, for Job Type, select **Normal Print**.
8. To set the paper feed orientation, for Paper Feed Edge Default, select an option.
9. To set the default paper size, for Paper Size, select an option.
   To set the default paper type and paper color, refer to Setting Default Paper Type and Color.
10. For Staple, select an option.
11. To scale the print automatically, for Scale PostScript® / PCL 6 print jobs to fit substituted paper size, select **On**.
12. For Scale PostScript® / PCL Suppress Blank Pages, select an option:
    - **Do Not Suppress Blank Pages**: This option prints all blank pages in a print job.
    - **Suppress All Blank Pages**: This option prevents all blank pages in a print job from printing.
    - **Suppress Last Page if Blank**: This option prevents the last page from printing if the page is blank.
13. To offset hard-copy output in the center tray, for Center Tray Offset, select **On**.

    Note: The offset feature provides a physical offset of hard-copy output in the following situations:
    - Between sets of copies within a copy job
    - Between separate print jobs
14. To offset output between separate print jobs, for Offsetting Between Print Jobs, select **On**.

    Note: Output from a copy job is offset automatically from the output of the previous job.

15. To increase productivity when the finisher operates at a lower speed than the device, enable conditional offset. For Conditional Finisher Offset, select an option:
    - **On**: If no other finishing settings are selected for a job, this option disables the offset function. If other finishing settings are selected, the offset function operates normally.
    - **Off**: This option enables the offset function to operate normally.

    Note: If the device and finisher operate at the same speed, the Conditional Finisher Offset setting is ignored.
16. Click **Save**.

Copying

This chapter contains:

Copy Overview 252
Specifying Default Copy Settings 253
Setting Copy Feature Defaults at the Control Panel 254
Setting Copy Presets 255
Setting ID Card Copy Feature Defaults 258
Specifying Output Settings 259

Copy Overview

The administrator password is required to access copy settings in the Embedded Web Server or at the control panel.

In the Embedded Web Server, use the Copy setup page to configure default settings. For details, refer to Specifying Default Copy Settings.

At the control panel, modify feature settings and presets.

- To configure default copy settings for non-logged-in users, customize the Copy App. For details, refer to Setting Copy Feature Defaults at the Control Panel.
- To view or modify copy feature presets, use the Tools menu. For details, refer to Setting Copy Presets.

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.

Specifying Default Copy Settings

1. In the Embedded Web Server, click **Properties > Apps**.
2. Click **Copy > Setup**.
3. For color devices, do the following:
   a. To require users to select the output color at the control panel, for Color Preset Screen, select **On**. This setting allows you to conserve supplies.
   b. If Color Preset Screen is set to Off, for Output Color, select the color mode that the device uses for copies. If you select Single Color, select a color.

   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.

   c. For 2-sided copying, select options:
      - For 2-Sided Copy, select an option.
      - To rotate the second side, select the check box for **Rotate Side 2**.
4. Click the **Defaults** tab, then select options:
   - For 2-Sided Copy, select an option.
   - To rotate the second side, select the check box for **Rotate Side 2**.
5. Click **Apply**.

Setting Copy Feature Defaults at the Control Panel

To specify the default copy feature settings:

1. At the control panel, press the **Home** button.
2. Touch the **Copy** App.
3. Edit settings as needed for output, image quality, layout, output format, and job assembly.

   Note: To reset all features to the current defaults for the device, touch **Reset**.

4. Scroll to the bottom of the feature list, then touch **Customize**.
5. Touch **Save Settings as Default**.
6. To apply the settings to non-logged-in users, at the prompt, touch **Guest**.

To customize the feature list or to remove the app customizations, refer to Customizing App Features or Removing App Customization Settings.

Setting Copy Presets

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 PRESET SCREEN

When the Color Preset Screen feature is enabled, a color preset screen appears each time a user accesses the Copy App. At the Make All My Copies screen, the user selects a color printing option for their copy jobs. The following options are available:

- Black & White
- Color
- Match My Originals

1. At the control panel, touch **Device**, then touch **Tools**.
2. Touch **App Settings > Copy App**.
3. Touch **Color Preset Screen**.
4. Touch **Off** or **On**, then touch **OK**.

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**.

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**.

Setting ID Card Copy Feature Defaults

To set feature defaults for ID card copy:

1. At the control panel, press the **Home** button.
2. Touch the **ID Card Copy** App.
3. Edit settings as needed:
   - 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, move the slider for Lighten / Darken.
   - To edit the default setting for Automatic Background Suppression, touch the toggle button.

   Note: To reset all features to the current defaults for the device, touch **Reset**.
4. Scroll to the bottom of the feature list, then touch **Customize**.
5. Touch **Save Settings as Default**.
6. To apply the settings to non-logged-in users, at the prompt, touch **Guest**.

To customize the feature list or to remove the app customizations, refer to Customizing App Features or Removing App Customization Settings.

Specifying Output Settings

You can specify output settings for copy jobs at the control panel. Some settings affect print and fax jobs.

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.

1. At the control panel, touch **Device > Tools**.
2. Touch **Device Settings > Output**.
3. 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.
4. To specify the output location for unfinished jobs, select **Output Location**, then select an output tray for copy, print, and fax jobs.

   Note:

   - The device determines the output location for finished jobs.
   - System-generated reports are sent automatically to the specified print tray.
5. To separate print sets within a copy or print job, select **Offset**, then select the needed options:
   - For Center Tray Offset, click the toggle button.
   - For Offsetting of Sets Within Copy Jobs, click the toggle button. If you disable this feature, the device stacks all printed sets together.
6. 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:
   - **Complete Job Without Stapling**: This option completes the print job and no stapling occurs.
   - **Fault / Hold Job**: This option holds staple jobs that have not started to print. For a staple job that is printing when the stapler is empty, the device returns a fault.
7. To specify how the device staples landscape documents, select **Staple Productivity Mode**, then select **Enable** or **Disable**.

Scanning

This chapter contains:

Scanning to an Email Address 262
Workflow Scanning..... 269
Scanning to a Folder on the Device 282
Scan To USB 286
Scanning to a User Home Folder..... 287
Configuring Scan To 289

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. You can customize the keyboard with general email selection. For more information, refer to Configuring the Custom Keyboard Button.

For instructions on using this feature, refer to the *User Guide* for your printer model.

CONFIGURING EMAIL

Configure email settings in the Embedded Web Server, on the Email Setup page. Email settings apply to other apps that use SMTP.

1. In the Embedded Web Server, click **Properties > Apps > Email > Setup**.
2. To configure settings, on the Email Setup page, select tabs as needed:
   - To configure the required settings for email messages, click the **Required** tab. For details, refer to Configuring Required Settings.
   - To configure the information that you want to appear in email messages sent from the printer, click the **General** tab. For details, refer to Configuring General Email Settings.
   - To determine the source of user email addresses, or to enable and configure the Network Address Book, click the **Smart Card Policies** tab. This tab is available only when Smart Card Authentication is enabled. For details, refer to Configuring Smart Card Policies.
   - To select an address book, edit address book information, and set address book policies, click the **Address Books** tab. For details, refer to Configuring Address Book Settings.
   - To configure the default settings for scanning to email, click the **Defaults** tab. For details, refer to Configuring Default Email Settings.
   - To select the compression settings for sending scanned images from the printer by email, click the **Compression** tab. For details, refer to Setting File Compression Options.
   - To configure the security settings, click the **Security** tab. For details, refer to Configuring Email Security Settings.

Note: If you are unsuccessful in setting up email, try the following:

- Use the SMTP configuration test to verify if the login credentials have changed and need updating.
- If you are using a cloud-based SMTP server, for assistance, refer to the Xerox® Customer Support Forum at https://forum.support.xerox.com.

Configuring Required Settings

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

2. On the Email Setup page, click the **Required Settings** tab.
3. To configure SMTP settings, for SMTP, click **Edit**. For details, refer to SMTP.
4. To configure the From field settings, for From Field, click **Edit**.

Configuring From Field Settings

To configure From field settings:

1. For Default From Address, type the email address that 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 the email sender name with the email address, select **Add sender's name to email address**.
6. Click **Save**.

Configuring General Email Settings

Use the General settings page to specify the information that you want to appear in email messages that are sent from the device.

1. In the Embedded Web Server, click **Properties > Apps > Email > Setup**.
2. On the Email Setup page, click the **General** tab.
3. In the Message Body area, select the information that you want to appear in the body of email messages:
   - To include a user name or email address in the message body, for User, select **User Name**, **Email Address**, or both.
   - To include attachment information in the message body, select **Number of Images**, **Attachment File Type**, or both.
   - To include information about the printer in the message body, for Multifunction printer System, select the details that you want to include.
4. For Signature, type the information that you want to appear at the end of email messages.
5. To add the email address of the sender to the To field, for Auto Add Me, select **Enabled**.
6. Click **Apply**.

Configuring Smart Card Policies

Use this page to determine the source from which the printer gets user email addresses. You can enable and configure the Network Address Book for acquiring email addresses.

1. In the Embedded Web Server, click **Properties > Apps > Email > Setup**.
2. On the Email Setup page, click the **Smart Card Policies** tab.

Note: The Smart Card Policies tab is available in Email Setup when Smart Card Authentication is enabled.

3. To select the source from which the printer gets the email address for a logged-in user, in the Policies area, select an option:
   - **Auto**: This option 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 that is specified in the From field.

   Note: You can review the From field setting on the Required Settings tab.

   - **Only Smart Card**: This option instructs the printer to retrieve the email address from the smart card.
   - **Only Network Address Book (LDAP)**: This option instructs the printer to retrieve the email address of the user from the network address book. If the From field is not configured, click **From Address Not Configured**.
4. To configure LDAP server settings, in the Server Configuration area, for Network Address Book (LDAP), click **Edit**.
5. To enable or disable the Personalization feature, in the Feature Enablement area, for Acquire Email from Network Address Book, click **Enable Personalization** or **Disable Personalization**.
6. Click **Apply**.

Configuring Address Book Settings

Use the Address Books page to select an address book, edit address book information, and set address book policies.

1. In the Embedded Web Server, click **Properties > Apps > Email > Setup**.
2. On the Email Setup page, click the **Address Books** tab.
3. To configure the address book settings that are stored in the device, for Device Address Book, click **Edit**.
4. To use a network address book, configure the LDAP server settings. For Network Address Book, click **Edit**.
5. If you configured Device Address Book settings, for Use Device Address Book, select options as needed:
   - To allow users to access the address book, select **Yes**.
   - To show Favorites as the initial view when entering the address book, select **View Favorites on App Entry (Email and Scan To)**.

   Note: This option requires that the device address book contains at least one contact with a valid email address.

   - To restrict users from accessing the address book, select **No**.
6. If you configured Network Address Book settings, for Use Network Address Book, select an option.
   - To allow users to access the address book, select **Yes**.
   - To restrict users from accessing the address book, select **No (Hide)**.

   Note: When no LDAP server is configured, the Use Network Address Book option does not appear.

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. To return settings to factory-default values, click **Apply Factory Settings**.
9. To save settings, click **Apply**.

Configuring Default Email Settings

Use the Defaults page to configure default settings for scanning to email.

Note: When Automatically Set Device Defaults is enabled for entry screen defaults, the following message appears: `Adaptive Learning is Setting Defaults`.

When Automatically Set Device Defaults is enabled, settings can change from the defaults that you specify. To change the Adaptive Learning configuration, refer to Adaptive Learning.

Note: For more information about specific scanning settings, refer to Help in the Embedded Web Server.

1. In the Embedded Web Server, click **Properties > Apps > Email > Setup**.
2. On the Email Setup page, click the **Defaults** tab.
3. For Subject, type the text that you want to appear in the subject line of emails that are sent from the printer.
4. To edit default scan settings, for Scan to Email, click **Edit**.

Note:

- If the printer supports Preview option, enable **Preview** to instruct the printer to create a multiple-step process for scanning a job. This process allows you to review the scanned images before you send the job.
- If Output Color is set to Black & White, the JPEG option is not available as a file format.

5. To edit default Image Options, Image Enhancement, Resolution, and Quality / File Size settings, for Advanced Settings, click **Edit**.
6. To edit default Original Orientation, Original Size, Edge Erase, and Blank Page Management settings, for Layout Adjustment, click **Edit**.
7. To edit default File Format and Filename Extension settings, for Email Options, click **Edit**.

Note: To make the PDF or PDF/A documents searchable, for File Options, select **Searchable**. By default, the **Image Only** option is enabled for PDF and PDF/A file format. The user can change the File Options from **Searchable** to **Image Only** at the local user interface (LUI).

Note: For PDF, PDF/A, and TIFF file formats, the scanned documents can also be split in to multiple files with fixed number of pages using the Choose Pages Per File option. For example, 10 original single-sided documents scanned with 2 Pages Per File will result in 5 files with each containing 2 Pages Per File.

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**.

Setting File Compression Options

1. On the Email Setup page, click the **Compression** tab.
2. Select **.tiff** and **.pdf** compression settings as needed. For details, refer to the Help in the Embedded Web Server.
3. Click **Apply**.

Configuring Email Security Settings

Use the Security page to configure email encryption settings and security policies.

1. In the Embedded Web Server, click **Properties > Apps > Email > Setup**.
2. On the Email Setup page, click the **Security** tab.
3. To edit email encryption and signing settings, in the Encryption / Signing area, click **Edit**. For details, refer to Configuring Email Encryption Settings and Configuring Email Signing Settings.
4. To configure domain and email filter settings, in the Network Policies area, click **Edit**. For details, refer to Editing Network Policy Settings.
5. To set user permission roles for access to the email service, in the User Policies area, for Manage user permissions, click **Edit**. For details, refer to User Roles.
6. To change user policies for email address fields, in the User Policies area, for Only Send to Self, click **Edit** For details, refer to Editing User Policy Settings.

Configuring Email Signing Settings

Before you begin:

- Configure the Smart Card Authentication settings. For details, refer to Configuring Smart Card Authentication Settings.
- Ensure that signing certificates are installed on all smart cards.

To configure email signing settings:

1. In the Embedded Web Server, click **Properties > Apps > Email > Setup**.
2. On the Email Setup page, click the **Security** tab.
3. For Encryption / Signing, click **Edit**.
4. On the Email Encryption / Signing page, click the **Signing** tab.

5. In the Enablement area, configure the settings:
   a. For Email Signing Enablement, select an option:
      - **Off**: Disables the Email Signing feature.
      - **Always On; Not editable by user**: Restricts users from disabling the Email Signing feature at the control panel.
      - **Editable by user**: Allows users to enable or disable the Email Signing feature at the control panel.
   b. If you selected Editable by user, select the default encryption settings for users at the control panel:
      - For Email App Signing Default, select **On** or **Off**.
      - For Scan To App Signing Default, select **On** or **Off**.
6. In the Policies area, for Signing Hash, select a method.
7. Click **Apply**.

Configuring Email Encryption Settings

Before you begin:

- If you want to use the public keys that are stored on smart cards to encrypt email messages, configure the Smart Card Authentication settings. For details, refer to Configuring Smart Card Authentication Settings.
- If you want to use the public keys that are stored in an address book, configure a Network Address Book or the Device Address Book.

Note:

- If you configure Smart Card Authentication only, users can send encrypted emails to themselves only.
- To store public keys in the Device Address Book, configure the Import Using Email feature with the Import encryption certificate from signed emails option.

To configure email encryption settings:

1. In the Embedded Web Server, click **Properties > Apps > Email > Setup**.
2. On the Email Setup page, click the **Security** tab.
3. For Encryption / Signing, click **Edit**.
4. On the Email Encryption / Signing page, click the **Encryption** tab.
5. In the Enablement area, configure the settings:
   a. For Email Encryption Enablement, select an option:
      - **Off**: Disables the Email Encryption feature.
      - **Always On; Not editable by user**: Restricts users from disabling the Email Encryption feature at the control panel.
      - **Editable by user**: Allows users to enable or disable the Email Encryption feature at the control panel.

b. If you selected Editable by user, select the default encryption settings for users at the control panel:
   - For Email App Encryption Default, select **On** or **Off**.
   - For Scan To App Encryption Default, select **On** or **Off**.

6. In the Policies area, for Encryption Algorithm, select an encryption method.
7. Click **Apply**.

Editing Network Policy Settings

Use the Security: Network Policies page to edit domain and email filter settings.

1. In the Embedded Web Server, click **Properties > Apps > Email > Setup**.
2. On the Email Setup page, click the **Security** tab.
3. For Network Policies, click **Edit**.
4. On the Security: Network Policies page, for Domain Filter Settings, select an option:
   - To have the printer ignore domains, click **Off**.
   - To allow access to addresses in selected domains or to restrict usage to approved domains only, click **Allow Domains**.
   - To block addresses in selected domains, click **Block Domains**.
5. For New Domain, type the domain that you want to add to the list, then click **Add**.
6. To remove a domain from the list, select a domain, then click **Remove**.
7. To allow LDAP email address searches without the @ symbol, for Allow LDAP Email Address without the @ Requirement, select **On**.

Note:

- Ensure that your mail server supports this requirement.
- If you select On for Allow LDAP Email Address without the @ Requirement, the number of items returned by an LDAP search can increase.

Editing User Policy Settings

Use the Security:User Policies page to configure user security policies.

1. In the Embedded Web Server, click **Properties > Apps > Email > Setup**.
2. On the Email Setup page, click the **Security** tab.
3. In the Security area, configure email recipient settings as needed:
   a. To restrict authenticated users from sending emails to others, for Only Send to Self, select **On**. This setting ensures that the email address of the logged-in users can be added as an email recipient only.
   b. To remove the ability for users to add an email address to the recipient list manually, for Restrict manual entry of recipients, select **On**.
   c. To clear the recipient fields after a user touches Send on the control panel, for Clear “To:”, “Cc:”, and “Bcc:” fields after selecting “Send”, select **On (clear recipient list)**.
4. Click **Save**.

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 directory for each job for 1 File Per Page or Choose Pages Per File jobs, enable **Create sub-folder (.XSM) for 1 File Per Page or Choose Pages Per File 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 directory for each job for 1 File Per Page or Choose Pages Per File jobs, enable **Create sub-folder (.XSM) for 1 File Per Page or Choose Pages Per File 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 printer to create .XSM directory for each job for 1 File Per Page or Choose Pages Per File jobs, enable **Create sub-folder (.XSM) for 1 File Per Page or Choose Pages Per File 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**.

     If you want the printer to create .XSM directory for each job for 1 File Per Page or Choose Pages Per File jobs, enable **Create sub-folder (.XSM) for 1 File Per Page or Choose Pages Per File jobs**.

   Note: To make the PDF or PDF/A documents searchable, for File Options, select **Searchable**. By default, the **Image Only** option is enabled for PDF and PDF/A file format. The user can change the File Options from **Searchable** to **Image Only** at the local user interface (LUI).

   - 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, 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 REMOTE SCAN START

Remote Scan Start allows users to manage scanning images into a TWAIN-compliant application using the TWAIN driver. This is EIP Scanning setting.

Remote Scan Start also allows users to manage scanning images to an eSCL compliant client. This is the eSCL Scanning setting.

1. In the Embedded Web Server, click **Properties > Apps**.
2. Click **Workflow Scanning > Remote Scan Start**.
   - Enabling Remote Scan Start allows you 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. To enable Remote Scan Start, click the toggle button for **EIP Scanning** and **eSCL Scanning (compatible with AirPrint/Mopria)**.

Note: Disabling Remote Scan Start can disrupt scanning functions in remote apps that rely on the TWAIN protocol.

   - To disable initiation of scan jobs from a client device, turn off **EIP Scanning** and **eSCL Scanning (compatible with AirPrint/Mopria)**.
   - To disable scanning from a TWAIN compliant client device, turn off **EIP Scanning**.
   - To disable eSCL Scanning (driverless scanning), turn off **eSCL Scanning (compatible with AirPrint/Mopria)**.

Note: Disabling EIP Scanning or eSCL Scanning (compatible with AirPrint/Mopria) does not guarantee that the scan jobs cannot be initiated from the client device. The client device may automatically revert to the scanning method that remains enabled. To ensure that remote scanning is disabled, both EIP Scanning and eSCL Scanning must be disabled.

