VERSION 2.0
JANUARY 2026
702P09472

Xerox® PrimeLink® C9265/C9275/C9281 Series Printer

System Administrator Guide

xerox™

©2026 Xerox Corporation. All rights reserved. Xerox®, PrimeLink™, MeterAssistant®, SuppliesAssistant®, Scan to PC Desktop®, and Xerox Extensible Interface Platform® are trademarks of Xerox Corporation in the United States and/or other countries.

Microsoft, Windows, and Windows Server are registered trademarks of Microsoft Corporation in the United States and/or other countries.

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

Android, and Google Play are trademarks of Google LLC.

GBC® and AdvancedPunch™ are trademarks or registered trademarks of General Binding Corporation.

HP, PCL and HP-UX are registered trademarks of Hewlett-Packard Corporation in the United States and/or other countries.

IBM® is a trademark or registered trademark of International Business Machines Corporation registered in many jurisdictions worldwide.

IOS is a registered trademark or trademark of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

Linux® is a registered trademark of Linus Torvalds 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).

ScanFlowStore® is a registered trademark of Nuance Communications, Inc.

UNIX® is a registered trademark of The Open Group.

Mopria® is a registered trademark and service mark of Mopria Alliance, Inc. in the United States and other countries. Unauthorized use is strictly prohibited.

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.

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

BR41797

Contents

Introduction....13

Configuration Steps....14
More Information....15

Initial Setup....17

Physical Connection....18
Initial Setup at the Control Panel....19
The Installation Wizard....19
Configuration Report....19
Printing the Configuration Report....19
Administrator Access at the Control Panel....20
Locking or Unlocking the Device....20
Manually Setting the Ethernet Interface Speed....21
Assigning a Network Address....21
Viewing Services and Options....22
Embedded Web Server....23
Accessing the Embedded Web Server....23
Enabling Services and Options....24
Enabling Services and Options at the Control Panel....24
Enabling Features in the Embedded Web Server....24
Enabling Features at the Control Panel....24
Changing the System Administrator Password....25
Using the Configuration Overview Page....26
Assigning a Name and Location to the Device....26

Network Connectivity....27

Connecting to a Wireless Network....28
Configuring Wi-Fi from the Embedded Web Server....28
Connecting to a Wi-Fi Network at the Control Panel....29
Disabling Wireless Networking From the Embedded Web Server....30
Disabling Wireless Networking from the Control Panel....30
Wi-Fi Direct....31
NFC....33
USB....34
Universal Print....35
Universal Print Status....35
Universal Print....35
ThinPrint....36
Configuring a ThinPrint....36
TCP/IP....37
Enabling TCP/IP....37
Configuring TCP/IP Settings at the Control Panel....37

Configuring TCP/IP Settings in the Embedded Web Server 39
SNMP 42
Enabling SNMP 42
Configuring SNMP 42
LPD 45
Enabling LPD 45
Configuring LPD 45
Raw TCP/IP Printing 46
Enabling Port 9100 46
Configuring Port 9100 46
SMTP 47
Configuring SMTP Server Settings 47
Configuring Optional SMTP Settings 47
Performing an SMTP Server Connection Test 48
Email Setup with Xerox® Device Code Flow Workgroup Email 48
Pre-Setup for Microsoft 365 Business or School Accounts 48
Registering the Printer for OAuth 2.0 Email 48
LDAP 50
Configuring LDAP Server Settings 50
Defining User Mappings 50
Configuring LDAP Custom Filters 51
Performing an LDAP Connection Test 51
POP3 52
HTTP 53
Enabling HTTP 53
Configuring HTTP Settings 53
Proxy Server 54
IPP 55
Enabling IPP 55
Configuring IPP 55
Universal Plug and Play Discovery 56
Enabling UPnP 56
Configuring UPnP 56
SSDP 57
WebDAV 58
Enabling WebDAV 58
Configuring WebDAV 58
WSD 59
Enabling WSD 59
Configuring WSD 59
FTP 60
Enabling FTP 60
Setting Up the FTP Transfer Mode 60
Enabling and Disabling a Secure FTP in the Embedded Web Server 60
Bonjour Multicast DNS 61