3. For Start Job via Remote Program, click **On**.
4. Click **Apply**.

To configure the other scan-related settings, do the following:

1. For (Scan Related) Web Services, click **Configure** to 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.
2. For EIP Scan Settings, click **Configure** to modify the EIP settings that are specific to scan applications.
3. For AirPrint, click **Configure** to modify the AirPrint-related settings.
4. For Mopria, click **Configure** to modify the Mopria-related settings.
5. 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 > Setup**.
3. In the Scan To Mailbox Setup area, configure settings as needed:
   - To enable Scan To Mailbox, select the check box for **Enable Scan To Mailbox**.
   - To disable Scan To Mailbox, clear the check box for **Enable Scan To Mailbox**.
   - To set the default view to show mailbox folders in the Embedded Web Server Scan tab, select **View Mailbox By Default on Device Website Scan Tab**.

   Note: When you enable the Scan To Mailbox feature, mailbox folders appear as workflows in the Workflow Scanning App on the device control panel.
4. To save the new settings, click **Apply**. 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

The Scan To USB feature allows you to scan a document, and store the scanned file on a USB flash drive that is connected to the USB port on the device control panel.

Note: Only USB Flash drives formatted to FAT16, FAT32, and exFAT file systems are supported. exFAT support is a licensed feature that requires a purchased FIK.

Note: To use the Scan To USB or Print From USB app, ensure that at least one USB Type A Port is enabled.

Before you begin:

- Ensure that the USB port is enabled. For details, refer to USB Port Management.
- Ensure that Scan To USB is enabled.

ENABLING SCAN TO USB

To enable the Scan To USB feature:

1. In the Embedded Web Server, click **Properties > Apps**.
2. Click **Scan To USB > General**.
3. In the Enablement area, select **Enabled**.
4. To view or modify scan settings:
   a. Click **Modify Settings**.
   b. At the Scan To USB settings page, for the settings that you need to modify, click **Edit**.
   c. Verify the settings and make adjustments if necessary, then click **Save**.
   d. To return to the Enablement page, in the navigation pane to the left, click **Scan To USB > General**.

Note: If you proceed to the scan settings page, any unsaved change to the enablement setting is not preserved.

5. To save the enablement setting, click **Apply**. To retain the previous setting, 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.

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**.
      - If you want the printer to create .XSM directory for each job for 1 File Per Page or Choose Pages Per File jobs, enable **Create sub-folder (.XSM) for 1 File Per Page or Choose Pages Per File jobs**.
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 associates with different scanning options. When scanning using the Scan To feature, users can select the contacts, update the address book, configure the remote cloud destinations, manage shared email settings and security policies.

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 (LDAP).
- An FTP, SFTP, or SMB folder location associated with a contact in the Device Address Book.
- A USB Flash drive.

  Note: Only USB Flash drives formatted to FAT16, FAT32, and exFAT file systems are supported. exFAT support is a licensed feature that requires a purchased FIK.
- An SMB shared folder. Users can specify a network folder path or browse to a shared folder.
- Cloud shared folders, such as Dropbox, Google Drive, and Microsoft OneDrive.

Note: For instructions on using this feature, refer to the *User Guide* for your device.

APP DEFAULTS

Use the App Defaults feature to select the default output settings, file formats, file extensions, scan to image settings, and scan compression settings for Scan To functions.

Note: When Automatically Set Device Defaults is enabled for entry screen defaults, the following message appears: `Adaptive Learning is Setting Defaults`.

When Automatically Set Device Defaults is enabled, settings can change from the defaults that you specify. To change the Adaptive Learning configuration, refer to Adaptive Learning.

1. In the Embedded Web Server, click **Properties > Apps > Scan To > Setup**.
2. On the Scan To Setup page, click the **App Defaults** tab.
3. To configure default settings for Scan To functions, make changes as needed:
   - To edit the subject text of the email that is sent for the job, for **Subject**, type the message text.
   - To change the default output settings for scanned documents, for Scan To, click **Edit**.
   - To configure the default image-quality settings, for Advanced Settings, click **Edit**.
   - To specify the size and orientation of the original document, for Layout Adjustment, click **Edit**.
   - To configure File Format and Filing Policy, for Filing Options, click **Edit**.

   Note: To make the PDF or PDF/A documents searchable, for File Options, select **Searchable**. By default, the **Image Only** option is enabled for PDF and PDF/A file format. The user can change the File Options from **Searchable** to **Image Only** at the local user interface (LUI).
   - To combine an assorted group of original documents for assembly into a single scan job, for Job Assembly, click **Edit**.

- Some operating systems are case-sensitive. To select the case of the default file name extensions settings, for Filename Extension, click **Edit**.
- To configure reports, for Report Options, click **Edit**.
- To configure the compression settings for sending scanned images from the printer by email, for Compression Capability, click **Edit**.

4. Click **Apply**.

For more information, refer to the Help in the Embedded Web Server.

To configure other settings for Scan To functions, select the appropriate tab:

- Remote Destinations: This tab provides access to enablement settings for cloud, FTP, SFTP, and SMB destinations. For details, refer to Remote Destinations.
- Print Scanned Document: This tab provides access to printing properties of the scanned document. For details, refer to Print Scanned Document Settings.
- Email Required: This tab provides access to configuration settings that are required for Scan To and Email functions. For details, refer to Email Required.
- Metadata: This tab provides an option to apply metadata to Scan To jobs. For details, refer to Metadata.
- Shared Email Settings: This tab provides configuration settings for Scan To and Email functions, including message text, email signatures, and file attachment types. For details, refer to Shared Email Settings.
- Address Books: This tab provides access to address book settings and address book policies for Scan To and Email functions. For details, refer to Address Books.
- Security: This tab provides access to configuration settings for Scan To functions, including encryption and signing settings, network policies, and user policies. For details, refer to Security.

REMOTE DESTINATIONS

Use this page to enable browsing and scanning to remote folder destinations:

- Cloud Services: Dropbox, Google Drive, and Microsoft OneDrive
- FTP and SFTP
- SMB

The Scan To Cloud service is a licensed feature. Access to the service requires a feature installation key. To enable this option, provide a Scan to Cloud Licensing feature installation key on the Feature Installation page. For details, refer to Installing a Software Feature in the Embedded Web Server. To purchase a Scan to Cloud Licensing feature installation key for your device, contact your Xerox representative.

Note:

- Enabled cloud services appear as cloud destinations in the Scan To App on the device control panel.
- Cloud destinations that are not enabled are hidden from view in the Scan To App.

1. In the Embedded Web Server, click **Properties > Apps**.
2. Click **Scan To > Setup**.
3. On the Scan To Setup page, click the **Remote Destinations** tab.

4. The Scan To Cloud service is a licensed feature that requires a valid feature installation key. If you have not installed the Scan to Cloud Licensing feature installation key, the Scan to Cloud options are not available. A message alerts you to install the feature installation key. When a message appears that requests the feature installation key, do the following:
   a. In your Scan To Cloud documentation, locate the Feature Installation Key.
   b. In the Cloud Services area, click **Feature Installation Key**.
   c. In the Enter Installation Key field, type the feature installation key, then click **Apply**.

      When a valid feature installation key is entered, the Scan To Cloud service is available for configuration.
5. To allow a walk-up user to scan to cloud folder destinations, in the Cloud Services area, configure the settings:
   a. For Allow Scanning To Cloud Destinations, select the check box.

Note:

- Both logged-in and non-logged-in users can use Scan To Cloud. Logged-in users are users who have done initial authentication at the device control panel touch screen. Non-logged-in users are guest users who access the device without any authentication.
- Authentication for cloud services is independent of authentication for login to the device or access to network services.

   b. To set the Cloud Services login session retention policy, for Allow User to Save Login Token, select an option:
      - **Always**: This option instructs the printer to retain the cloud login session for a non-guest user across device logins.
      - **Never**: This option instructs the printer to delete the cloud login session for a non-guest user at the end of a session.
      - **Let Each User Choose**: This option instructs the printer to prompt a non-guest user for consent to retain the cloud login session.

Note:

- The default setting for the cloud login session retention policy is **Always**.
- The login session retention policy does not apply to non-logged-in guest users. After the session ends, the device does not retain the cloud login session of a guest user.
- The login session retention policy applies to both Print From and Scan To functions.
- If the device authentication method is changed, any retained cloud login sessions are deleted automatically.
- If cloud sessions are not used for 366 days, the sessions expire. Expired sessions are deleted from the device automatically. Users with expired sessions are required to reenter credentials to access the cloud service.

   c. To enable Scan to Cloud destinations, select options as needed:
      - To enable printing from a Dropbox folder, select the check box for **Dropbox**.
      - To enable printing from a Google Drive folder, select the check box for **Google Drive**.

- To enable printing from a Microsoft OneDrive folder, select the check box for **Microsoft OneDrive**.

Note:

- When cloud browsing is enabled or disabled in the Scan To App, cloud browsing is not enabled or disabled in the Print From App automatically.
- When a cloud service is enabled and selected in the Scan To App, users are prompted for credentials to access the cloud service. On successful authentication, users can access the cloud service and see authorized documents.
- To select a destination in the Scan To App, users can browse folders in the cloud repository only. Users cannot create or delete folders in the cloud repository.

6. To allow a walk-up user to browse FTP or SFTP scan folder destinations, in the FTP/SFTP area, configure the settings:
   a. For Allow Users to Save Credentials, select an option:
      - **Always Save Credentials**: This option instructs the printer to retain the FTP or SFTP user credentials. When the user next scans to the named server, the user is not required to reenter credentials.
      - **Never Save Credentials**: This option is for customer environments where you do not want the printer to retain the FTP or SFTP user credentials for future use.
      - **Prompt to Save Credentials**: This option instructs the printer to prompt users for consent to retain their FTP or SFTP credentials.
   b. To enable scanning to an FTP or SFTP folder destination, select options as needed:
      - To scan to an FTP folder destination, select the check box for **FTP**.
      - To scan to an SFTP folder destination, select the check box for **SFTP**.
7. To allow walk-up users to browse all available SMB share locations, in the SMB area, select the check box for **SMB**.
8. Click **Apply**.

PRINT SCANNED DOCUMENT SETTINGS

Use this page to set the default print scanned document settings:

- Add Print as Destination: Enable or Disable.
- 2-Sided Printing, Finishing, Quantity, Paper Supply, Output Color, and Image Scale and Placement.

Note: The Finishing feature appears as Collation if there is no finisher present.

Note: If the Accounting Method is Auxiliary Access Device, the Print Scanned Document feature will not be available.

Note: Output Color is not displayed on mono machines.

EMAIL REQUIRED

Use this page to access configuration settings for email or for the Scan To feature.

To send emails, for your device, configure the SMTP server, the default From Address, and the Domain Name.

1. In the Embedded Web Server, click **Properties > Apps > Scan To > Setup**.
2. On the Scan To Setup page, click the **Email Required** tab.
3. To configure required settings, in the Required Configuration Settings area, for an option, click **Edit**.

Note: To send email, ensure that you provided information about your SMTP server and configured the settings that are related to the From Field of email messages.

For more information, refer to Configuring Required Settings and Configuring General Email Settings.

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

METADATA

Metadata is any data associated with a scan file that can provide more information about the scan file. Using customizable metadata, workflows can be streamlined, and downstream processes can be automated for efficient document management.

Use this page to create and manage customizable metadata collections. These metadata collections can then be accessed from the control panel in the Scan To app, to selectively apply information from the collections to a scan job. The information will be applied as metadata to the scan files by the multifunction printer.

Subsequently, the metadata in the scan files can be inspected for streamlining document management by downstream processes. For instance, when a scan file with a very specific set of metadata reaches a remote destination, an automatic email can be sent to an authority to take some action. The following describes creation and management of metadata collections.

Note: If no metadata collection is created, then the empty variant of the page appears to **Get Started** to configure Metadata for the first time. If at least one metadata collection is configured, then the configured variant of the page appears.

If you are creating a metadata collection for the first time, perform the following:

1. Click **Get Started** in the empty variant of Metadata page.

   A prompt appears to create a **New Metadata Collection**. Enter a **Name** for the collection and select and **Icon**. This pair of collection name and icon will allow identification and selection of this metadata collection in the Scan To app at the control panel.

2. Click **Create**.

   A screen appears for the created metadata collection to add **Job-Specific** and **Predefined** metadata.

Note: Job-Specific metadata is a list from which items can be selected at the control panel to apply the selected information to the scan job. For example, the job-specific metadata is a list of students. At the control panel, a specific student name can be selected from the list and that becomes the job-specific metadata for the scan job.

Note: Predefined metadata is a set of information that is mandatorily applied to the scan job without any input at the control panel. For example, the name and location of a school where a student is enrolled.

Job-Specific Metadata

To add job-specific metadata for the first time to a collection, perform the following:

1. Click **Add Job-Specific Metadata**.
   A screen appears, which explains on how to create job-specific metadata for the collection by following three steps:

   a. **Step 1 Download**: Download a sample Comma Separated Values (.csv) file that provides a template for how job-specific metadata should be created to ensure the correct structure and formatting of job-specific metadata.

      To proceed, click **Download Template**. Select the **Language** and **Delimiter** and click **Next** to download the sample template.

      A prompt appears to **save the template file**. You can open and edit the saved template in software like Microsoft Excel.

   b. **Step 2 Customize**: To customize and understand how to modify the template file to suit your specific need. To proceed, click **Sample File Guidelines**.

      A **Sample File Guidelines** screen appears. Follow the steps mentioned on the screen and customize the template in software, such as Microsoft Excel. The instructions are also present in the saved template file. After customization, the file must be saved in .csv UTF-8 format.

Note: Only .csv UTF-8 format is supported by the multifunction printer. Other. csv encodings results in import errors.

   c. **Step 3 Import**: Import your customized file to create your job-specific metadata. To proceed, click **Import Custom File**.

      An **Import Metadata File** screen appears. Follow the instructions on the screen to browse to your custom . csv UTF-8 file and import your job-specific metadata.

Note: If import is unsuccessful, an alert message appears. Identify and correct any errors in your file and try again. For details, refer to Metadata Import Errors.

   d. If import is successful, you can use remote control panel to check your metadata. To proceed click on **Remote Control Panel** and follow the instructions to start the remote session. Once the remote session is active, click **Reset** and **Reset All Apps**. Then access the Scan To app and add a destination.

2. After a destination is added, a prompt will be shown to select items from your customized job-specific data.

Note: If a prompt is not shown to select your customized job-specific data, scroll down the feature rows in the Scan To app and locate the Metadata row and touch the row to make your job-specific metadata selection.

Predefined Metadata

To add predefined metadata for the first time to a collection, perform the following:

1. Click **Add Predefined Metadata**.
2. Enter the required **Name** and **Value** pairs and click **Add**.
3. Repeat the step to add more.

You can also edit or delete predefined metadata.

Collection Preferences

Collection preferences allow management of the collection.

Collection Status

1. A collection is **Active** when it is available for selection in the Scan To app at the control panel.
2. A collection is **Off** when it is not available for selection in the Scan To app at the control panel.
3. A collection can have errors if a collection is available at the control panel but contains no job-specific or predefined metadata.

To access preferences of a collection, select a collection and in the Preferences area, click **Collection Preferences**.

Collection Availability

Collections can be made available for selection or hidden at the control panel.

For a collection to be available for selection in the Scan To app,

1. Ensure that **Make available in the Scan To app** is enabled.
2. By default, a newly created collection is available for selection at the control panel if the collection has no errors.

Collection Name and Icon

Collection name and icon will be available at the control panel, which allows identification and selection of the collection in the Scan To app.

In the **Preferences** area of a collection, **Icon** and **Name** can be modified and edited, if required.

Filename

For a collection, a policy can be set to include the job-specific metadata in the scanned file name.

Note: If enabled, this policy works in conjunction with other file naming policies of the Scan To app.

1. To enable the scan file to contain its filename selections from the Job-Specific metadata, ensure that **Auto Populate File Name based on selected Job-Specific metadata** is enabled.
2. By default, this policy is disabled.

Predefined Metadata Visibility

Predefined metadata of a collection can be visible or hidden to the walk-up user at the control panel.

1. To hide the predefined metadata from the walkup user, ensure that **Hide Predefined Metadata from walk-up-user** is enabled.
2. By default, the predefined metadata is hidden at the control panel.

Metadata Formats

Metadata format for scanned documents determines how the metadata is applied to the scan files. The options are:

1. XMP-Adobe's Extensible Metadata Platform

   XMP is an ISO 16684-1:2019 standard. In this format, the metadata is embedded within the pdf, pdf/a, jpg, and tiff scan files.

2. XST-Xerox Standard Template

   A Xerox format where the metadata is in a .xst file separate from the scan files.

   Note: XST format is not applicable to email jobs. A .xst file will not be sent as an attachment to an email. Only repository destinations will contain .xst file along with the scan files.

3. XMP and XST

   Metadata for the scanned documents will be both in XMP and XST formats.

   Note: For a detailed example on how the metadata will be formatted and structured in the XMP format and in the XST files, refer to Metadata Structure.

After making the required changes, click **Save**.

To delete the collection, click **Delete This Collection**.

Metadata Import Errors

ERROR TYPE	ERROR RESOLUTION
Invalid file type. Please use a file in CSV format (. csv) for successful import.	The CSV file being imported can only be in CSV UTF-8 format. Save the file on the PC in CSV UTF-8 format.
Your file could not be uploaded successfully. Import validation failed. Please try again.	Generic error or session timeout. Try logging in to the EWS as an admin.
The CSV file contains metadata levels exceeding the allowed limit (3).	Reduce the number or levels in the CSV file. Or check that the CSV file is structured similar to the template.
The CSV file is missing required line ending characters (CR/LF or LF), or a line exceeds the maximum size of 1500 bytes.	A single line contains too many characters. Reduce the number of characters on a single line.
The CSV file contains characters that do not comply with the UTF-8 encoding standard.	Unrecognized UTF-8 characters. Verify which line in the CSV file is causing this error and remove the characters that are not allowed.
The CSV file contains invalid characters.	Verify that invalid characters are not present in the CSV file. The list of invalid characters is documented in the template file.
The CSV file column (level) headings exceed maximum length (31).	Reduce the length of column heading in the CSV file.
The CSV file contains a column heading with zero-length string (after leading and trailing spaces removed).	Malformed CSV file. Empty column heading. CSV file cannot contain empty headings.
The CSV file contains more data lines (excluding	Reduce the number of lines in the CSV file.

ERROR TYPE	ERROR RESOLUTION
comment, empty or heading lines) than the maximum allowed limit (2048).	
The CSV file contains an inconsistent number of columns and data. For example, the file may have 3 column headings, but the data line contained 2 or 4 columns.	Malformed CSV file. Re-check the CSV file structure and follow the template for the proper structure.
The CSV file contains one or more columns (levels) that exceed the maximum length (63).	Reduce the number of characters in an entry.
The CSV file contains non-empty data on multiple columns. Data is allowed only on one column (except for the column headings row).	Verify that each line has only one entry.
The CSV file structure has an invalid parent-child hierarchy. Check the file for columns without parent references.	Malformed CSV file. Re-check the CSV file structure and follow the downloadable template to structure the CSV file properly.
The CSV file is missing Job-Specific selections. For example, the file contains only comments, empty lines or column headers.	Malformed CSV file. Re-check the CSV file structure and follow the downloadable template to structure the CSV file properly.
The CSV file contains duplicate values for the same parent column. Metadata values must be unique under each heading.	Malformed CSV file. Remove duplicate entries or structure your CSV file in a different way.

Metadata Structure

XMP Structure

Adobe's extensible metadata platform toolkit (XMP Toolkit SDK) can be used by downstream processes to inspect scan files generated by the Scan To app and extract the metadata from the scan files.

Internet resources can be used to search and identify where to obtain the toolkit and how to use it.

For scan files generated by multifunction printers,

- The XML name space shall be `http://ns.xerox.com/xrxmd/1.0/`
- The value of the XML element name `MetadataCollectionName` will indicate the collection name.
- The XML element name for names of the job-specific headings will be of the form `JobSpecificDataFieldX`.
- The XML element name for names of the job-specific selections will be of the form `JobSpecificDataValueX`.
- The XML element name for names of the predefined names will be of the form `PredefinedDataFieldX`.
- The XML element name for names of the predefined values will be of the form `PredefinedDataValueX`.

Example

The following section shows an example of the metadata embedded in the scan files by the multifunction printer in a pdf, pdf/a, jpg, and tiff files. The MetadataCollectionName is **School**.

The three headings for making selections at the control panel are **Teachers, Grades and Subject, and Students**.

The selections chosen at the control panel for each of the headings are **Sherlock Holmes, 9th-Math**, and **Ronald Adair**.

The predefined metadata for this collection are the **Principal**, **Conan Doyle**, and the **Address**, **221 Bleeker Street**.

```
<?xpacket begin="ï»¿" id="W5M0MpCehiHzreSzNTczkc9d"?>
<x:xmpmeta xmlns:x="adobe:ns:meta/">
<rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#">
<rdf:Description rdf:about="" xmlns:xrxmd="http://ns.xerox.com/xrxmd/1.0/">
<xrxmd:MetadataCollectionName>School</xrxmd:MetadataCollectionName>
<xrxmd:JobSpecificDataField1>Teachers</xrxmd:JobSpecificDataField1>
<xrxmd:JobSpecificDataValue1>Sherlock Holmes</xrxmd:JobSpecificDataValue1>
<xrxmd:JobSpecificDataField2>Grades and Subject</xrxmd:JobSpecificDataField2>
<xrxmd:JobSpecificDataValue2>9th-Math</xrxmd:JobSpecificDataValue2>
<xrxmd:JobSpecificDataField3>Students</xrxmd:JobSpecificDataField3>
<xrxmd:JobSpecificDataValue3>Ronald Adair</xrxmd:JobSpecificDataValue3>
<xrxmd:PredefinedDataField1>Principal</xrxmd:PredefinedDataField1>
<xrxmd:PredefinedDataValue1>Conan Doyle</xrxmd:PredefinedDataValue1>
<xrxmd:PredefinedDataField2>Address</xrxmd:PredefinedDataField2>
<xrxmd:PredefinedDataValue2>221 Bleeker Street</xrxmd:PredefinedDataValue2>
</rdf:Description>
</rdf:RDF>
</x:xmpmeta>
```

XST Structure

Xerox Standard Template (XST) is a human readable file that contains information about the scan job. This file also contains metadata.

The following shows an example of the metadata embedded in the `.xst file`.

`xrx_dscrpt_metadata` section of the `.xst file` contains the metadata for the scan job.

Metadata Collection Name

For identifying the collection name, `MetaDataFieldName` and `MetaDataType` will always be `MetadataCollectionName`. The `MetaDataValue` of this triplet indicates the metadata collection name.

Job-Specific Metadata

For identifying the job-specific metadata, the value of the MetaDataType triplet will always be JobSpecificData. The values for `MetaDataFieldName` and `MetaDataValue` in this triplet indicates the job-specific heading and the selections at the control panel for the scan job.

Predefined Metadata

For identifying the predefined metadata, the value of the MetaDataType triplet will always be PredefinedData. The values for `MetaDataFieldName` and `MetaDataValue` in this triplet shall indicate the predefined name-value

pairs for the collection.

The following section shows an example `xrx_dscrpt_metadata` section from an `xst` file. The information in this example is same as the **XMP Structure Example** above.

```
[description xrx_dscrpt_metadata]
 1{
      string MetaDataFieldName = "MetaDataCollectionName";
      string MetaDataType = "MetaDataCollectionName";
      string MetaDataValue = "School";
 }
 2{
      string MetaDataFieldName = "Teachers";
      string MetaDataType = "JobSpecificData";
      string MetaDataValue = "Sherlock Holmes";
 }
 3{
      string MetaDataFieldName = "Grades and Subject";
      string MetaDataType = "JobSpecificData";
      string MetaDataValue = "9th-Math";
 }
 4{
      string MetaDataFieldName = "Students";
      string MetaDataType = "JobSpecificData";
      string MetaDataValue = "Ronald Adair";
 }
 5{
      string MetaDataFieldName = "Principal";
      string MetaDataType = "PredefinedData";
      string MetaDataValue = "Conan Doyle";
 }
 6{
      string MetaDataFieldName = "Address";
      string MetaDataType = "PredefinedData";
      string MetaDataValue = "221 Bleeker Street";
 }
end
```

Metadata Feature Preferences

1. On a configured variant of the Metadata page, in the Metadata area, click **Preferences**.
   A Global Preferences screen appears.
2. To enable the feature, ensure that **Apply Metadata to Scan To Jobs** is enabled.
3. To force walk-up users at the control panel to always apply metadata to Scan To jobs, ensure that **Require walk-up-users to choose Job-Specific metadata** is enabled to send their jobs.

Note: When this option is enabled, ensure that the Scan To app has valid metadata collections with job-specific metadata defined. Otherwise, the Scan To app will not allow scanning to occur.

SHARED EMAIL SETTINGS

Use this page to configure confirmation sheets and the information that you want to appear in email messages that are sent from the device.

1. In the Embedded Web Server, click **Properties > Apps > Scan To > Setup**.
2. On the Scan To Setup page, click the **Shared Email Settings** tab.
3. For Subject, type the text that you want to appear in the subject line of emails that are sent from the device.
4. For Message body, type the text that you want to appear in the body of emails.
5. To include the user name or email address in the body of emails, for User, select **User Name** or **Email Address**.
6. To include attachment information in the email message body, select **Number of Images**, or **Attachment File Type**.
7. To include information about the device in the email message body, for Multifunction Printer System, select the information that you want to include.
8. For Signature, type the information that you want to appear at the end of the email message.
9. To add the email address of the sender to the To field in email messages, for Auto Add Me, select **Enabled**.
10. Click **Apply**.

ADDRESS BOOKS

Use this page to select which address book to use, edit address book information, and set policies for using and editing the address book.

For address book settings and policies, the Scan To feature shares configuration settings with the Email App. To configure default scan settings for address book:

1. In the Embedded Web Server, click **Properties > Apps**.
2. Click **Scan To > Setup**.
3. On the Scan To Setup page, click the **Address Books** tab.
4. To configure the address book settings that are 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 (LDAP), click **Edit**.
6. If you configured Device Address Book settings, for Use Device Address Book, select options as needed.
   - To allow users to access the address book, in the Policies area, select **Yes**.
   - To show Favorites as the initial view when entering the address book, select **View Favorites on App Entry (Email and Scan To)**.

Note: This option requires that the device address book contains at least one contact with a valid email address.

   - To restrict users from accessing the address book, in the Policies area, select **No (Hide)**.

7. If you configured Network Address Book settings, for Use Network Address Book, select an option.
   - To allow users to access the address book, in the Policies area, select **Yes**.
   - To restrict users from accessing the address book, in the Policies area, select **No (Hide)**.

   Note: When no LDAP server is configured, the Use Network Address Book option does not appear.
8. To return settings to factory-default values, click **Apply Factory Settings**.
9. Click **Apply**.

SECURITY

Use this page to view and edit network and user email security policies.

For security settings and policies, the Scan To feature shares some configuration settings with the Email App. To configure default scan settings for Security:

1. In the Embedded Web Server, click **Properties > Apps**.
2. Click **Scan To > Setup**.
3. On the Scan To Setup page, click the **Security** tab.
4. To configure user permissions, in the User Permissions for Non-Logged-In User area, click **Edit**. For details, refer to User Roles.
5. To edit encryption and signing settings, in the Encryption / Signing area, click **Edit**. For details, refer to Configuring Email Encryption Settings and Configuring Email Signing Settings.
6. To edit domain filter and email filter settings, in the Network Policies area, click **Edit**. For details, refer to Editing Network Policy Settings.

   Note:
   - Settings configured on this page are applied to Email services.
   - If you select On for Allow LDAP Email Address without the @ Requirement, the number of items returned by an LDAP search can increase.
7. To edit user security policies, in the User Policies area, click **Edit**. For details, refer to Editing User Policy Settings.
   - To set user permission roles for access control of email service, in the User Policies area, for Manage user permissions, click **Edit**.
   - To change user policies for Only Send to Self, Restrict manual entry of recipients, or Clear "To:", "Cc:", and "Bcc:" fields after selecting "Send", in the User Policies area, for Only Send to Self, click **Edit**.
8. To return settings to factory-default values, click **Apply Factory Settings**.

Faxing

This chapter contains:

Fax Overview 304
Fax 305
Server Fax 315
LAN Fax 320

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.
- **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.

USB Fax Card

USB Fax Cards are only supported in ALC82XX and ALB82XX series printers. USB Fax Card is a 1-Line Fax Card. You can use maximum of two USB Fax Cards. You can connect the USB Fax Card in any of the following ways:

- If only one USB Fax Card is used, it can be plugged in any of the rear USB ports.
- If two USB Fax Card are used, Line 1 card should be in L1 USB port and Line 2 card should be in one of the L2 USB ports.

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**.

Enabling Error Correction Mode

To enable or disable the Error Correction Mode, click the toggle button. This option is enabled by default to detect and correct errors in the fax transmission process.

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 you can print or delete a fax.

1. On the Incoming Fax Defaults screen, touch **Secure Receive Settings**.
2. To enable the Secure Receive feature, touch **Passcode Protect**.

   Note: To engage or disengage the Secure Fax Receive option, use the administrator password.
3. To change the passcode, use the touch screen keypad to type the new passcode.
4. To allow guest users to enable or disable the Secure Fax feature, for 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.

To change the default fax feature settings:

1. At the control panel, press the **Home** button.
2. Touch the **Fax** App.
3. Edit settings for size, resolution, image quality, layout, fax options, and job assembly, as needed.

   Note: To reset all features to the current defaults for the device, touch **Reset**.

4. Scroll to the bottom of the feature list, then touch **Customize**.
5. Touch **Save Settings as Default**.
6. To apply the settings to non-logged-in users, at the prompt, touch **Guest**.

To customize the feature list or to remove the app customizations, refer to Customizing App Features or Removing App Customization Settings.

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.

   Note: To make the PDF document searchable, for File Format Type, select **PDF - Searchable**. By default, the **PDF - Image Only** option is enabled for PDF file format.

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

You can set up Fax Reports at the control panel touch screen. You can configure the reports that the device can generate, and configure the default report that the device produces.

Setting Up the Generated Fax Reports

To set up the fax reports that the device can generate:

1. At the control panel touch screen, log in as administrator.
2. Touch **Device**, then touch **Tools**.
3. Touch **App Settings > Fax App**.
4. Touch **Setup Fax Reports**.
5. 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**.
6. Touch **OK**.
7. Touch **Confirmation Report**. For Report Options, touch an option:
   - To allow users to print a confirmation report when a fax transmission error occurs, select **Print On Error**. If you select Print On Error, users can choose Print Confirmation Report, or Print on Error Only in the Fax App.
   - To allow users to disable printing a confirmation report, select **Off**. If you select Off, users can choose Print Confirmation Report, or Off in the Fax App.

8. 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**.
9. Touch **OK**.
10. Touch **Broadcast and 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**.
11. Touch **OK**.
12. Touch **Close**.

Setting the Default Fax Confirmation Report

To set up the default fax report that is generated when a user sends a fax:

1. At the control panel touch screen, log in as administrator.
2. Touch **Fax App**. If needed, close the Fax pop-up window.
3. Touch **Show Additional Features**.
4. Touch **Confirmation Report**.
5. Select an option:
   - Touch **Print Confirmation**, or touch **Print on Error Only**.
   - Touch **Print Confirmation**, or touch **Off**.

   The options that are available depend on the reports that you set up. For details, refer to Setting Up the Generated Fax Reports.
6. Touch **Customize**.
7. Touch **Save Setting as Default**.
8. Touch **Save**.

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**.

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.

Accounting

This chapter contains:

Xerox® Standard Accounting Tool..... 322
Network Accounting..... 330
Accounting Using an Auxiliary Access Device..... 334
Enabling Accounting in Print Drivers..... 337
Printing a Copy Activity Report..... 338

Xerox® Standard Accounting Tool

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 Backup and Restore feature to back up settings. If Xerox® Standard Accounting settings are lost or deleted, you can restore them using the 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 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, and server 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, 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 the toggle button for **Job Limits Server Proxy**.

   Note: If the **Proxy Server** is disabled, the **Job Limits Server Proxy** toggle will be off and disabled. To enable the Proxy Server, user can navigate to Proxy Server page. For more information, refer to Proxy Server.

5. To change or save the Proxy Server Address, for Proxy Server, click on the Proxy Server Address displayed.

   In the Job Limits Server window, the following message appears: `You are about to direct to the Proxy Server page. Your current settings will be saved.` To save the changes, click **Continue**.

   The Proxy Server page is displayed.

6. In the Proxy Server page, make the required changes and click **Save**.

   User will be looped back to the Job Limits Server page, and changes will be applied.

7. 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. For Prompt Options, for Presets, for ConnectKey Apps option, select **Prompt** or **No Prompt**.
   The selected Prompt options are applied to all ConnectKey Apps as a group.

   Note: ConnectKey Apps row is always visible, even if there are no ConnectKey Apps installed.

7. 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 V3 PRINT DRIVER

1. From the Start menu, select **Settings**, then select **Devices > Devices and Printers**.
2. Left-click the printer in the list, then select **Manage > Printer Properties > Configuration > Accounting**.
3. From the Accounting System menu, select **Xerox Standard Accounting or Auditron**, or **Xerox Network Accounting**.
4. For Print-Time Prompt, select an option:
   - **Always Prompt**: Select this option to prompt users for their user ID and account ID each time they print.
   - **Do Not Prompt**: Select this option if you do not want users to log in to print. Type the default user information in the Default User ID and Default Account ID fields.
5. To show characters as asterisks when the user types an ID, select **Mask User ID** and **Mask Account ID**.
6. To show the last entered code when users are prompted for their account ID, select **Remember Last Entered Codes**.
7. If you are using Xerox Standard Accounting with an external accounting device, select **Auxiliary Accounting Interface**.
8. To specify the default user ID and account ID, type the information in the Default User ID and Default Account ID fields. Select the default account type.
9. Click **OK**.
10. To exit, 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 **Accounting**.
4. For Accounting System, select **Xerox Standard Accounting**, **Auditron**, or **Xerox Network Accounting**.
5. If you want users to type their User ID and Account ID every time they print, select **Prompt for Every Job**.
6. To show characters as asterisks when the user types an ID, select **Mask User ID** and **Mask Account ID**.
7. To specify the default User ID and Account ID, type them in the Default User ID and Default Account ID fields, then select the default account type.
8. To use Xerox Standard Accounting with an external accounting device, select **Auxiliary Accounting Interface**.
9. To save your settings, click the **Presets** menu, then select **Save As**.
10. Type a name for the preset.
11. 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**.

Administrator Tools

This chapter contains:

Viewing Device Status and Configuring Apps 341
Display Device Information 343
Quick Access 344
Accessibility 345
Customizing Device Contact Information 346
Configuring Alerts 347
Energy Saving Settings 351
Remote Control Panel 357
Entry Screen Defaults 358
Remote Services 360
Remote Management Server Setup 362
Security Dashboard 363
Fleet Orchestrator 366
Cloning 386
Language and Keyboard 388
Backup and Restore Settings 390
Supplies 392
Billing Impression Mode 393
Address Books 394
Font Management Utility 400
Network Logs 401
Restarting the Device in the Embedded Web Server 402
Restarting the Device at the Control Panel 403
Taking the Device Offline 404
Erase Customer Data 405
Resetting the User Interface to Factory Default Settings 406
Reverting to Previous Settings 407
Updating the Device Software 408
Updating Card Reader Firmware 409
Adjusting Color, Image, and Text Detection Settings 411

Test Drive 412
Configuring Lockdown Security Solution 414
Configuration Watchdog 416

Viewing Device Status and Configuring Apps

The Home page in the Embedded Web Server displays device status and information. The page provides an overview of notifications, supplies usage, tray settings, app configuration, and billing information for your device. At the bottom of the page, the Quick Links section provides access to driver downloads, reports, the Remote Control Panel, and other frequently used functions.

To access the Home page, refer to Accessing the Embedded Web Server as a System Administrator.

The Home page is divided into the following sections:

- Notifications: To configure control panel alerts and email notifications, click **Settings**. For details, refer to Configuring Alerts.
- Trays: To manage paper and tray settings, click **Settings**. For details, refer to Configuring Tray Settings.
- Supplies: To view detailed information for toner, cleaning kits, and other user-replaceable items, click **Details**. For details, refer to Supplies.
- Billing: To view billing meter and usage details, click **Usage**.
- Apps: This section displays the configuration status for all apps that are enabled on the device. User-installed apps appear at the end of the list. If an app is not listed, check the App Enablement page. For details, refer to App Enablement.

  To configure apps and device functions, click the link associated with the app or function that you want to edit.

  - To configure the Copy App, click **Copy**. For details, refer to Specifying Default Copy Settings.
  - To configure email settings, click **Email**. For details, refer to Email Setup.
  - To configure the fax function, click **Fax**. For details, refer to Faxing.
  - To configure the ID Card Copy App, click **ID Card Copy**. For details, refer to Setting ID Card Copy Feature Defaults.
  - To configure the Print From App, click **Print From**. For details, refer to Configuring Print From.
  - To configure the Scan To App, click **Scan To**. For details, refer to Configuring Scan To.
  - To configure the fax filing repository, click **Server Fax.** For details, refer to Fax Repository Setup.
  - To manage file repositories and configure the Workflow Scanning App, click **Workflow Scanning**. For details, refer to Workflow Scanning.
  - To configure display settings and permissions for custom apps, click **Xerox® App Gallery**. For details, refer to Configuring Xerox® App Gallery Settings.
  - To configure settings for other weblets or EIP Apps, click the weblet or EIP App name. For details, refer to Weblet Management.
- Quick Links: This section provides links 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**. For details, refer to Restarting the Device in the Embedded Web Server.
- 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 time only, date only, time and date, 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 **Save**.

Quick Access

The Quick Access provides easy access to the features on the control panel. To configure Quick Access from the Embedded Web Server, do the following:

1. Select the features you want to add to the Quick Access link.
2. Click **Save**.
3. On the control panel, touch the circled-ellipsis icon, which represents Quick Access links to access the configured features without leaving your current task.

Accessibility

INVERTING DISPLAY COLOR FOR THE CONTROL PANEL

You can invert the display color of the control panel touch screen for all users.

1. Log in as a system administrator at the control panel.
2. Press the **Home** button.
3. Touch **Device > Tools**.

   A new window appears for Tools.
4. Touch **Device Settings > General > Accessibility**.

   A new window appears for Accessibility.
5. To invert the display color of the control panel screen, touch the **Invert Display Color** toggle button.
6. Touch **OK**.

You can clone the settings for Accessibility from Embedded Web Server. In the Embedded Web Server, there is an Accessibility group in Configuration Settings. For more information, refer to Cloning.

REMOTE CONTROL PANEL SPEECH OUTPUT

To enable or disable speech output access through the Remote Control Panel, select **Remote Speech Output Access** check box, then click **Save**. For more information, refer to Remote Control Panel.

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. In **"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 ranging 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

You can configure Energy Saver and Sleep Mode settings for the device.

The sleep timeout setting specifies the delay before the device enters Sleep Mode. If there is no activity at the control panel within the chosen interval of time, any logged-in user is logged out, device settings are reset to default values, and the device enters Sleep Mode.

Note: When the sleep timeout setting is set to a lower value than the session timeout setting, the sleep timeout setting overrides the session timeout setting. For details, refer to System Timeout.

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.
   - **Job Activated**: The device wakes when it detects activity.

     To set the delay before the device enters Sleep Mode, enter the number of minutes.

Note: Depending on the print speed capability of the device, the maximum value of the sleep timeout setting is 60 or 120 minutes.