Enabling Bonjour 61
Configuring Bonjour 61
AirPrint 62
Configuring AirPrint 62
Mopria® 64
Configuring Mopria® 64
SOAP 65

Security 67

Setting Up Access Rights 68
Overview 68
Authentication 68
Authorization 68
Personalization 69
Configuring Permissions for Personal Favorites 69
Local Authentication 70
Setting Up Local Authentication 70
Defining User Information 70
Editing the User Information Database 70
Specifying Login Requirements 70
Network Authentication 72
Setting Up Network Authentication 72
Configuring Authentication Server Settings for Kerberos 72
Configuring Authentication Server Settings for SMB 72
Configuring Authentication Server Settings for LDAP 73
Setting the Convenience Login Method 73
Installing a USB Card Reader Plug-in 74
Authentication Using a Card Reader System 75
Setting Up Authentication for a USB Smart Card Reader System 75
Authentication Common Access Card (CAC) 80
Authentication Common Access Card (CAC) Overview 80
Supported Card Types 80
Supported Card Readers 80
Controlling Access to Tools and Features 82
Controlling Access for All Users 82
Enabling a Software Option 86
Digital Certificates 87
Installing a Digital Certificate 87
Creating a Self-Signed Certificate 87
Creating a Request 87
Uploading a Certificate 88
Managing Certificates 88
Certificate Revocation Retrieval Settings 89
Enabling Automatic Self-Signed Certificates 89
Enabling Certificate Path Validation 89
Configuring the Printer for IC or Smart Cards 90

Secure HTTP and SSL/TLS 91
Configuring Settings for SSL/TLS 91
Configuring Domain Filtering 93
S/MIME 94
IPsec 95
Configuring IPSec 95
802.1X 97
Configuring 802.1X 97
FIPS 140 Data Encryption 98
IP Filtering 99
Creating an IP Filter Rule 99
Unbounded Ports 100
Adding an Unbounded Port 100
Editing an Unbounded Port 100
Deleting an Unbounded Port 100
Audit Log 101
Enabling Audit Log 101
Saving an Audit Log 101
Interpreting the Audit Log 101
Setting System Timeouts 103
PDF Signatures 104
Restricting Access to Job Information 105
Hiding or Password Protecting Completed Job Information 105
Hiding Active Job Information 105
Allowing or Restricting Job Operations 105
Restricting Service Representative Operations 107
Setting up Service Representative Restrictions 107
USB Port Security 108
Enabling or Disabling USB Ports 108

Printing 109

General Printer Settings 110
Changing the Tray Settings 110
Configuring Policies for Print Jobs 111
Enabling Print From USB 111
Setting Paper Size Preferences 112
Language Emulation Settings 113
Configuring PostScript Language Emulations 113
Configuring PCL® 6/5e Language Emulations 113
Configuring TIFF and JPEG Language Emulations 113
Configuring HP-GL/2 Language Emulations 113
Configuring PDF Language Emulations 114
Managing Banner Page Printing Options 115
Enabling Banner Page Printing in the Embedded Web Server 115
Enabling Banner Page Printing from the Control Panel 115

Enabling Banner Page Printing in the Xerox Version 3 Print Driver 115
Enabling Banner Page Printing in the Xerox Version 4 Print Driver 116
Print Service Settings 117
Allocating Memory for Print Settings 117
Configuring Other Types of Print Settings 117
UNIX®, Linux®, and AS/400 Printing 120
Xerox® Printer Manager 120
Printing from a Linux® Workstation 121
AS/400 for IBM Power Systems 122

Copying 123

Confirming the Position of Document Guides 124
Setting a Default Image Gradation Mode 125
Specifying Default Copy Settings 126
Copy Control 127
Configuring Presets for Original Page Sizes 128
Reduce and Enlarge Presets 129
Defining Custom Colors 130