   - **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 time, select the time of day.
3. To allow the device to power off after a period of time in Sleep Mode, select **Auto Power Off**.

   To set the delay before the printer powers off from the Sleep Mode setting, enter the number of hours.

Note: Selecting Auto Power Off is not recommended because the device does not respond until you power on the device manually.

4. For Additional Features, configure settings as needed.
   - **Smart Proximity Sensor**: If your printer has a Smart Proximity Sensor, you can enable the device to wake up and sleep based on the detection of a user.

     To set the printer to wake and sleep on the detection of a user, for Smart Proximity Sensor, click **Edit**. For details, refer to Configuring Smart Proximity Sensor Settings in the Embedded Web Server.
   - **Power in Sleep Mode**: Use this feature to select the power-saving option for Sleep Mode.

     To set the device Sleep Mode for optimized standard savings, or maximum savings, for Power in Sleep Mode, click **Edit**. For details, refer to Power in Sleep Mode.

   Note:
   - If a sensor is not detected, the Smart Proximity Sensor feature does not appear.
   - The Status area displays the current settings for each feature.
5. Click **Apply**.
6. If you applied settings for scheduled sleep and wake up times, the Enable Screen Saver pop-up window appears. Select an option:
   - **Enable**: This option enables the screen saver.
   - **Ignore**: This option does not enable the screen saver.

   To configure the screen-saver timer, use the Screen Saver page. For details, refer to Screen Saver.

   The device applies the Energy Saver settings with the selected screen saver option.

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 the Energy Saver feature does not appear, log in as a system administrator. For details, refer to Accessing the Control Panel as a System Administrator.
3. For Sleep Mode, select an option.
   - **Job Activated**: The device wakes when it detects activity.
   - **Scheduled**: The device wakes and sleeps according to a schedule that you specify.

4. For Job Activated, to change the default power-saver timeout periods, touch **Sleep Timers**.
   - To change the number of minutes before the device enters Sleep Mode, for Sleep Mode, touch the Plus (**+**) or Minus (**-**) icon, or touch the minute number, then use the keypad to enter a value.

   Note: Depending on the print speed capability of the device, the maximum value of the sleep timeout setting is 60 or 120 minutes.

   - To allow the device to power off after a period of time in Sleep Mode, for Allow Auto Power Off from Sleep Mode, touch the toggle button.

   Note: A check mark on the toggle button indicates that the feature is enabled.

   To change the number of hours before the device powers off after entering Sleep Mode, for Power Off, touch the Plus (**+**) or Minus (**-**) icon, or touch the hour number, then use the keypad to enter a value.

   - To save the timer settings, touch **OK**.
5. For Scheduled, to specify the schedule, touch **Scheduled Settings**.
   - To allow the device to wake when it senses activity on a specific day of the week, for Schedule Based On, touch **Activity**.
   - To allow the device to wake and sleep at a specific time of day, 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. If you are using a 12-hour clock, touch **AM** or **PM**.

   - To save the schedule settings, touch **OK**.
6. For Additional Features, configure the settings as needed.
   - To set the printer to wake and sleep on the detection of a user, touch **Smart Proximity Sensor**. For details, refer to Configuring Smart Proximity Sensor Settings at the Control Panel.
   - To optimize power savings for Sleep Mode, touch **Power in Sleep Mode**. For details, refer to Configuring Power in Sleep Mode at the Control Panel.

   Note:

   - If a sensor is not detected, the Smart Proximity Sensor feature does not appear.
   - The current settings are displayed next to the feature on the Energy Saver screen.
7. To save the Energy Saver settings, touch **OK**.

SMART PROXIMITY SENSOR

The Smart Proximity Sensor uses a reflection-type sensor to detect when a user approaches or leaves the device. This feature provides convenience for users, and can reduce power consumption.

Note: If a proximity sensor is not available in your printer configuration, the Smart Proximity Sensor option does not appear in the control panel menu.

Configuring Smart Proximity Sensor Settings in the Embedded Web Server

To configure Smart Proximity Sensor settings in the Embedded Web Server:

1. In the Embedded Web Server, click **Properties > General Setup > Energy Saver**.
2. In the Additional Features area, for Smart Proximity Sensor, click **Edit**.
3. To set the printer to wake when a user approaches the device, for Wake on Arrival, click the toggle button.
4. To set the printer to sleep when a user leaves the device, for Sleep on Departure, click the toggle button.

   Note: When Sleep Mode is based on scheduled settings, the Sleep on Departure option is disabled.

   After a user leaves the device, the device waits 14 seconds, then enters Sleep Mode.
5. To increase the proximity sensor detection range from 0–350 mm to 0–600 mm (0–13.78 in. to 0–23.6 in.), for Maximize Detection Range, click the toggle button.
6. Click **Save**.

Configuring Smart Proximity Sensor Settings at the Control Panel

To configure Smart Proximity Sensor settings at the control panel:

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **Device Settings > General > Energy Saver**.
3. In the Additional Features area, touch **Smart Proximity Sensor**, then configure the settings.
   a. To set the printer to wake when a user approaches the device, for Wake on Arrival, touch the toggle button.
   b. To set the printer to sleep when a user leaves the device, for Sleep on Departure, touch the toggle button.

   Note: When Sleep Mode is based on scheduled settings, the Sleep on Departure option is disabled.

   After a user leaves the device, the device waits 14 seconds, then enters Sleep Mode.

   Note: If the Build Job feature is selected at the device control panel, the 14 seconds delay is deactivated. The device enters Sleep Mode based on the Energy Saver timer settings.

   c. To increase the proximity sensor detection range from 0–350 mm to 0–600 mm (0–13.78 in. to 0–23.6 in.), for Maximize Detection Range, click the toggle button.
4. To save the proximity sensor settings, 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.

POWER IN SLEEP MODE

The Power in Sleep Mode feature controls the power usage when the device is in Sleep Mode.

The Standard Savings setting allows USB Type A accessories to operate when the rest of the device is in Sleep Mode. This setting permits Wi-Fi to maintain communication during Sleep Mode, and USB or card reader activity to wake the device, and the device to get ready to print sooner if it has been in Sleep Mode for only a short while.

The default setting is Maximum Savings. This setting saves the most power, but some USB accessories may not wake the device.

Note: You can configure Power in Sleep Mode from the Connectivity setup page in the Embedded Web Server, and from the Network Settings screen at the control panel. For more information, refer to USB Settings.

Configuring Power in Sleep Mode in the Embedded Web Server

To configure Power in Sleep Mode from the Energy Saver page in the Embedded Web Server:

1. In the Embedded Web Server, click **Properties > General Setup > Energy Saver**.
2. In the Additional Features area, for Power in Sleep Mode, click **Edit**.

3. On the Power in Sleep Mode page, select a power-savings option:
   - To achieve the highest amount of power savings, select **Maximum Savings**.

   Note:

   - The Maximum Savings option can prevent some USB Type A devices, such as card readers, from waking the device during Sleep Mode.
   - When wireless network adapter hardware is installed, the power state cannot be set to Maximum Savings.

   - To permit USB Type A accessories, such as card readers to operate during Sleep Mode, select **Standard Savings**.

   Note: Enabling Standard Savings can cause the device to consume more power in Sleep Mode, but can help to avoid issues with the following:

   - Network accessibility, such as network pings and device website access.
   - The ability to wake up from sleep mode or wake on the submission of print jobs.
   - Interoperability with some managed network switches.
4. Click **Save**.

Configuring Power in Sleep Mode at the Control Panel

To configure Power in Sleep Mode from the Energy Saver screen at the control panel:

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **Device Settings > General > Energy Saver**.
3. In the Additional Features area, touch **Power in Sleep Mode**.
4. For Power State in Sleep Mode, select **Maximum Savings** or **Standard Savings**. For details, refer to Configuring Power in Sleep Mode in the Embedded Web Server.

   Note: When a wireless network adapter is installed, the power state cannot be set to Maximum Savings.
5. To save the power state setting, 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 launch the Remote Control Panel with speech output, select **Use Speech Output**. The device interactions will only be heard through the screen reader if Use Speech Output option is enabled.

Note: Operating the Remote Control Panel while using your screen reader may require switching the screen reader mode (Browse/Focus Mode). Different screen readers have different ways to toggle the screen reader mode. For example, use the Caps Lock + Space Bar or Insert + Space Bar to toggle between the screen reader modes.

Note: Screen readers have their own shortcuts, behaviors, and announcements. For more information, refer to the screen reader documentation provided by the respective vendor.

Note: Remote control panel speech output is independent from the speech output on the local user interface. Accessibility controls on the Local Control Panel do not affect the Remote Control Panel. When you start speech output on the Remote Control Panel while the speech output is active on the device, the announcements on the local user interface will be stopped.

To access the control panel remotely, click **Start Remote Session**.

Entry Screen Defaults

Use the Entry Screen Defaults page to set screen defaults or actions for a walk up or guest user.

You can set the default app that appears on the device control panel touch screen. You can also set the default app that appears when original documents are detected in the automatic document handler or on the document glass.

Note: When Automatically Set Device Defaults is enabled for entry screen defaults, the following message appears: `Adaptive Learning is Setting Defaults`.

When Automatically Set Device Defaults is enabled, settings can change from the defaults that you specify. To change the Adaptive Learning configuration, refer to Adaptive Learning.

To configure the Entry Screen Defaults settings at the Embedded Web Server, refer to Setting the Default Walk-up Screen, Setting the Default Screen when Originals are Detected, and Enabling the Auto Start when Originals are Detected Feature.

SETTING THE DEFAULT WALK-UP SCREEN

Default walk-up screen is the default screen displayed when the user walks up to the machine.

To set the default walk-up screen, do the following:

1. In the Embedded Web Server, click **Properties > General Setup > Entry Screen Defaults**.
2. In the Default Walkup Screen area, select Home or select an app from the list.
3. Click **Apply**.

Note: When Personalization is enabled, a logged-in user can personalize their walk-up app. The preferred app opens when the user logs in at the device control panel.

For more information on setting the default app screen at the control panel, refer to Setting the Default Walk-Up Screen at the Control Panel.

SETTING THE DEFAULT SCREEN WHEN ORIGINALS ARE DETECTED

Note: When Personalization is enabled, a logged-in user can personalize their default app for when original documents are detected. The personalized setting for the default app when original documents are detected applies to a logged-in user when the control panel displays the home screen. The preferred app opens when the user places documents in the automatic document feeder.

For more information on configuring this setting at the control panel, refer to Setting the Default Screen when Originals are Detected at the Control Panel.

This feature sets the default app to launch when original documents are loaded in the automatic document feeder.

To set the default screen when original documents are detected, do the following:

1. In the Embedded Web Server, click **Properties > General Setup > Entry Screen Defaults**.
2. For Default Screen when Originals are Detected, select an app from the list. To take no action, select **None**.
3. Click **Apply**.

ENABLING THE AUTO START WHEN ORIGINALS ARE DETECTED FEATURE

The Auto Start when Originals are Detected feature allows the device to start a job automatically within an app. The feature applies when an app is open and Auto Start is enabled for that app. When the device detects documents in the automatic document feeder, the job starts automatically within 7 seconds, unless the user cancels the automatic operation. Each user can configure the Auto Start setting.

Note:

- The Auto Start feature is disabled for all of the listed apps by default.
- When Auto Start occurs for a job, the app displays a 7-second countdown before the job starts. The user can change the job settings or start the job immediately.
- When Auto Start is enabled for an app that is open, each time original documents are loaded in the automatic document feeder, the device starts a job automatically. The user does not need to close and reopen the app between jobs.

To enable the Auto Start feature and start a job automatically within an app, do the following:

1. In the Embedded Web Server, click **Properties > General Setup > Entry Screen Defaults**.
2. In the Auto Start when Originals are Detected area, click **Choose Apps**.
3. To enable or disable the Auto Start feature for a listed app, click the toggle button for that app.

   Note: The Auto Start feature applies to Copy, Email, Fax, Scan to, and 1-Touch apps.

   Note: When Personalization is enabled, a logged-in user can personalize their Auto Start settings for all supported apps.
4. To enable the Auto Start feature for all listed apps, click **Turn On Auto Start For All Apps**.
5. To disable the Auto Start feature for all the listed apps, click **Turn Off Auto Start For All Apps**.
6. Click **Save**.
7. Click **Apply**.

Remote Services

Remote Services is a suite of features that simplify device ownership and administration. Remote Services provides free services to enable the administration of reporting for metered billing, supplies replenishment plans, and automatic software upgrades for devices on a network.

Remote Services allows the device to send diagnostic information to Xerox for analysis and fault correction. For more information, refer to Managing Diagnostics and Usage Information.

Before you begin, if your network uses an HTTP proxy server, configure settings on the Proxy Server page. For details, refer to Proxy Server.

CONFIGURING REMOTE SERVICES

Use the Remote Services page to configure communication to the Xerox datacenter, and to process received updates.

Note: If your network uses an HTTP or HTTPS proxy server to access the internet, ensure that the correct configuration or remote services will not operate as required. For details, refer to Proxy Server.

To configure Remote Services:

1. In the Embedded Web Server, click **Properties > General Setup > Remote Services**.
2. To enable Remote Services, for Policies and Schedule, click **Configure**. For details, refer to Policies and Schedule.
3. To send or receive data between the device and the Xerox datacenter, click **Check Now**.
4. When the check is complete, the Receiving Status area displays an updated status message:
   - `No new update is available`
   - `New update is available to manually install`
   - `New update is available to install on <date/time>`
   - `New update is available; installation is paused`
   - `New update has been submitted for installation`
5. If an update is available, for Available Update, select an option:
   - **Cancel**
   - **Pause**
   - **Resume**
   - **Install Immediately**
6. The Sending Status area shows the last date that device diagnostic fault information was sent to Xerox. To disable the automatic sending of diagnostic information to Xerox, refer to Policies and Schedule.

POLICIES AND SCHEDULE

To enable Remote Services and configure communication policies:

1. In the Embedded Web Server, click **Properties > General Setup > Remote Services**.

2. At the Remote Services page, for Policies and Schedule, click **Configure**.
3. At the Policies and Schedule page, select the check box for **Enable Remote Services**.
4. In the Receiving Policies area, set the policies, as needed:
   - To set when the device checks for updates, for Daily Check, set the time of day.
   - To enable the device to receive keys from the Xerox Corporate Licensing Server, select the check box for **Allow device to receive keys from the Xerox Corporate Licensing Server (XCLS)**.
   - To enable the device to receive software updates, select the check box for **Allow device to receive updates**.
   - To allow the Xerox datacenter to modify internal non-volatile memory settings, select the check box for **Allow device settings to be changed (non-volatile memory)**.
   - To set the installation schedule, for Installation Schedule, select an option:
     – To install the updates as soon as possible after the updates are available, select **Automatically**.
     – To set a daily installation time, select **Daily**, then set the time of day.
     – To set a weekly installation time, select **Weekly**, then set the day of the week and the time of day.
   - To notify administrators when updates are available, for Email System Administrator when updates are available, click **Configure**. On the Notification Settings page, configure email alerts. For details, refer to Email Alerts.
5. In the Sending Policies area, set the policies, as needed:
   - To view what is included in the basic device information, for Basic Device Information, click **Download**. Right-click the file link, then save the file to your computer.

     Basic device information and meter readings are included automatically in the information sent to Xerox.
   - To allow the device to send diagnostic information automatically to Xerox when a fault occurs, select the check box for **Automatically send diagnostic information to Xerox when faults, that require Xerox assistance, occur on the device**.

   Note: If your network uses an HTTP or HTTPS proxy server to access the internet, ensure that the correct configuration or remote services will not operate as required. For details, refer to Proxy Server.
6. To apply the new settings, click **Save**, or to retain the previous settings, click **Cancel**.

Remote Management Server Setup

When enabled, 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.

Note: The service discovery runs after the device starts, or when you request that the device performs the discovery.

To detect the remote-management server, the Remote Management Server Setup feature queries your DNS server.

- The feature searches for a server called `XeroxDiscoverServices` 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 server `XeroxDiscoverServices.yourdomain.com` in your DNS server. This is the simplest process for the printers to find the remote-management servers automatically.
- If you cannot change the host name of the Remote Management Server as suggested, the 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 of `XeroxDiscoverServices.yourdomain.com`. Use the alias to refer to `server1.yourdomain.com`.
- If you have multiple remote-management servers to find in one domain, 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 XeroxDiscoverServices keyword. DNS returns the server list to the device. The device works down the list of up to 10 servers, then attempts to check in to all of them.

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**.
   - The Claim Status field displays claim status messages that are sent from the server.
   - Information about the last check-in appears in the Last Status Results area.
6. Click **Apply**.

Security Dashboard

The Security Dashboard displays both user-defined and default security configurations, and also allows the user to monitor the security status of the device. The majority of the security features are user-specified and few security features cannot be altered. To configure the security features, in the embedded web server, click **Properties > Security Dashboard** and navigate to list of security options available in the Security Dashboard window and click **GoTo** icon for the specific security feature.

Security Template

To choose a security template in the Embedded Web Server, perform the following:

1. Click **Choose a Security Template**.
2. In the Choose a Security Template window, perform the following:
   a. From the Template menu, select **Default**, **Elevated**, or **High**.

      The security features for Device, Print, and Scan functions are displayed.

   b. To view the features and settings of each template selected, click toggle button for **Show Features**.
3. Click **OK**.

To choose a security template at the control panel, perform the following:

1. At the control panel, touch **Device**, then touch **Tools**.
2. Touch **Security Settings > Security Template**.
3. In the Choose a Security Template window, perform the following:
   a. From the Templates menu, select **Default**, **Elevated**, or **High**.

      The security features for Device, Print, and Scan functions are displayed.

   b. To view the features and settings of each template selected, click toggle button for **Show Features**.
4. Click **OK**.

Note: Every time you click **Choose a Security Template**, the following message appears: `Choosing a security template may overwrite existing security settings`. To save the changes, click **Continue** or click **Cancel**.

Note: If you select Elevated or High security template, the following message appears: `The selected Security Template will disable USB ports, impacting connected devices such as WiFi dongles`. To proceed further, click **Use Current USB Settings** or **Update USB Settings**.

Note: If the Security Template is not applied, the following message appears: `Security Template was not applied. Try again`. To proceed further, click **Close**.

AUTHENTICATION

These features identify users and grant access.

- **Methods**: This feature allows the user to set the authentication method, enable personalization options, and configure related settings.
- **Permissions**: This feature sets permissions for both guest and logged-in users and configures the role for all users who are not logged in to the printer.
- **System Timeout**: This feature allows users to specify a duration for an inactive user to remain logged-in to the printer and the Embedded Web Server before being logged out automatically.
- **Admin Password**: This feature allows you to set a new password and to configure the password requirements for local authenticated users, and also unlocks settings in the Embedded Web Server or in the device control panel.

CONFIDENTIALITY

These features keep user data private.

- **Print Jobs**: The Print Jobs page has various security features that allow users to configure data privacy and security in all phases of the jobs being printed and also removes all stored data associated with print jobs.
- **User-Name (PII)**: This feature hides the user name of a logged-in user and completed jobs from the control panel display.
- **Scan Jobs**: The Scan Jobs page has various security features that allow users to define data privacy and security policies in all scanning phases, as well as store and manage scan data locally and remove all stored data associated with scan jobs.

INTEGRITY

These features keep device policies safe.

- **Configuration Policies**: This security feature allows you to ensure devices stay in the appropriate configuration throughout the day with no need for external device monitoring.
- **File System Protection**: This feature maintains the integrity of device software and enhances security features with the ability to monitor and prevent unauthorized files.
- **Tracking (Logs)**: The Tracking (Logs) page has various security features that allow users to configure log settings, device authentication log details, and security solutions that help the device to recognize and alert the user about potential threats.

AVAILABILITY

These features monitor hardware components.

- **USB Ports**: This feature allows the user to enable or disable USB host ports, and to manage USB device port policies.
- **Mobile Devices**: This feature allows the devices to connect to each other without requiring a wireless access point.
- **Drive Storage**: This feature stores the data on the optional drive when installed and on the internal drive through the User Data Encryption protocol.

QUICK LINKS

- **Security Dashboard Access**: This feature allows you to restrict the security dashboard access for other users.
- For more security features, refer to https://www.xerox.com/security.

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:

- 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.
- Software upgrade files: A software upgrade file contains the latest firmware for the device. Xerox releases upgrades when needed.
- 1-Touch Add-On files: A 1-Touch Add-On file adds workflows to a device without overwriting existing apps or workflows.

For devices that have the Xerox Fleet Orchestrator feature installed:

- You can share clone files across different models of Xerox® AltaLink® multifunction printers. Devices can be on the same or different versions of system software.
- You can share software upgrade files across devices that use the same upgrade file only.
- You can share 1-Touch Add-On files to devices on the same or a higher version of system software. Due to feature changes, it is not guaranteed that 1-Touch Add-On files can be shared to devices on a lower version of system software.
- If you are sharing all types of files, the software upgrade file installs first, followed by the clone files, then the 1-Touch Add-On files.

For details on this feature:

- Continue to Automatic File Sharing.
- In the Embedded Web server, click **Properties > Fleet Orchestrator**, then click **Learn More**.

Note: Fleet Orchestrator is an optional feature. It is possible that Fleet Orchestrator is not appropriate for some enterprises or situations.

AUTOMATIC FILE SHARING

The Fleet Orchestrator feature allows you to share files automatically between devices in your fleet. The Fleet Orchestrator feature uses a distribution tree to share files from one device to other devices. To share files, you set up a file-sharing group of devices. This group is also called a trust community. Devices in a trust community work together automatically, without manual intervention.

You can set up the Publisher to share files with other linked devices within a trust community. A trust community forms when the Publisher connects to one or more devices. When file-sharing groups are formed, the devices within the trust community can share files. The Publisher maintains and manages the trust relationship for all of the devices in the distribution tree. The trust relationship remains intact until you revoke it.

You can customize the Fleet Orchestrator and Auto-Assembly to provide as much or as little management and automation as you want. You can configure the features to provide no fleet management at all to fully automated assembly and healing of all printers in a fleet.

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. Each trust community can have only one tree. To set up more than one tree, you can set up multiple Publishers.

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 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 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 Subscribers, 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.

Configuration Overview

To set up file sharing, on the Publisher, you can arrange trusted devices into a hierarchy called a Tree. File sharing includes the following tasks:

- Designate a device as the Publisher of the tree.
- Designate a friendly name for the Publisher. The friendly name of the Publisher 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 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 in the trust relationship can be a Xerox® Device Manager server, or a Xerox® CentreWare® Web server.

- 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, you can view the complete tree structure. On Subscriber, 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.

Configuring Automatic Assembly of a Fleet

To facilitate the management of a fleet of Xerox® multifunction printers, you can configure Fleet Orchestrator to assemble a fleet of compatible printers automatically.

After you configure the Publisher, you can distribute the configuration settings to Subscribers, as needed. You can configure the Publisher to share any or all of the following file types: clone, software upgrade, and 1-Touch Add-On. The Publisher distributes its shared files to the entire fleet. Each device downloads the files from its parent device and installs the files automatically based on a defined schedule.

The device discovery process is based on DNS and DHCP.

The Auto-Assembly process requires that you have more than one Xerox® AltaLink® multifunction printer.

Setting Up the Publisher

1. Choose one Xerox® AltaLink® multifunction printer to be the Publisher.
2. Set the host name on that printer as `XeroxDiscoveryFleet`. For details, refer to Configuring DNS.

   Note: If it is not possible to use the name `XeroxDiscoveryFleet`, you can set up an alias. Refer to Configuring DNS.

   Note: If you use DHCP addressing on your network, the name is added to your DNS server automatically. If you use Static addressing, add the name to your DNS server manually. For details, refer to Configuring DNS.
3. To ensure that the Publisher can be found on your network, test the connection using one of the following methods:
   - Ping the device on your network at XeroxDiscoveryFleet.{your.domain.com}.
   - To view the Publisher webpage, in a browser, open http://XeroxDiscoveryFleet.{your.domain.com}.

   Note: If you cannot connect to the Publisher, ensure that the Host Name is correct.
4. After you verify that the Publisher host name is correct, log in as administrator to the Embedded Web Server for the Publisher. Click **Properties > Fleet Orchestrator**.
5. To configure the device as a Publisher:
   a. Click **Configure File Sharing**.
   b. On the Configure File Sharing page, select **Publish Files & Manage File Sharing Group**.
6. To add new Subscribers automatically, on the Configure File Sharing page, click **Publisher Policies**. In the Publisher Policies area, for Automatically Accept New Devices, select the toggle button. A check mark indicates that the feature is enabled.

7. Specify where Subscribers are situated in your trust community. In the Publisher Policies area, from the New Device Location in Group list, select an option:
   - **Publisher**: This option allows additional Subscribers to be situated in your trust community and be attached to the Publisher directly. If there are more than 5 Subscribers and they attempt to download at the same time, file sharing from the Publisher can be delayed.
   - **Community**: This option allows additional Subscribers to be situated in your trust community automatically or be attached to the Publisher directly. This option is the default.
   - **Unassociated**: This option places additional Subscribers into an on-hold state. For details, refer to Unassociated Devices.

   Note: If you want a partial level of automated assembly, the process begins when you assign the name `XeroxDiscoveryFleet` to the Publisher. When you choose to assign Subscribers to the Unassociated group, the new devices are gathered, but files are not shared to them. To begin sharing files to a device in the Unassociated group, move the device into the trust community.
8. In the New Subscriber Admin Credentials area, type the administrator user name and password that you use for the devices on your network. These credentials are used to add other devices to the fleet.
   - The administrator can use the Auto-Assembly feature to situate new printers as child devices of the Publisher or of other trust community members. In this scenario, files are shared from the parent device to the child devices automatically.
   - Alternatively, the administrator can choose for the devices to join the trust community and to be placed into the Unassociated group. This scenario holds the devices but does not allow files to be shared with those devices until the administrator moves the devices into place manually.

   Note: The Publisher attempts to add new Subscribers with the user name and password that you specified in Publisher policies. If necessary, the Publisher uses the default credentials for new devices.
9. To exit the Publisher Policies page, click **Save**.

After Auto-Assembly is set up, the device is now a Publisher for this trust community. The other Xerox devices in the network are able to contact the Publisher and try to join the trust community automatically. You can create a clone file on the Publisher with the typical settings that your devices use, then share the clone file with the Subscribers. For more information, refer to Adding Files to the Publisher for Distribution.

As new devices connect to the network for the first time, if they can find a fleet and a clone file, the devices skip many of the questions in the Installation Wizard. For more information, refer to Installation Wizard.

Adding Files to the Publisher for Distribution

1. Create a clone file on the Publisher. A clone file is a snapshot of the settings to be shared to the Subscribers. For details, refer to Creating a Clone File.
2. On the same network, connect a second device, then power on the device.

   At startup, the second device looks for the Publisher in the DNS server and attempts to connect to the Publisher. The Publisher adds the second device automatically.

As each printer that supports Auto-Assembly powers on, or each day, the devices contact the Publisher and join the fleet. If necessary, you can pause Auto-Assembly. For details, refer to Setting the Security Installation Policy for File Sharing.

After a Publisher shares a clone file, the Subscriber downloads and installs the clone file according to your schedule.

If a Publisher is sharing a clone file already, when a new device joins the fleet, the new device downloads the clone file immediately.

Schedule Cascade

When a Subscriber is situated in the tree, the schedule for the Subscriber is set to one hour later than the schedule for its parent device. The schedule difference allows time for the parent device to receive and install files before the Subscriber issues a request for the files.

Self-Heal

If a Subscriber cannot contact its parent device for more than 10 days, the Subscriber contacts the Publisher and requests a different parent device.

You can manually choose to reconnect a Subscriber. To reconnect a Subscriber manually, in the Receiving Details area, click **Reconnect To Publisher**.

Activity Log

On both the Publisher and Subscriber, the activity log records activity for each of the major Auto-Assembly operations. If a device shows unexpected activity, or if a device is not showing expected activity, the activity log can be a helpful resource. The activity log is an .xml file that you can download and open in a spreadsheet program or text editor. The newest entries are at the end of the file.

To view or download the activity log, in the Embedded Web Server, click **Properties > Fleet Orchestrator**. Click **Activity Log**, then open or save the .zip file. From the .zip file, extract the .xml file, then open the file in a text editor or spreadsheet program.

Compatibility

You can use Fleet Orchestrator across various Xerox® AltaLink® printer models, but the Auto-Assembly functions require that the latest software version is installed on all devices.

Setting Up a Fleet Manually

To create a fleet manually, you begin with a Publisher, then add each Subscriber manually. You can add Subscribers from the Publisher or from other Subscribers.

1. Create a tree structure for the file-sharing group. To create a tree, add Subscriber and Distributors to the file-sharing group. The added devices form a trusted relationship. For details, refer to Adding a Device from a Publisher or Adding a Device from a Subscriber.

   Note: If you use Xerox® Device Manager or Xerox® CentreWare® Web software, the Publisher in the trust relationship can be a Xerox® Device Manager server, or a Xerox® CentreWare® Web server.

2. Create download and installation schedules for each device. For details, refer to Adding a Device from a Publisher.
3. Make a clone file, software upgrade file, or both types of files available for distribution. For details, refer to Creating a Clone File or Software Upgrade Files.

   Note: If two or more devices require a device-specific clone file or software upgrade, you can create a separate distribution tree. You can create as many distribution trees as required.

On the Publisher, you can view the complete tree structure. On Subscribers, you can view only some 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 for the device. As you add more devices, you can use this system to send files to one device, then send the files from that device to other devices.

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 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. Select or clear **Allow Auto Assembly**:
   - When Allow Auto Assembly is selected, new printers are added as Subscribers to the Publisher automatically.
   - When Allow Auto Assembly is not selected, new printers are not added as Subscribers automatically. This option requires that you add the Host information manually. For details on how to join a Publisher manually, refer to Adding a Device.
4. Click **Apply**.

Configuring File Sharing

You can use the Configure File Sharing feature to configure your printer as a Publisher.

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:

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. You can subscribe to the file-sharing group from a Subscriber.

Adding a Device from a Publisher

To add a device to the file-sharing group from the Publisher:

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.
   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.

d. For Random Download Delay, select the number of minutes for the random delay.
Setting the Random Download Delay minutes ensures that devices do not pull configuration files from a Distributor 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, but you can change the relationships between Distributor and Subscriber.

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, select an option:

- **Auto Join**: This option allows the device to join a Publisher with a DNS Host Name of `XeroxDiscoveryFleet`. To instruct the device to join a Preferred Publisher, select the **Join a Preferred Publisher** toggle button. To add the host information for the Preferred Publisher, select an option:
  - **Fully Qualified Domain Name**: Type the domain name for the Preferred Publisher.
  - **IPv4 Address**: Type the IPv4 address for the Preferred Publisher.

Note: The Auto Join option is available when the security installation policy for Fleet Orchestrator is set to Allow Auto Assembly. For details, refer to Setting the Security Installation Policy for File Sharing.

- **Manual Join**: This option requires that you add the Host information manually. Select an option:
  - **Fully Qualified Domain Name**: Type the domain name for the Publisher.
  - **IPv4 Address**: Type the IPv4 address for the Publisher.

5. Click **Start Sharing**.

Note: If you selected **Manual Join** in the Receiving Details area, the Add Device page of the Publisher appears.

To add the download schedule and installation settings for the Subscriber, use the Add Device page. For more information, refer to Adding a Device from a Publisher.

Editing a Device

From the Publisher, you can edit the download schedule and installation settings for Subscribers. 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. To edit one device, choose Tree view and select **Edit Selected**.
5. To edit one or more devices at a time, choose Table view and do the following:
   - Select one or more check boxes for the device you want to edit.
   - Select **Edit Selected**.
6. 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.
7. 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.
8. Click **Update**.
   The Share Configuration Files page appears. To change the file-sharing group, use the options on this page.
9. To close the Share Configuration Files page, click **Close**.

Deleting a Device

At the Publisher, to delete a Subscriber 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.

   To delete one device at a time, choose Tree view and do the following:

   - In the Devices area, select a device.
   - Click **Delete Selected**.
   - At the prompt, confirm the deletion.

   Note: To select multiple devices, choose Table view, then select the check box for each device to be deleted.

4. To delete more than one device, use Table view. Do the following:
   - Select the check box for each device you want to delete.
   - Click **Delete Selected**.
   - At the prompt, confirm the deletion.

Deleting a Device Connection

The preferred method for deleting a device is from the Publisher. For details, refer to Deleting a Device.

> **Caution:** Deleting the connection from a Subscriber 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, 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, 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 Publisher from communicating with other devices in the file-sharing group:

1. In the Embedded Web Server for the Publisher, 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:

1. In the Embedded Web Server for the Subscriber, 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, and do not receive updated configuration files.

A device is Unassociated when:

- You drag a Subscriber 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 for the device is deleted.

Reconnecting Unassociated Devices

To reconnect an Unassociated device to the file-sharing group on the Publisher, do the following:

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.
4. Click **Close**.

To reconnect or edit an Unassociated device, do the following:

- On the File Sharing page, in the Devices area, using the Table view, select the device.
- Click **Edit Selected**.
- In the Edit Devices area, click Download Files Form.

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 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.

Working with Multiple Fleets

In an environment with multiple fleets, to keep devices separate, you can choose one of the following options:

- You can disable automatic fleet assembly.
- You can use one device as a gathering point, then move the various printers to separate fleets manually.

If you have more than one domain, you can choose one of the following options:

- You can set up separate Publishers for each domain.
- To allow devices on one domain to find the Publisher on another domain, you can use a DNS alias. Refer to Configuring DNS.

If two or more devices require a device-specific clone file or software upgrade, you can create a separate distribution tree for those devices. You can create as many distribution trees as required.

Troubleshooting

Errors can occur when you are managing your devices. The best way to troubleshoot is to open the Publisher and the Subscriber, then view the status of each device.

To view troubleshooting information 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 Share Configuration Files area, click **Advanced > Troubleshooting**.

Automatic Retries

If a scheduled download to a Subscriber fails, the device attempts to retry the download up to three 3 times on the same day. The retry schedule is determined by a fixed time factor and a random time delay (R). The device performs a retry at the following time intervals:

- 0.5 hours plus R minutes after the scheduled download time
- 1 hour plus R minutes after the first download retry
- 2 hours plus R minutes after the second download retry

Note:

- The random time delay is specific to a device.
- The range for the random time delay is 1-60 minutes.
- If a retry operation is successful, subsequent retries are cancelled.

When a retry is scheduled, the File Sharing page displays the following status message:

```
Retrying download at <date-time-stamp>
Updated: <date-time-stamp>
```

Configuration File Types for Automatic Sharing

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. To allow clone files to install on the device, for Cloning, select **Allow Clone File Installation**.

   Note: The cloning policy allows encrypted clone files to install on the device only. The policy does not allow unencrypted clone files to install on the device.

3. To allow the device to receive clone files through a remote print job, select **Allow Print Submission**. At the confirmation prompt, click **Allow**.

   Note: The Allow Print Submission option allows the device to receive clone files using print submission methods, such as Line Printer Remote (LPR). The installation of clone files through the print path can allow unauthenticated clone files to install on the device. It is recommended to use this feature temporarily, when needed.

4. To prevent installation of clone files through the print path, either remove your selection from **Allow Print Submission**, or click **Permanently Restrict Print Submission**. At the confirmation prompt, click **Restrict**.

   Note: If you restrict print submission permanently, you cannot reinstate the print submission option at a later date.

5. 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 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**.

   Note: By default, the FIPS group is not selected when creating a clone file. To clone the FIPS settings, you need to select **Select All Groups** to ensure that all FIPS settings are included in the clone file.

   - 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. After the clone file installation is complete, you can reenable FIPS 140. If you are using the file-sharing function of Fleet Orchestrator, you do not have to disable FIPS 140 to receive clone files. For information on FIPS 140 settings, refer to FIPS 140.

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.

For FIPS 140 Users only:

Devices using the FIPS 140 security modes can share Software Upgrade, 1-Touch Add-On, and Clone files with other devices in the Tree, using Fleet Orchestrator.

- If you want to share the Clone files from a FIPS 140 Publisher, ensure that the FIPS 140 mode is set for each Subscriber individually. There may be conflicts that have to be resolved by the SA for some devices.
- Set FIPS 140 on each device. Browse to each device web page, change the settings for FIPS 140, then follow the onscreen prompts to resolve any FIPS 140 conflicts.
    1. Start File Sharing on the Publisher.
    2. Create a Clone file on the Publisher and mark it as Sharing.
    3. Add Subscribers to the Trust Community.

Note:

- The Publisher can enable or disable FIPS 140 for the Publisher itself without affecting the Subscribers. The default setting is Disabled.
- If a Subscriber device is enabled for FIPS 140, the device can receive Clone files using Fleet Orchestrator.
    - Manual Clone file installation is not allowed to a device already in FIPS 140 mode.
    - If you have a Clone file to apply to a Publisher, disable FIPS 140 temporarily.

Extended Clone Details

The Extended Clone Details page displays information about the latest installation of a clone file.

At the top of the page, the status area displays the name of the clone file, the most recent installation date, and the status of the installation. The possible statuses include:

- `Clone file failed to install`: The clone file installation failed.
- `Clone file installed successfully`: The clone file installed without exceptions.
- `Clone file installed with exceptions`: The clone file installed with an exception in at least one area.

The Area table lists the cloned features with the status for each feature.

Note: The areas listed depend on the groups included in the clone file. A clone file that includes all groups contains many areas. A clone file that includes fewer groups contains fewer areas.

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**.

Clone Troubleshooting

Use the Clone Troubleshooting page to investigate cloning exceptions. If your clone file installs with exceptions, this signifies that one or more cloned areas installed with an exception.

Exceptions can occur in the following situations:

- When a clone file is created from a different version of software to the version installed on your device, a mismatch between settings in the two versions can occur.
- When a clone file is created on a different model to your device, some settings are not applicable to your device. For example, if a clone file with color print settings is applied to a black and white printing device.
- When a clone file is created on a device with a different hardware configuration to your device, some settings are not applicable to your device. For example, if a clone file with fax settings is applied to a device with no fax option installed.

To troubleshoot exceptions:

1. In the Embedded Web Server, click **Properties > Fleet Orchestrator**.
2. In the Configuration Files area, for Clone, click **View**.
3. Review the detailed status on the Extended Clone Details page. Note all areas with exceptions.
4. For the relevant areas, do the following:
   a. Review the feature settings where an exception occurred. To verify the settings, refer to the relevant settings page in the Embedded Web Server.
   b. Test the feature on the device. Ensure that the feature is working as expected.

c. Adjust the feature settings, as needed.

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:

Note: Downgrades may be restricted to some software releases because of hardware configurations and software version incompatibility.

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 install the upgrade on a Publisher, and you use file sharing, select the **Share This File** option.

Note: On the Fleet Orchestrator page, when you select Configure File Sharing, the Share This File feature appears. This feature is available for a Publisher only. For details, refer to Configuring File Sharing.

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 a Configuration Report. To verify that the software has updated, check the Configuration Report, or view the current software version in the Embedded Web Server or on the local User Interface (UI). For details, refer to Extended Software Upgrade Details.

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**.

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 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**.

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 USB Port Management at the Control Panel.

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.

   Note: By default, the FIPS group is not selected when creating a clone file. To clone the FIPS settings, you need to select All Groups in the embedded web server to ensure that all FIPS settings are included in the clone file. For details, refer to Creating a Clone File.
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**.

Configuring the Custom Keyboard Button

The custom keyboard button allows you to customize the keyboard for the printer at the control panel. You can configure the custom keyboard button according to your need. For example, you can configure the keyboard button to appear as `@xerox.com`.

To configure the custom keyboard button, do the following:

1. At the control panel touch screen, touch **Device**, then touch **Tools**.
2. Touch **Device Settings > General > Custom Keyboard Button**.