Scanning 131

Configuring General Scan Service Settings 132
Setting Scan Defaults 132
Configuring Other Scan Settings 132
Setting Scan to PC Defaults 132
Setting Up Scanning to an FTP Server 133
Setting Up Scanning to an SFTP Server 134
Setting Up Scanning to an Email Address 135
Scanning to a Folder on the Device 136
Managing Folders and Scanned Files 137
Creating and Editing a Folder 137
Scheduling Deletion of Files Stored in Folders 137
Configuring Scan Folder Service Settings 137
Scanning to an Email Address 139
Configuring Email Settings 139
Editing Email Settings 139
Scanning to a USB Drive 141
Enabling Scan to USB Functionality 141
Job Flow Sheets 142
Setting Up a Job Flow Sheet 142
Job Flow Sheet Restrictions 143
Linking the Job Flow Sheet to a Folder 144
Enabling Network Scan Utility 3 145

Faxing 147

Embedded Fax 148
Enabling Embedded Fax 148
To Set Up a Fax 148
Configuring Fax Common Settings 148
Enabling the Output Destination 149
Configuring Fax Control Settings 150
Configure Incoming Fax Settings 151
Setting Incoming Fax Options 152
Storing and Forwarding Received Faxes 153
Storing and Forwarding Faxes Using Fax Identifiers 155
Internet Fax 157
Configuring Internet Fax Settings 157
Configuring Internet Fax General Options 157
Configure Incoming Fax Settings 159
Internet Fax Addresses 159
LAN Fax 160
Session Initiation Protocol Fax 161
Enabling SIP Settings 161
Configuring VoIP Gateway Registration 162
Configuring T.38 Settings 163
Configuring SIP Settings at the Device Control Panel 163
Printing Fax Reports 164
Configuring Reports 164
Printing a Fax Activity Report 164

Accounting 165

Xerox® Standard Accounting Tool 166
Enabling Xerox® Standard Accounting 166
Creating a User Account 166
Editing the Account Settings for Individual Users 167
Changing a User Password 167
Deleting an Account 168
Generating and Downloading a Xerox® Standard Accounting Report 168
Resetting Usage Limits 168
Network Accounting 169
Accounting Using an Auxiliary Device 171

Administrator Tools 173

Monitoring Alerts and Status 174
Xerox Vitals Lightbar (Optional) 174
Setting Up Job Completion Alerts 174
Setting Up Device Status Alerts 174
Fault History 175
Viewing Fault History 175
Activating a Supplies Plan 176
Paper Tray Settings 177

Accessing Paper Tray Settings 177
Custom Paper Settings 177
Establishing Start-Up Attributes 179
Paper Type Priority 179
Setting Paper Tray Attributes 180
Setting Up a Dedicated Paper Tray 181
Changing Paper Settings During Tray Loading 181
Establishing Bypass Tray Defaults 181
Customizing the Paper Supply Screen 182
Paper Tray Priority 182
Managing Automatic Tray Switching 183
Image Quality 183
NVM adjustments required for GBC AdvancedPunch Pro (APP) Software Version 184
Paper Catalog 184
SMart eSolutions 186
SMart eSolutions Overview 186
Configuration Planning 186
Configuring SMart eSolutions 187
Viewing SMart eSolutions Information 188
Troubleshooting 188
Configuring Stored File Settings 192
Retrieving Stored Files 193
Setting Default Touch Screen Settings 194
Taking the Printer Offline 195
Restarting the Device in the Embedded Web Server 196
Changing the Power Saver Settings 197
View Usage and Billing Information 198
Billing Information 198
Usage Counters 198
Enabling the Billing Impression Mode 198
Cloning 199
Creating a Clone File 199
Installing a Clone File 199
Xerox® Device Manager Cloning Feature 199
Public Address Book 200
Address Book Options 200
Editing the Public Address Book as a CSV File 200
Importing an Address Book File 201
Adding, Editing, and Deleting Address Book Entries 201
Font Management Utility 203
Customizing Device Contact Information 204
Xerox Online Support 204
Resetting and Restarting the Printer 205
Restarting the Printer at the Control Panel 205
Updating the Device Software 206
Determining the Current Software Version 206