   The Custom Keyboard Button screen appears.
3. To configure the custom keyboard button, in the text field, type the text as you want it to appear on the button. Touch **Preview**.
4. To save the setting, 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.

To backup settings on the device Daily or Manually, click **Update Now** or **Backup Settings Now**. The date and time of the backup file created appears in the **Backup Date/Time** column.

Note: The settings contained in the Daily backup file will be reapplied after a software upgrade. Updating this file before upgrading software maintains the most recent settings of the device.

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.

Supplies

Supplies include toner, ink, paper, cleaning kits, and other items that you can order and replace yourself. The Supplies page displays a list of currently installed printer supplies and reports status for each item.

- To order the supplies, click **Order Supplies**.
- To update the page, click **Refresh**.
- To view supply details, including part numbers for reordering, area coverage information, and installation date of supplies, click **Details**.

DETAILS

The Details page shows all of the supplies currently installed on the printer. You can view details for each supply including the date installed and the Xerox reorder number when your supplies run low.

Note: Average Area Coverage indicates how much ink or toner you are using per page. If the Average Area Coverage is higher than 5%, you are using a relatively high amount of ink or toner per page. Your ink or toner supply can expire more quickly than the rated lifetime.

ORDER SUPPLIES

The Order Supplies page contains Buy From, Supplies Plan, and Supplies Log.

- **Buy From**: This area allows users to order the required supplies and, optionally, add a supplier for you and your users to contact.

  Note: The Xerox Retail Store is listed as a supplier for your convenience.

  In the Buy From area, perform the following:

  1. To order, click **Order** on the respective supplier.

     It shows the complete information of the supplier, such as Supplier Name, Phone Number, and Website URL. Click **Buy** to order supplies.

  2. To add a preferred supplier, click **Add**, enter the supplier information, then click **Add** in the Supplies Plan page. For more information, refer to Supplies Plan.

  Note: User must be logged in to access Supplies Plan Page in the Properties tab.

- **Supplies Plan**: This area displays current Plan/Feature of the supplies. The following are the options of Plan/Feature:
  - Metered/Page Pack
  - Learning Mode/Unknown
  - Sold
  - Third Party

  For more information on your Metered Plan, visit the Metered Supplies page at www.xerox.com.

- **Supplies Log**: This area allows user to save the last ordered date of the supplies and also details of the ordered supplies in the Notes filed which is optional.

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**.

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. 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, or 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**.

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.xerox.com/office/support, 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

To restart the device, use the Software Restart option. The restart process is faster than powering the device off and on.

Note: Restarting the device can take up to five minutes. During this time the Embedded Web Server is not available.

1. At the control panel, log in as an administrator. For details, refer to Accessing the Control Panel as a System Administrator.
2. Touch **Device**, then touch **Tools**.
3. Touch **Troubleshooting**, then touch **Resets**.
4. In the Resets window, touch **Software Restart**.
5. At the Software Restart screen, touch **Restart**.
6. At the restart confirmation prompt, 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 and if equipped, remove the wireless dongle.
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. If not already done, 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. Software downgrades are not recommended.

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 Software Upgrade Files.

MANUALLY UPDATING THE SOFTWARE USING A USB FLASH DRIVE

Note: Ensure that at least one USB Type A Port is enabled.

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.

Note: To eject the USB from the computer, follow the Microsoft's Safely Remove the USB procedure.

Note: Downgrades may be restricted to some software releases because of hardware configurations and software version incompatibility.

To set the installation policy for software upgrades, refer to Setting the Security Installation Policy for Software Upgrade.

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 a Configuration Report.

Updating Card Reader Firmware

You can use the Firmware Update feature to install a card reader firmware update. The Firmware Update feature enables you to submit a firmware update to a card reader that is connected to the device.

Note:

- Not all card readers support firmware updates. For more information, refer to the documentation included with the card reader.
- Install a card reader firmware update only when a card reader is connected to the device.
- The firmware update for a card reader is independent of other software upgrade processes for the device.
- If no card reader is detected on the device, the Firmware Update feature is not available.

The device detects whether an attached card reader is upgradable. The status area displays the firmware version installed on the card reader and the date that it was installed.

Note: If the card reader has received no updates, the factory-installed firmware version is displayed without a system time stamp. A time stamp appears after the first firmware update.

To update the firmware on a card reader attached to the device:

1. Ensure that the update policy for card reader firmware is enabled.
   a. In the Embedded Web Server, click **Security > Installation Policies**.
   b. For Card Reader Firmware, select the check box for **Allow Firmware Update**.
   c. Click **Apply**.
2. In the Embedded Web Server, click **Login/Permissions/Accounting > Login Methods**.
3. For Card Reader Setup, click **Edit**.
4. In the Update Firmware area, for Choose File, click **Browse**, then locate the firmware update `.dlm` file that you want to install.
5. Select the update file, then click **Open**. The device validates the file. If validation succeeds, the file name appears in the Choose File text field.
6. If validation fails, an error window appears. Error messages include the following:
   - `The submitted file is not related to the Card Reader`: This message occurs when the chosen file is not a valid file for updating the card reader.
   - `The submitted file is not approved by Xerox for firmware updates`: This message occurs when the chosen file is not a Xerox-approved file.

   Close the error window, then verify the file name.

7. To submit the update file to the card reader, click **Update**.

   Note:

   - A Card Reader Firmware Update in Progress window appears while the update processes. An update takes approximately 20 seconds.
   - You cannot use the card reader while an update is in progress. If you swipe a card during an update, the device ignores the card and the update continues.

8. If the update fails, an error window displays the message: `A system error has occurred. Card Reader firmware was not updated. Please try again.`

   Close the error window, then retry the update.

9. If the update succeeds, the status area displays the latest firmware version with a system time stamp.
10. Click **Close**.

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.
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.

Test Drive

The Test Drive option allows you to try out new features and provide feedback to Xerox. The feedback helps Xerox to make improvements in the software for future releases.

Note: Although Test Drive features are complete, it is possible that they are not fully optimized. If you experience an issue or have feedback, contact Xerox at TestDrive@xerox.com.

You can access Test Drive features from the Properties tab in the Embedded Web Server, and from the Device app at the control panel.

ENABLING TEST DRIVE FEATURES IN THE EMBEDDED WEB SERVER

To enable Test Drive features in the Embedded Web Server:

1. In the Embedded Web Server, click **Properties > General Setup > Test Drive**.
2. To enable a test drive feature, click the check box next to the feature, then click **Save**.

ACCESSING TEST DRIVE FEATURES AT THE CONTROL PANEL

Before you begin, ensure that any required Test Drive features are enabled in the Embedded Web Server.

To access a Test Drive feature at the device control panel:

1. At the control panel, press the **Home** button, then touch **Device**.
2. Scroll down the screen, then select the feature.

Note: The name of a test drive feature is suffixed by (Test Drive).

WEB-BASED CONFIGURATION USING THE CONTROL PANEL

Web-Based Configuration (using the Control Panel) is the first of the Test Drive features.

Your device has many configuration options, most of which are accessible from the Embedded Web Server only. Previously, to update configuration options, a Xerox representative or user was required to connect to the Embedded Web Server using a computer or mobile device. The Web-Based Configuration function provides access to the Embedded Web Server directly from the device control panel.

The Embedded Web Server pages are adjusted for the touch screen display. It is possible to configure every relevant option available in the Embedded Web Server from the control panel. Features that are inappropriate to configure from the touch screen, or options that link to websites, are disabled.

Note: To perform administrator functions, log in using administrator credentials, as in the Embedded Web Server.

1. At the control panel, press the **Home** button, then touch **Device**.
2. Scroll down the screen, then touch **Web-Based Configuration (Test Drive)**. The web-based configuration pages appear.

Note: If the Web-Based Configuration feature is not available, check that the feature is enabled in the Embedded Web Server. For details, refer to Enabling Test Drive Features in the Embedded Web Server.

3. Configure the settings required. If administrator login details are required, touch **Log In**, then enter the administrator login credentials. Click **Done**.
4. To exit the web-based configuration pages, touch **Exit** or press the **Home** button.

Configuring Lockdown Security Solution

The Lockdown Security Solution provides the facility to lock down a fixed set of security settings on your device. When you install this feature, the device settings are locked down permanently, and no user or administrator can unlock the settings.

Installation of the Lockdown Security Solution requires a feature installation key. For details, refer to Installing Optional Software Features.

Caution: After you install the Lockdown Security Solution, you cannot remove this feature.

When the Lockdown Security Solution is installed, the device monitors the locked-down settings daily. If a setting needs correction, the device remediates the setting to its required value. After the daily check, the device reports on the status of the locked-down settings. The device reports on the following situations:

- If all locked-down settings are compliant, the device generates a confirmation report.
- If a locked-down setting is not compliant, the device generates a lockdown error report.
- When a remediation is successful, the device generates a remediation confirmation report.
- When a remediation fails, the device generates a remediation error report.

Use the Lockdown & Remediate page to schedule daily checks and to configure settings for alerts and status reports.

To configure Lockdown & Remediation:

1. In the Embedded Web Server, click **Properties > Security > Lockdown and Remediate**.
2. For Check Daily at:, type the time of day in hours and minutes, then select **AM** or **PM**. The default daily time is 2:00 AM.

   If a setting needs remediation, the device sends an email alert to the contacts configured on the Email Alerts page.

   If the check is successful, the device generates status reports according to the report settings.

   Note:

   - After a check action begins, you cannot cancel the operation.
   - If remediations are needed, the process takes approximately 20 minutes.
   - Corrections to certain security settings take the device offline.
   - Corrections to certain security settings require a device restart.
3. To generate an email alert when a setting needs remediation, click the **Email Alerts** link. For details, refer to Email Alerts.
4. To invoke a manual check, click **Check Now**. At the confirmation prompt, click **Check Now** or **Cancel**. After the check action begins, the **Check Now** option remains grayed out until the check completes. After the check completes, the device generates status reports according to the report settings.

5. To print a status report after the daily check, for Printed Confirmation Report, select an option.
   - **Errors Only**: This option instructs the device to print a status report only when a non-compliant setting is detected. This option is the default.
   - **Always**: This option instructs the device to print a status report after every check.
   - **Never**: This option instructs the device not to print status reports.
6. To email a status report after the daily check, for Email Confirmation Report, select an option.
   - **Errors Only**: This option instructs the device to email a status report only when a non-compliant setting is detected. This option is the default.
   - **Always**: This option instructs the device to email a status report after every check.
   - **Never**: This option instructs the device not to email status reports.

   To send reports by email, ensure that recipients are configured for email alerts. For details, refer to Email Alerts.
7. To specify the text to appear on error reports, for Action Text, click **Edit**. In the text field, type up to 255 characters.
   The action text appears on the lockdown error and remediation error reports.
8. To generate a simulation test, click the check box for **Error Simulation**. The simulation verifies that the device can recognize insecure conditions, and generates test reports.
9. To save settings, click **Apply**. To cancel changes, click **Undo**.

Note: If you selected **Error Simulation**, the simulation test starts at the scheduled daily time.

Configuration Watchdog

Configuration Watchdog is a security feature that allows administrators to ensure that their devices stay in the appropriate configuration throughout day-to-day operations, without the need for external device monitoring.

Note: To restrict access to Configuration Watchdog, create a custom restricted-administrator role. When access is restricted, all options are grayed out and the following message appears: `Current device policy prevents configuration of this feature.`

Configuration Watchdog monitors feature settings to ensure that values remain compliant. When a watched setting changes, Configuration Watchdog detects the change on the next manual or scheduled check. After a change is detected, Configuration Watchdog remediates the feature to the required settings.

If remediation fails, a notification appears on the Configuration Watchdog page in the Embedded Web Server. If email notification is enabled, the device sends an alert to the contacts configured on the Email Alerts page.

Note: Certain features are monitored only, and are not remediated. For example, features that store credentials as part of the configuration of the feature.

CONFIGURATION WATCHDOG STATUS

The Configuration Watchdog area shows the status for the feature. The status information includes the watch status, a date time stamp, and the email notification setting.

When watching is not enabled, no features are being monitored. The watch status shows `Not Watching`. No other status information is displayed.

When watching is enabled, or the Watch List is changed, the status area shows the following information:

- A watch status of `Watching Enabled`: This status occurs when at least one feature is being monitored but no check has been made.
- One of the following Watchdog check settings:
  - `Next Check: <System Date Time Stamp>`: This setting shows when the next Watchdog check is scheduled. To change this setting, select the **Check Frequency** option.
  - `Auto-check is not on, use 'Check Now'`: This setting shows when the check frequency is configured to Manual Only. To run a manual check, click **Check Now**.
- The email notification setting: To enable or disable this setting, select the **Email Notification** option.

After a manual or scheduled Watchdog check, the status area shows the following information:

- One of the following watch statuses:
  - `No Changes Detected`: The monitored settings for the features have not changed since the last check.
  - `Changes Detected and Remediated`: The monitored settings for the feature changed since the last check and were returned to the expected settings.
  - `Changes Detected and Remediation Failed`: The monitored settings for the feature changed since the last check, but did not return to the expected settings.
  - `Changes Detected, Some Failed to Remediate`: The monitored settings for the feature changed since the last check, but did not all return to the expected settings.
- The date and time of the check: `Last Check: <System Date Time Stamp>`.

To view details about remediation, click **Review Changes**. The Review Changes window lists the items that required remediation after the check. The list shows the remediation status for each item. Remediation failures appear at the top of the list.

Note:

- The **Review Changes** option is available only when one or more changes are detected and remediated.
- The Review Changes list displays results from the most recent check only.

CONFIGURING SETTINGS FOR FEATURES TO BE MONITORED

Before you begin, to prevent unintentional remediation and possible device restart, ensure that each item to be monitored is configured as required.

To verify or edit configuration settings for features that you want to monitor:

1. In the Embedded Web Server, click **Properties > Configuration Watchdog**.
2. In the Watch List area, click **Feature List**.
3. Click the link to the feature that you need to configure. A message states that you are being redirected to the feature settings page. Click **OK**.

Note: If you proceed to a feature page, any unsaved changes to Watch Status settings are not preserved.

4. Verify the settings and make adjustments, as needed, then click **Apply**.
5. To return to Configuration Watchdog, in the navigation pane to the left, click **Configuration Watchdog**.

Note: Alternatively, you can configure feature settings using the Tools menu at the device control panel.

SELECTING FEATURES TO MONITOR

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

2. To select features to monitor, in the Watch List area, click **Feature List**:
   - To monitor individual features, for the feature, in the Watch Status column, select the Watch icon.
   - To stop monitoring individual features, for the feature, in the Watch Status column, deselect the Watch icon. The Not Watched icon shows a strike-through line.
   - To monitor all or none of the features, click the **Watch All** or **Watch None** toggle button.
   - To filter the watch list features, from the Watch Status menu, select **Entire List**, **Watched**, or **Not Watched**. The corresponding Watch or Not Watched icons are shown.
   - To sort the watch list alphabetically by feature, click **Feature**. To sort the list in reverse order, click **Feature** again.
   - To sort the watch list alphabetically by category, click **Category**. To sort the list in reverse order, click **Category** again.

   Note: When Lockdown Security Solution software is installed using a feature installation key, some features become locked. Locked features are unavailable for selection in the Configuration Watchdog feature. Locked features are managed through Lockdown Security Solution software, and locked features are no longer monitored by Configuration Watchdog. Locked features are indicated by a padlock icon in the watch list.
3. To save Watch Status changes, click **Save**. The Watch List area shows the status for the feature:
   - `Click to Begin Watching`: No Watchdog features are being monitored.
   - `Watching — Custom List`: Some Watchdog features are being monitored.
   - `Watching — Entire List`: All Watchdog features are being monitored.

SETTING THE CHECK FREQUENCY

To specify how often Configuration Watchdog monitors the selected features, do the following:

1. In the Embedded Web Server, click **Properties > Configuration Watchdog**.
2. In the Actions area, click **Check Frequency**.
   - To monitor features manually using the Check Now option, from the Frequency menu, select **Manual Only**.
   - To monitor features hourly, from the Frequency menu, select **Hourly**. The Occurrence area shows that the features are monitored at the beginning of each hour.
   - To monitor features daily, from the Frequency menu, select **Daily**. Select a time in hours and minutes. The Occurrence area shows that the features are monitored daily at the specified time.
   - To monitor features weekly, from the Frequency menu, select **Weekly**. Select the day required, then select a time in hours and minutes. The Occurrence area shows that the features are monitored on the specified day at the specified time.
3. To save Check Frequency changes, click **Save**.

4. To run a check at any time, click **Check Now**.

Note:

- If no features are being monitored, the **Check Now** option is disabled.
- For certain features, where configuration changes are detected, remediation requires a restart of the device.

EMAIL NOTIFICATION

To view or select email group notification settings:

Note: On the Email Alerts page, in the Recipient Group Preferences area, the Configuration Watchdog settings determine the enablement of email notification.

- If at least one check box is selected for Configuration Watchdog, email notification is enabled.
- If no check boxes are selected for Configuration Watchdog, email notification is disabled.

1. In the Embedded Web Server, click **Properties > Configuration Watchdog**.
2. In the Actions area, click **Email Notification**. This link navigates to the Email Alerts page. Configure the notifications required, then click **Apply**.
   For details, refer to Email Alerts.

Customization and Expansion

This chapter contains:

Xerox Extensible Interface Platform® (EIP) 422
Auxiliary Interface Kit 427
Driver Download Link 428
Customizing the Home Screen in the Embedded Web Server 429
Customizing the Home Screen at the Control Panel 431
1-Touch Apps 435
Adaptive Learning 438
Setting Defaults and Policies for Scan Services 441
Creating a Custom Scan App 443
Weblet Management 446
Managing Diagnostics and Usage Information 452
Editing Support Settings 453

Xerox Extensible Interface Platform® (EIP)

The Xerox Extensible Interface Platform® allows independent software vendors and partners to develop personalized and customized document management solutions. EIP is a software platform that allows you to install customized applications on your device, and access the applications directly from the control panel. These applications can leverage existing printer infrastructure and databases.

For more information on Xerox Extensible Interface Platform® applications for your printer, contact your Xerox representative, or refer to Xerox Office Products and Solutions - Xerox on the Xerox website.

You can configure Xerox Extensible Interface Platform® services from the Properties tab in the Embedded Web Server.

- To enable and configure Extensible Services, refer to Configuring Extensible Services.
- To verify connectivity settings, and to enable or disable the EIP Remote Web Inspector, refer to Diagnostics.
- To configure EIP settings for scan applications, refer to Extensible Service Scan Settings.
- To test individual EIP applications, refer to Accessing Extensible Services Setup for Apps.
- To review memory allocation and usage for the EIP browser, refer to Extensible Service Advanced Setup.

CONFIGURING EXTENSIBLE SERVICES

To configure extensible services:

1. In the Embedded Web Server, click **Properties > General Setup**.
2. Click **Extensible Service Setup > Settings**.
3. To enable Extensible Service Registration and other services, for Extensible Service Registration, click **Edit**.
   a. On the HTTP Web Services page, ensure that the following services are enabled:
      - Extensible Service Registration Web service
      - Web services that are required by the solutions that you are installing

      For more information, refer to HTTP Web Services.
   b. To return to the Extensible Service Setup page, click **Cancel** or **Save**.
4. If your EIP app requires a user password, in the Enable Extensible Services area, select **Export password to Extensible Services**.

5. In the Browser Settings area, configure the settings.
   - To enable the browser, select the check box for **Enable the Extensible Services Browser**.
   - To verify the certificates that are received from the remote server, select the check box for **Verify server certificates**.
   - To display the control panel keypad within EIP apps, select **Show based on individual app setting**.
   - The Extensible Services Browser supports secure connections (TLS). The digital certificates used for these secure connections are contained on the device within its certificate pool. For more information on digital certificates, navigate to **Properties > Security > Certificates > Security Certificates**.

     Browser Client Certificate Login allows prioritization of the Smart Card Certificate Pool for browser client login. For more details, refer to Acquire a Feature Installation Key.
   - To hide the control panel keypad within EIP apps, select **Hide within all apps**.

   Note: The control panel keypad mimics the buttons that were included on previous Xerox devices. The keypad includes numbers 0–9, #, *, clear, Reset, Access, for logging in, Start, and Stop.
6. In the Browser/Widget Versions area, the details of **Third Generation Browser** and **Widget Versions** are displayed.
7. In the EIP Advanced Setting area, enter the number of times that EIP apps are allowed to load before the EIP browser restarts. This setting determines when the embedded browser performs a hard reset.

   Note: The Number of EIP application loads before restart setting does not need adjustment typically, unless otherwise directed by Xerox.
8. In the Proxy Server area, configure the settings as needed.
   - To use a proxy server, from the list, select **Proxy**.
   - To configure HTTP proxy server settings, in the HTTP area, click **Edit**.
   - To use the same proxy server for HTTPS, select the check box for **Use settings for all protocols**.
   - To use a separate proxy server for EIP apps that use HTTPS, in the HTTPS area, configure the HTTPS proxy server settings.
   - In the Bypass Proxy Rules area, type the required values. Separate the required values with commas.

   Note: The Bypass Proxy Rules do not apply to the following features:
   - Remote Services: For details, refer to Remote Services.
   - HTTP(S) File Destinations: For details, refer to Configuring File Repository Settings for HTTP/HTTPS.
   - HTTP(S) Template Pool: For details, refer to Configuring Workflow Pool Repository Settings.
9. In the Cross Origin Resource Sharing (CORS) area, configure the settings as needed. Typically, EIP app developers use these settings. For more information, refer to the EIP Software Developers Kit.
   - To allow resource sharing across domains, select the check box for **Enable Cross Origin Resource Sharing (CORS) Validation**.

   Note: When Cross Origin Resource Sharing is disabled, you can still enter trusted domains.
   - To add trusted domains, in the Trusted domains area, type the domain information. Separate multiple domains with commas. The maximum number of characters allowed is 1024.

10. 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. You can use this page to verify device connectivity settings, and to enable or disable the EIP Remote Web Inspector feature.

Connectivity settings directly impact EIP apps. Improper settings can impair functionality for these applications.

The following settings impact EIP apps:

- Proxy: These settings allow the device to reach external networks.
- DNS: These settings allow the device to convert DNS names or Fully Qualified Domain Names (FQDN) into IP addresses.
- IP Address: 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**.

To use the EIP Remote Web Inspector feature, refer to Xerox Extensible Interface Platform® Software Development Kit (SDK) at Xerox Developer Program.

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 URLs

To test a URL:

1. To test connectivity to a URL, enter the URL path that you want to test.
2. Click **Test**. The results for the tested URL appear on 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. For more information, refer to Memory Usage.

To configure memory allocation for the EIP browser:

1. In the Embedded Web Server, click **Properties > General Setup**.
2. Click **Extensible Service Setup > Memory Usage**.
3. To update the memory allocation and usage information, in the Third Generation EIP Browser area, click **Refresh**.
4. To change the EIP browser memory allocation, in the Memory Allocation Setup area, select a usage option.
5. Click **Apply**.

Memory Usage

This 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.

There are separate memory allocations for EIP Applications used for job related services in Job Services Apps area and EIP Applications used for authentication in Authentication Apps area:

- To update the memory allocation and usage information, click **Refresh**.
- To change the EIP Browser memory allocation, for Memory Allocation Setup, select an option. Click **Apply**.

The unique setting of Retain App Authentication in Memory within the Authentication Apps section may be used to

allow the authentication process to begin more quickly, if required.

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 disable or enable apps, and change the display order of apps on the control panel home 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.

APP ENABLEMENT

Use the App Enablement page in the Embedded Web Server to enable or disable the apps that appear on the control panel home screen.

Availability: Determines whether an app is available for use on the local user interface.

Visibility: Visibility determines whether an app is visible to users on the home screen. Visibility can be changed, regardless of availability state, or whether app is active or inactive.

To make an app available for customization and personalization at the control panel, enable the app.

When an app is disabled, it is not available for use at the control panel, and the administrator cannot apply permissions to the app.

Standard apps are installed and enabled or available on the device by default. When an app is disabled, it is not available for use at the local user interface, and the administrator cannot apply permissions to the app. When a standard app is disabled or unavailable, any 1-Touch Apps based on the app are disabled or unavailable. If the standard app is re-enabled, the 1-Touch Apps are not enabled automatically, and it is necessary to enable them individually. For example, if the Email app is disabled, any 1-Touch Apps that use Email are also disabled. If the Email app is re-enabled, each 1-Touch Apps that uses the Email app remains disabled until you enable the app individually.

Note: It is not possible to disable the Jobs and Device apps, and apps that are set as entry-screen defaults.

To enable or disable apps:

1. In the Embedded Web Server, click **Properties > Apps > App Enablement**.
2. To enable or disable an app, select the check box for the app. A check mark indicates that the app is enabled.
3. Click **Apply**.
4. Verify if the available apps appear on the device home screen.
5. If they do not appear on the device home screen, check the visibility of the app.
   To enable the visibility of the apps, perform the following:

   Note: Visibility can be changed, regardless of availability state, or whether app is active or inactive.

   a. On the App Enablement page, click the **Visible** icon under the Visibility column.

      The Visible icon indicates if the selected apps are visible or not on the local user interface.

   b. Click **Apply**.

   c. Verify if the apps are visible on the device home screen.

6. For an app to appear at the local user interface, the app must be available and visible. If an enabled app does not appear on the control panel home screen, perform the following additional steps:
   a. At the control panel, log in as an administrator.
   b. At the bottom of the Home screen, touch **Customize**.
   c. Touch **Customize Home**.
   d. To apply the setting to non-logged-in users, at the prompt, touch **Guest**.
   e. If the app does not appear on the Customize Home screen, at the top of the screen, touch the **Plus** (**+**) icon. All enabled apps that do not already show on the Home screen appear.
   f. Touch the app that you want to show on the Home screen.
   g. Touch **Done**.

SETTING THE DISPLAY ORDER FOR APPS

You can arrange the order in which apps appear on the control panel home screen.

1. In the Embedded Web Server, click **Properties > Apps > Order**.
2. Select, drag, then drop the apps on the screen until the apps are in the preferred order.
3. Click **Apply**.

Customizing the Home Screen at the Control Panel

Use the Customization feature to configure Home screen settings for all users.

Customization allows you to configure the following settings:

- Hide, show, and rearrange apps on the Home screen
- Hide or show app features
- Configure and save the default settings for an app
- Create 1-Touch Apps

Note: Customization settings apply to non-logged-in or Guest users. Personalization settings configured by logged-in users override any corresponding customization settings.

SETTING THE DEFAULT WALK-UP SCREEN AT THE CONTROL PANEL

The walk-up screen is the initial screen that appears to a walk-up of guest user.

To set the default walk-up screen at the control panel, do the following:

1. At the control panel, press the **Home** button.
2. Scroll to the bottom of the Home screen, then touch **Customize**.
3. Touch **Entry Screen Defaults**.
4. To apply the setting for a walk-up or guest user, at the prompt, touch **Guest**.
5. In the Device Default App area, select **Home** or any app from the list.
6. Click **OK**.
7. Click **OK** again to save the change.

SETTING THE DEFAULT SCREEN WHEN ORIGINALS ARE DETECTED AT THE CONTROL PANEL

This feature sets the default app to launch when original documents are loaded in the automatic document feeder.

To set the default screen when original documents are detected at the control panel, do the following:

1. At the control panel, press the **Home** button.
2. Scroll to the bottom of the Home screen, then touch **Customize**.
3. Touch **Entry Screen Defaults**.
4. To apply the setting for a walk-up or guest user, at the prompt, touch **Guest**.
5. In the Originals Detected area, select an app from the list. To take no action, select **No Action**.
6. Click **OK**.
7. To save the change, click **OK** again.

REARRANGING APPS ON THE HOME SCREEN

To rearrange apps on the Home screen:

1. At the control panel, press the **Home** button.
2. Scroll to the bottom of the Home screen, then touch **Customize**.
3. Touch **Customize Home**.
4. To apply the setting to non-logged-in users, at the prompt, touch **Guest**.
5. Touch and hold the required app, then drag the app to the new location. Release the app. Repeat the process for each app that you want to rearrange.
6. Touch **Done**.
7. Verify that the apps appear in the preferred locations on the Home screen.

DISPLAYING OR HIDING AN APP ON THE HOME SCREEN

To change the display of apps on the Home screen:

1. At the control panel, press the **Home** button.
2. Scroll to the bottom of the Home screen, then touch **Customize**.
3. Touch **Customize Home**.
4. To apply the setting to non-logged-in users, at the prompt, touch **Guest**.
5. To display an installed, but hidden app:
   a. Touch the **Plus** (**+**) icon.
   b. Touch the app that you want to appear on the control panel.
   c. Touch **Done**.
6. To hide an installed app:
   a. For the required app, touch **X**.
   b. At the prompt, touch **Hide**.
   c. Touch **Done**.
7. Verify that only the required apps appear on the Home screen.

DELETING AN APP FROM THE HOME SCREEN

Note: Deletion is permanent. You cannot restore a deleted app.

To delete an app from the Home screen:

1. At the control panel, press the **Home** button.
2. Scroll to the bottom of the Home screen, then touch **Customize**.
3. Touch **Customize Home**.
4. To apply the setting to non-logged-in users, at the prompt, touch **Guest**.
5. To delete an installed app:
   a. For the required app, touch **X**.

b. At the prompt, touch **Delete**.

c. Touch **Done**.

6. Verify that only the required apps appear on the Home screen.

CUSTOMIZING APP FEATURES

To customize the feature list for an app:

1. At the control panel, press the **Home** button.
2. Touch the app required.
3. Scroll to the bottom of the feature list, then touch **Customize**.
4. Touch **Customize Feature List**.
5. To apply the setting to non-logged-in users, at the prompt, touch **Guest**.
6. Touch the needed 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.

Note: If a policy-based feature is enabled, the feature appears at the bottom of the Feature List. You can customize the feature to be hidden or shown. If a policy-based feature is not enabled, the feature does not appear in the Feature List, and you cannot customize the feature.

Encryption is an example of a policy-based feature for the Email App.

7. To reorder the menu features, touch and drag the features into the appropriate order.
8. To save the current configuration, touch **Done**.

CUSTOMIZING APP DEFAULT SETTINGS

To customize the default settings for an app:

1. At the control panel, press the **Home** button.
2. Touch the app required.
3. Configure the required default settings.
4. Touch **Customize**, then touch **Save Settings as Default**.
5. To save the default settings for non-logged-in users, at the prompt, touch **Guest**.

The new settings override the previous default settings.

REMOVING APP CUSTOMIZATION SETTINGS

To remove the current customization settings for an app:

1. At the control panel, press the **Home** button.

2. Touch the app required.
3. Scroll to the bottom of the feature list, then touch **Customize**.
4. Touch **Remove App Customizations**.
5. To remove the app customization for non-logged-in users, at the prompt, touch **Guest**.

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

Administrators and users with certain privileges can create individual 1-Touch Apps that allow completion of frequent jobs or tasks.

The following types of 1-Touch Apps are available:

- Public 1-Touch Apps: Refer to Public 1-Touch Apps.
- Private 1-Touch Apps: Refer to Private 1-Touch Apps.

After you create a 1-Touch App, the app appears on the printer Home screen.

- 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.

PUBLIC 1-TOUCH APPS

System administrators and users with customization privileges can create public 1-Touch Apps, which are available for all device users.

When you create a public 1-Touch App, you can configure the app to allow users to make temporary changes to the app feature settings. When the app is reset, any temporary changes are discarded. You can configure the app to prevent users from viewing or changing the app feature settings.

After you create a public 1-Touch App, the app appears on the device Home screen.

Device administrators and users with customization privileges can save an existing public 1-Touch App as a new public 1-Touch App, then adjust the appearance and default settings for the new app as needed.

If Personalization is enabled, all logged-in users can save a public 1-Touch App as a new private 1-Touch App, then adjust the appearance and default settings for the new app as needed.

Note: For details on Personalization, refer to Personalization.

PRIVATE 1-TOUCH APPS

If Personalization is enabled, all logged-in users can create private 1-Touch Apps. Private 1-Touch Apps are available only for the user that created the app, and appear on the Home screen for the logged-in user only.

After you create a private 1-Touch App, you can save the app as a new private 1-Touch App. You can adjust the appearance and default settings for the new app as needed.

Note: All private 1-touch Apps allow for temporary changes. When the app is reset, any temporary changes are discarded.

Note: For details on Personalization, refer to Personalization.

CREATING A 1-TOUCH APP

To create a 1-Touch App:

1. At the control panel, press the **Home** button.
2. Touch the app required.
3. To configure the 1-Touch App, select the job settings.
4. Scroll to the bottom of the feature list, then touch **Create 1-Touch App**.
5. Do one of the following:
   - To create a 1-Touch App for all users, at the prompt, touch **Guest**.
   - To create a private 1-Touch App, at the prompt, touch **You**.
6. Touch the **Enter 1-Touch App Name** entry field, then use the alphanumeric keypad to enter a name. Touch **Next**.
7. Do one of the follwing:
   - To create the 1-Touch App with the default customization settings, touch **Create 1-Touch App**. The system saves the app, and the app appears on the printer Home screen.
   - To modify the customization settings, touch **Customize Appearance**.
8. If you selected **Customize Appearance**, do the following:
   a. Touch a color scheme option for your 1-Touch App, then touch **Next**.
   b. Touch an icon that best suits the 1-Touch App that you are creating, then touch **Next**.
   c. To provide instructions that appear at the top of the app screen, touch the **Enter App Instructions** entry field, then use the alphanumeric keypad to enter instructions for users.
   d. Do one of the following:
      - If you created a private 1-Touch App, touch **Done**. The system saves the app, and the app appears on the printer Home screen.
      - If you created a public 1-Touch App, touch **Next**.

e. Do one of the following:

- To allow other users to make temporary changes to the app settings, enable the **Allow Editing** option. If you enable the **Allow Editing** option, all users can make temporary changes to the 1-Touch App settings. If Personalization is enabled, logged-in users can also save the changes as a new 1-Touch App.
- To prevent other users from viewing or editing the 1-Touch App settings, disable the **Allow Editing** option, then touch the app settings required:
  - **Allow Editing Quantity**: This option allows users to view and update the print quantity. This option appears only if the parent app supports print quantity. For example, the Copy App.
  - **Show Destinations**: This option allows users to view the recipient list. This option appears only if the parent app supports destinations. For example, the Email App.
  - **Show Feature Settings**: This option displays the feature settings that are configured for the 1-Touch App.

Note: For 1-Touch Apps that you create, you can always edit the app settings. If you disable the **Allow Editing** option, you can still edit the app settings.

f. Touch **Done**.

The 1-Touch App appears on the Home screen.

Adaptive Learning

Adaptive Learning feature reacts to everyday usage of the device to help streamline tasks for users and administrators. The Adaptive Learning feature aggregates usage data for individual logged-in users and walk-up users. The feature then uses that data to provide workflow suggestions for individual users and to customize some default settings for the device.

Use the Adaptive Learning feature to manage Adaptive Learning policies for the device.

Adaptive Learning provides the following features:

- Suggest Personalized App Workflows: This feature provides personalized workflow suggestions for a logged-in user based on their use of certain applications. An individual user can choose the types of suggestions that they receive. Individual users can enable and disable their personalized suggestion options at the device control panel.

  The Suggest Personalized App Workflows feature is available only when the Personalization feature is enabled. Personalized suggestions apply to the Copy, Email, and Scan To Apps only.

- Automatically Set Device Defaults: This feature provides customization of default settings based on device usage by walk-up users. Options include the default walk-up screen, the default screen when original documents are detected, and default settings for the Email and Scan To Apps.

The Adaptive Learning area shows the enablement status of Adaptive Learning. The status messages are as follows:

- `Adaptive Learning Active`: This status appears in one or both of the following scenarios:
  - Adaptive Learning personalization is enabled.
  - Adaptive Learning for device defaults is enabled for at least one option.
- `Adaptive Learning is Active; Not Fully Configured`: This status appears when Adaptive Learning personalization is enabled and Personalization is disabled.

  Note: Adaptive Learning Suggest Personalized App Workflows and Personalization are separate features.

- `Adaptive Learning Not Active`: This status appears when Adaptive Learning personalization is disabled and Adaptive Learning for device defaults is disabled.

  Note: Suggest Personalized App Workflows and Automatically Set Device Defaults are separate features.

SUGGEST PERSONALIZED APP WORKFLOWS

Adaptive Learning personalization offers workflow-automation suggestions to help logged-in users streamline their workflow. Personalized app workflow suggestions include the following:

- Creation of personalized 1-Touch Apps for repetitive tasks
- Creation of personalized 1-Touch Apps for complex tasks
- Reordering of app feature settings according to frequency of use
- Language preference settings

Note: The Adaptive Learning personalization feature is available to logged-in users only.

To enable Adaptive Learning personalization, do the following:

1. In the Embedded Web Server, click **Properties > Adaptive Learning**.
2. In the Manage area, for Suggest Personalized App Workflows, click **Configure**.
3. In the Suggest Personalized App Workflows window, click the toggle button for **Make Personalized Suggestions for Logged-In Users**.
4. Click **Save**.

   The Adaptive Learning area shows the enablement status of Adaptive Learning.
5. If the status shows that Adaptive Learning is not fully configured, enable Personalization. Click the **Turn on Personalization** link. For details, refer to Personalization.

Note:

- Adaptive Learning personalization is enabled by default.
- When Adaptive Learning personalization is enabled, all personalization suggestion options for logged-in users are enabled by default.
- When Adaptive Learning personalization is enabled, logged-in users can manage their personalization suggestions at the control panel.
- When Adaptive Learning personalization is disabled, individual personalization suggestions are not available to logged-in users, regardless of their enablement status.

AUTOMATICALLY SET DEVICE DEFAULTS

Adaptive Learning for device defaults offers adaptation of feature defaults to optimize device settings. Adaptive Learning analyzes the usage of features by guest users to determine commonly used settings. The device gathers data on the most frequently used apps and information on the job settings configured in the Email and Scan To Apps.

When Adaptive Learning for device defaults is enabled, settings can change automatically from the defaults that an administrator specifies. An administrator can view the history of recent changes to device defaults made by Adaptive Learning.

Note: When Adaptive Learning makes changes to the device defaults, a notification banner appears. You can temporarily dismiss the banner, but it reappears at each session during the 8-day notification period to inform everyone using the device about the changes.

To enable Adaptive Learning policies for device defaults, do the following:

1. In the Embedded Web Server, click **Properties > Adaptive Learning**.
2. In the Adaptive Learning area, to view the changes of Adaptive Learning history, do the following:
   a. Click **View Automatic Update History**.
   b. A list of the latest updates appears, sorted by the most recent. The list shows up to 10 items and includes a time stamp for each item.
   c. Click **Close**.
3. In the Control Panel, click **Device > Notifications > Adaptive Learning Updates**.
4. To view or change the policies, perform the following:
   a. In the Manage area, for Automatically Set Device Defaults, click **Configure**.

b. To use Adaptive Learning to set the default app for walk-up users, click the toggle button for **Default Walkup Screen**. For details, refer to Entry Screen Defaults.

c. To use Adaptive Learning to set the default screen when original documents are detected, click the toggle button for **Default Screen When Originals Are Detected**. For details, refer to Entry Screen Defaults.

d. To use Adaptive Learning to set Email and Scan To App defaults, click the toggle button for **Email and Scan To App Defaults**. For details, refer to Configuring Default Email Settings and App Defaults. This policy applies to both Email and Scan To Apps.

Note:

- The policy for **Email and Scan To App Defaults** does not apply to the following settings:
  - Text-based fields, such as Subject, Message, and Attachment File Name.
  - Workflow items, such as **Auto Start When Originals are Detected**, **Build Job**, and **Preview** if applicable.
- The device can modify defaults for the Email App independently of defaults for the Scan To App. The converse applies also.

e. Click **Save**.

The Adaptive Learning area shows the enablement status of Adaptive Learning.

Note: When Adaptive Learning for device defaults is enabled for a feature, an alert appears on the defaults page on the Embedded Web Server and at the control panel. The alert states that Adaptive Learning is setting defaults and may overwrite any defaults that you set.

If you do not want Adaptive Learning to modify the defaults that you set, disable the Adaptive Learning policy for that feature.

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.

You can disable the multi-feed detection feature to prevent feed error messages at the device user interface when using the automatic document feeder. This feature is available only when the multi-feed detection sensor hardware is installed.

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. To allow the device to create a temporary lock file at the remote destination ,enable **Locking of Files**. This avoids conflicts, such as multiple devices creating a file with the same name. The device deletes the temporary lock file after the filing is complete.

Note: By default, Locking of Files is enabled.

Note: If a lock file is created and the device is unable to remove it due to some issue for example, network disruption, the lock file may remain at the remote location that needs to be cleaned up manually. Further filing to the same remote folder may fail until the lock file is removed manually at the remote location.

5. 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.

DISABLING MULTIFEED DETECTION

If the multifeed sensor is installed on your device, the multifeed detection feature is available. The feature is enabled by default. If a multifeed condition occurs, the device stops scanning and a message appears at the control panel. The message indicates a jam in the duplex automatic document feeder. The user can cancel the job or reload the original documents and continue the job with or without multifeed detection enabled for that job.

To disable the multifeed detection feature, do the following:

1. In the Embedded Web Server, click **Properties > Apps**.
2. Click **Scan Services > Defaults & Policies**.
3. For Document Feeder Multi-feed Detection, select **Disable**.
4. Click **Save**.

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 programs that you can install on your Xerox device to add functionality to the device. You can download Job Service weblets from the Xerox® App Gallery at appgallery.services.xerox.com. You can also download weblets at the device control panel using the Xerox® App Gallery app.

Note: For instructions on using the Xerox® App Gallery app, refer to the *User Guide* for your device.

An EIP weblet can be registered as a Job Service app or an Authentication app.

- A job service app provides a workflow for the execution of a specific task on the device. For example, a workflow using the print, scan, or copy service. Registered job service apps appear on the device Home screen.
- An authentication app provides an authentication method for user access to the device. If enabled, an authentication app is invoked when a user attempts to log in at the control panel.

Note: Only one EIP authentication app can be registered on the device at a time.

You can access Weblet Management from the Properties tab in the Embedded Web Server, and at the control panel, from the Tools menu.

- To enable weblet installation, refer to Enabling Weblet Installation in the Embedded Web Server or Enabling Weblet Installation at the Control Panel.
- To set the security policy for unencrypted weblets, refer to Setting the Security Policy for Unencrypted Weblets.
- To configure settings for the Extensible Services Browser, refer to Configuring Extensible Services.
- The Weblet Management page in the Embedded Web Server shows the weblets that are installed on the device. To install a weblet, refer to Installing a Weblet in the Embedded Web Server or Installing a Weblet at the Control Panel.

Note: When the EIP Remote Web Inspector is enabled, the Install Weblet function is not available.

- To configure weblet settings, refer to Configuring Weblet Settings.
- To configure settings for the Xerox® App Gallery, refer to Configuring Xerox® App Gallery Settings.

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**.

ENABLING WEBLET INSTALLATION IN THE EMBEDDED WEB SERVER

1. In the Embedded Web Server, click **Properties > Apps > Custom Apps > Weblet Management**.
2. Click **Security Installation Policy**.
3. In the Weblet area, select **Allow Weblet Installation**.
4. Click **Apply**.

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**.

INSTALLING A WEBLET IN THE EMBEDDED WEB SERVER

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**.

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.

TROUBLESHOOTING A WEBLET INSTALLATION

A weblet installation can fail for one of the following reasons.

- A problem with the weblet itself. For example:
  - The weblet contains invalid contents or formatting.
  - The weblet has invalid encryption settings.
  - The weblet contains an invalid or expired security certificate.

To remediate the problem, contact the weblet or app provider with detailed information about the error. Obtain an updated weblet from the provider.

- A device issue that prevents weblet installation. For example:
  - The device has exceeded its storage capacity.
  - The maximum number of apps that the device supports is reached. The limit is 64 apps.

  To address the issue, remove any unused apps or weblets.
- A device policy conflict that prevents weblet installation. For example:
  - The device has a restricted weblet installation policy.
  - A weblet encryption mismatch. If the device policy allows the installation of encrypted weblets only, and the weblet is not encrypted, a mismatch can occur.
  - A mismatch with the Extensible Services policy for displaying the control keypad within EIP apps. If the device policy for the control keypad is set to **Hide within all apps**, and the weblet requires the control keypad, a mismatch can occur.
  - A security conflict due to invalid security certificates. If the device is FIPS 140 enabled, but the weblet contains non-FIPS 140 compliant certificates, a security conflict occurs.
  - A security conflict due to invalid certificate key-lengths. If the key lengths of certificates within the weblet do not meet the minimum key-length requirements for the device, a security conflict occurs.

  To resolve the conflict, review the following device policies:
  - Weblet installation policy in Weblet Settings.
  - Encrypted weblet installation policy in Weblet Settings.
  - Extensible Services policy for displaying the control keypad within EIP apps. Refer to Xerox Extensible Interface Platform® (EIP).
  - FIPS 140 enablement status. Refer to FIPS 140.
  - Certificate key-length requirements. Refer to Specifying the Minimum Certificate Key Length.

  Reconfigure the device as needed. Otherwise, contact the weblet or app provider with detailed information about the error. Obtain an updated weblet from the provider.

CONFIGURING WEBLET SETTINGS

1. In the Embedded Web Server, click **Properties > 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 Home screen, for Displayed on Touch Interface, click **Edit**. For details, refer to App Enablement.
4. To configure the weblet app as the default control panel entry screen, for Default Walk-Up Screen, click **Edit**. For details, refer to Entry Screen Defaults.
5. To configure user access to the weblet app, for User Permissions, click **Edit**. For details, refer to User Permissions.
6. Click **Close**.

CONFIGURING XEROX® APP GALLERY SETTINGS

You can download weblets from the Xerox Home Page or Xerox® App Gallery. For more information about the Apps and capabilities, go to Workplace Apps and Solutions section, and follow the web link to Workplace Apps - ConnectKey - Xerox. You can select the different Apps that are available for installation on the device.

To configure Xerox® App Gallery settings, perform the following steps:

1. In the Embedded Web Server, click **Properties > 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 Home screen:
   a. For Displayed on Touch Interface, click **Edit**.
   b. To display the Xerox® App Gallery icon, select the check box for **Xerox® App Gallery**. To hide the Xerox® App Gallery icon, clear the check box for **Xerox® App Gallery**.
   c. Click **Apply**.
4. To configure the Xerox® App Gallery as the default control panel entry screen:
   a. For Default Walk-Up Screen, click **Edit**.
   b. For Default Walkup Screen, from the list, select **Xerox® App Gallery**.
   c. Click **Save**.
5. To configure access to the Xerox® App Gallery for non-logged-in users:
   a. For User Permissions, click **Edit**.
   b. On the Non-Logged-In Users tab, in the Permission Role area, for Non-Logged-In User, click **Edit**.
   c. Select the **Apps & Tools** tab.
   d. For Xerox® App Gallery, select an option:
      - **Allowed**: This option permits Xerox® App Gallery usage.
      - **Not Allowed**: This option displays the Xerox® App Gallery icon at the control panel and restricts usage of the app.
      - **Not Allowed & Hidden**: This option restricts Xerox® App Gallery usage and does not display the icon for the app at the control panel.
6. Click **Apply**.

CONFIGURING XEROX® XMPIE APP

With the Xerox® Connect for XMPie App, you can have instant access to 50 or more templates. In one touch, you can create personalized content from your ConnectKey® Technology-enabled multifunction printers. For example, holiday cards, birthday cards, and calendars. Use the Xerox® Connect for XMPie App for free access to templates and the ability to personalize them for immediate printing.

The main screen displaysFeatured Products and Product Categories. You can browse the categories for the products that you wish to create. Follow the instructions on screen to create a job with customized fields. You can preview and print, as needed. To configure the Connect for XMPie App on your printer, do the following:

1. In the Embedded Web Server, click **Properties > Apps > Custom Apps > Weblet Management**.

2. In the Installed Weblets area, for Xerox® Connect for XMPie App, click **Edit**.

   The Connect for XMPie Setup page appears.

3. To hide or display the XMPie setup icon on the control panel Home screen:
   a. For Displayed on Touch Interface, click **Edit**.
   b. To display the XMPie setup icon, select the check box for **Connect for XMPie**. To hide the XMPie setup icon, clear the check box for **Connect for XMPie**.
   c. Click **Apply**.
4. To configure the Connect for XMPie as the default control panel entry screen for walk-up users:
   a. For Default WalkUp Screen, click **Edit**.
   b. For Default Walkup Screen, from the list, select **Connect for XMPie**.
   c. Click **Save**.
5. To configure access to the Connect for XMPie for non-logged-in users:
   a. For User Permissions, click **Edit**.

      The User Permission Roles page appears.

   b. On the Non-Logged-In Users tab, in the Permission Role area, for Non-Logged-In User, click **Edit**.
   c. Select the **Apps & Tools** tab.
   d. For Connect for XMPie, select an option:
      - **Allowed**: This option permits XMPie usage.
      - **Not Allowed**: This option displays the XMPie icon at the control panel and restricts usage of the app.
      - **Not Allowed & Hidden**: This option restricts XMPie usage and does not display the icon for the app at the control panel.
   e. Click **Apply**.
6. To return to the main menu, click **Close**.

CONFIGURING AN EIP AUTHENTICATION APP

An EIP authentication app is an EIP application that provides authentication for users to access the device. If an EIP authentication app is installed, the app is listed in the Embedded Web Server, in the Installed Weblets area of the Weblet Management page. For details, refer to Weblet Management.

To configure an EIP authentication app:

1. In the Embedded Web Server, click **Properties > Apps > Custom Apps > Weblet Management**.
2. For the EIP authentication app that you want to configure, click **Edit**.
3. To enable or disable EIP Authentication, click the toggle button for **Enable**.

4. For Notify Before System Timeout, select a timeout value from the drop-down menu.
   The timeout defines how long prior to the System Timeout the EIP Authentication App is displayed. This setting provides the user an opportunity to interact with the EIP Authentication App as part of the logout workflow.

   Note: If you select the option as **Off (No Notification)**, there will be no notice provided and system timeout occurs as schedule.

5. In the Secure Connection area, select security certificates.
   a. For Server Certificate Validation, from the All Trusted CA Certificates list, select a certificate. To view the content of a certificate, select the certificate, then click the information icon.
   b. For Device Certificate, select **Xerox Default Device Certificate** or **Any Matching Certificate** option from the list. To view the content of a certificate, select the certificate, then click the information icon.

   Note: **Any Matching Certificate** option allows the EIP authentication app to determine the certificate to use, based on all the appropriate certificates installed in the device certificate store.

   c. To install a certificate that is required, click **Missing Certificate**. If you select this option after you change authentication settings, an alert notifies you that the settings are not saved. To apply the changes, click **OK**.

      The **Missing Certificate** option provides a link to the Security Certificates page. For details, refer to Security Certificates.

6. In the Card Readers area, for **Use any connected card reader**, click the toggle button.
   - If this option is enabled, EIP authentication app will receive card data from any supported card reader currently plugged into the device.
   - If this option is disabled, then the System Administrator can select the specific card readers which are plugged into the device.
7. To save the settings, click **OK**.

If you need to learn more about EIP Authentication Applications, contact Xerox at Xerox.Global.Developer.Program@xerox.com.

DELETING A WEBLET

1. In the Embedded Web Server, click **Properties > Apps > Custom Apps > Weblet Management**.
2. In the Installed Weblets area, for the weblet name, click **Delete**.
3. Click **Close**.

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**.

Audit Log Event Identification Numbers

This appendix contains:

Audit Log Event Identification Numbers 456

Audit Log Event Identification Numbers

Note: Refer to the *Xerox® AltaLink® and VersaLink® Series Security Information and Event Management Reference Guide*.

Note: Not all events might be available in your device.

EVENT IDENTIFICATION NUMBER	DESCRIPTION
1	System Startup
2	System Shutdown
3	Standard Disk Overwrite Started
4	Standard Disk Overwrite Complete
5	Print Job
6	Network Scan Job
7	Server Fax Job
9	Email Job
10	Audit Log Disabled
11	Audit Log Enabled
12	Copy Job
13	Embedded Fax Job
14	LAN Fax Job
15	Data Encryption enabled
16	Full Disk Overwrite Started
17	Full Disk Overwrite Complete
18	Data Encryption disabled
20	Scan to Mailbox Job
21	Delete File/Dir
23	Scan to Home
24	Scan to Home Job
27	Postscript Passwords
29	Network User Login
30	SA Login
31	User Login

EVENT IDENTIFICATION NUMBER	DESCRIPTION
32	Service Login Diagnostics
33	Audit Log Download
34	Immediate Job Overwrite Enablement
35	SA PIN Changed
36	Audit Log File Saved
37	Force Traffic over Secure Connection (HTTPS)
38	Security Certificate
39	IPsec
40	SNMPv3
41	IP Filtering Rules
42	Network Authentication Configuration
43	Device Clock
44	Software Upgrade
45	Clone File Operations
46	Scan Metadata Validation
47	Xerox Secure Access Configuration
48	Service Login Copy Mode
49	Smartcard Login
50	Process Terminated
51	Scheduled Disk Overwrite Configuration
53	Saved Jobs Backup
54	Saved Jobs Restore
55	SA Tools Access Admin
57	Session Timer Logout
58	Session Timeout Interval Change
59	User Permissions
60	Device Clock NTP Configuration
61	Device Administrator Role Permission
62	Smartcard Configuration

EVENT IDENTIFICATION NUMBER	DESCRIPTION
63	IPv6 Configuration
64	802.1x Configuration
65	Abnormal System Termination
66	Local Authentication Enablement
67	Web User Interface Login Method
68	FIPS Mode Configuration
69	Xerox Secure Access Login
70	Print from USB Enablement
71	USB Port Enablement
72	Scan to USB Enablement
73	System Log Download
74	Scan to USB Job
75	Remote Control Panel Configuration
76	Remote Control Panel Session
77	Remote Scan Feature Enablement
78	Remote Scan Job Submitted
79	Remote Scan Job Completed
80	SMTP Connection Encryption
81	Email Domain Filtering Rule
82	Software Verification Test Started
83	Software Verification Test Complete
84	Trellix Security State*
85	Trellix Security Event*
87	Trellix Agent*
88	Digital Certificate Import Failure
89	Device User Account Management
90	Device User Account Password Change
91	Embedded Fax Job Secure Print Passcode
92	Scan to Mailbox Folder Password

EVENT IDENTIFICATION NUMBER	DESCRIPTION
93	Embedded Fax Mailbox Passcode
94	FTP/SFTP Filing Passive Mode
95	Embedded Fax Forwarding Rule
96	Allow Weblet Installation
97	Weblet Installation
98	Weblet Enablement
99	Network Connectivity Configuration
100	Address Book Permissions
101	Address Book Export
102	Software Upgrade Policy
103	Supplies Plan Activation
104	Plan Conversion
105	IPv4 Configuration
106	SA PIN Reset
107	Convenience Authentication Login
108	Convenience Authentication Configuration
109	Embedded Fax Passcode Length
110	Custom Authentication Login
111	Custom Authentication Configuration
112	Billing Impression Mode
114	Clone File Installation Policy
115	Save for Reprint Job
116	Web User Interface Access Permission
117	System Log Push to Xerox
120	Mopria Print Enablement
123	Near Field Communication (NFC) Enablement
124	Invalid Login Attempt Lockout
125	Secure Protocol Log Enablement
126	Display Device Information Configuration

EVENT IDENTIFICATION NUMBER	DESCRIPTION
127	Successful Login After Lockout Expired
128	Erase Customer Data
129	Audit Log SFTP Scheduled Configuration
130	Audit Log SFTP Transfer
131	Remote Software Download Policy
132	AirPrint & Mopria Scanning Configuration
133	AirPrint & Mopria Scan Job Submitted
134	AirPrint & Mopria Scan Job Completed
136	Remote Services NVM Write
137	FIK Install via Remote Services
138	Remote Services Data Push
139	Remote Services Enablement
140	Restore Backup Installation Policy
141	Backup File Downloaded
142	Backup File Restored
143	Google Cloud Print Services Configuration
144	User Permission Role Assignment
145	User Permission Role Configuration
146	Admin Password Reset Policy Configuration
147	Local User Account Password Policy
148	Restricted Administrator Login
149	Restricted Administrator Role Permission
150	Logout
151	IPP Configuration
152	HTTP Proxy Server Configuration
153	Remote Services Software Download
154	Restricted Administrator Permission Role Configuration
155	Weblet Installation Security Policy
156	Lockdown and Remediate Security Enablement

EVENT IDENTIFICATION NUMBER	DESCRIPTION
157	Lockdown Security Check Complete
158	Lockdown Remediation Complete
159	Send Engineering Logs on Data Push
160	Print Submission of Clone Files Policy
161	Network Troubleshooting Data Capture
162	Network Troubleshooting Data Download
163	DNS-SD Record Data Download
164	One-Touch App Management
165	SMB Browse Enablement
166	Standard Job Data Removal Started
167	Standard Job Data Removal Complete
168	Full Job Data Removal Started
169	Full Job Data Removal Complete
170	Scheduled Job Data Removal Configuration
171	Cross-Origin-Resource-Sharing (CORS)
172	One-Touch App Export
173	Fleet Orchestrator Trust Operations
174	Fleet Orchestrator Configuration
175	Fleet Orchestrator - Store File for Distribution
176	Xerox Configuration Watchdog Enablement
177	Xerox Configuration Watchdog Check Complete
178	Xerox Configuration Watchdog Remediation Complete
179	ThinPrint Configuration
180	iBeacon Active
181	Network Troubleshooting Feature
182	POP3 Connection Encryption (TLS)
183	FTP Browse Configuration
184	SFTP Browse Configuration
185	EIP Scheduled Data Push Web Service Enablement

EVENT IDENTIFICATION NUMBER	DESCRIPTION
186	EIP Scheduled Data Push Configuration
187	EIP Scheduled Data Push Run
189	Smart Proximity Sensor “Sleep on Departure” Enablement
190	Cloud Browsing Enablement
192	Scan to Cloud Job
193	Xerox Workplace Cloud Enablement
194	Scan To Save FTP and SFTP Credentials Policy Configured
195	Card Reader
196	EIP App Management
197	EIP App Enablement
199	Card Reader Upgrade Policy
200	Card Reader Upgrade Attempted
201	OCSP Responder Incomplete
202	OCSP Responder Returns a ‘revoked’ Status
203	Log Enhancement
204	Syslog Server Configuration
205	TLS Configuration
206	Security Dashboard Configuration
207	Productivity Kit
208	Canceled Job
209	Embedded Accounts
210	SNMP v1/v2c
211	Xerox Workplace Cloud Remote Management
212	Native Content Protection Configuration
213	Native Content Protection Keyword Detected
214	Delete Job on Error Configuration
215	Delete Job on Error Timer Expired
216	Infrared Security Configuration

EVENT IDENTIFICATION NUMBER	DESCRIPTION
217	Infrared Security Mark Detected
218	Universal Print Enablement
219	Universal Print Registration
220	IDP Authentication Login Attempt
221	External IDP Authentication Enablement
222	Increased Data Analysis
223	FTP Client
224	On Device Card Registration and Login Configured
225	On Device Card Login Attempt
226	Security Template Applied
227	EIP Session Data Modification
228	EIP Registration Data Modification
229	802.1x Authentication Status
230	Fax Card Detection
231	Fax App Configuration

Note: An asterisk (*) next to value indicates Trellix® formerly known as McAfee®.

External Keyboard

This appendix contains:

External Keyboard Shortcuts 466

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
Power Saver / Power Off / Restart	CTRL+F7