Updating the Software 206
Date and Time Settings 207
Fax Speed Dial Setup Settings 208
Watermarks and Annotations 209
Creating a Watermark 209
Creating a Universal Unique ID 209
Forced Annotations 209
Memory Settings 211
Backup and Restore 212
Backing Up Device Settings 212
Restoring Device Settings 212
Printer Management 213
Exporting Job History 213
Automatically Deleting Held Jobs 213
Locking the Printer 213

Image Quality and Registration 215

Image Quality and Calibration 216
Setting Image Quality for the Scanner 216
Calibrating Image Color 217
Combined Calibration 219
Two-Sided Color Scanning Calibration 219
Spots/Streaks Diagnostics 220
Simple Image Quality Adjustment (SIQA) Tools 221
Simple Image Quality Adjustment (SIQA) Tools Overview 221
Image Registration Adjustments 221
Density Uniformity Adjustment 226
Creating a Custom Curl Profile as Administrator 228

Customization and Expansion 229

Xerox Extensible Interface Platform® 230
Enabling Extensible Services 230
Enabling Extensible Service Registration 230
Setting Up a File Repository 231
Configuring Template Pool Repository Settings 231
Customizing Apps on the Printer 232
Xerox App Gallery 232
Customizing Apps Available at the Control Panel 232
Pins (Formally Known as Stored Programming) 233
Enabling Pins for Copy App 233
Selecting a Job from Pins 233
Editing Pins 233
Plug-ins and Kits 234
Enabling Plug-ins 234
Managing Plug-Ins 234

Enabling Digital Signature Verification for Secure Plug-Ins..... 234
Auxiliary Interface Kit..... 235
Setting Up the Inserter Module..... 236

Introduction

This chapter contains:

Configuration Steps....14
More Information....15

Configuration Steps

Note: Most configuration settings are on the Home tab under Device Details in the Embedded Web Server. If your device is locked, log in as a system administrator.

1. Connect an Ethernet cable from your device to the network.
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.
3. To provide basic information, such as your location, time zone, and date and time preferences, complete the Installation Wizard.
4. Print a Configuration Report that lists the current configuration for the device. Review the report and locate the IP address for the device.
5. To access the Embedded Web Server, open a Web browser. In the address field, type the IP address of your device. The Embedded Web Server is administration and configuration software installed on the device.
6. Configure the Authentication settings.
7. Configure the Security settings.
8. Enable services in the Embedded Web Server.
9. Configure Print, Scan, and Optional Fax features.
10. Configure the Accounting features.

More Information

Refer to the following sources for more information about your device and its capabilities.

INFORMATION	SOURCE
Installation Guide	Packaged with the device.
Other documentation for your device	Go to www.xerox.com/office/PLC92XXsupport, then select your specific device model.
Technical support information for your device, including online technical support, Online Support Assistant, and print driver downloads.	
Third-party and open-source software disclosure notices and terms and conditions	
Online Support Assistant	
Device Management Tools	
Tested Substrate List (TSL)	A list of substrates or media is validated on this printer. To obtain the list, go to Xerox® PrimeLink® C9265/C9275/C9281 Tested Substrate List or contact your Xerox sales representative.
Information about menus or error messages	On the control panel, touch **Settings > Device Status > Print Reports > Printer Reports**.
Order supplies for your device	Go to www.xerox.com/office/PLC92XXsupplies, then select your specific device model.
Local sales and Technical Customer Support Local sales and customer support	www.xerox.com/office/worldcontacts
Device registration	www.xerox.com/office/register

Initial Setup

This chapter contains:

Physical Connection 18
Initial Setup at the Control Panel 19
Administrator Access at the Control Panel 20
Manually Setting the Ethernet Interface Speed 21
Viewing Services and Options 22
Embedded Web Server 23
Enabling Services and Options 24
Changing the System Administrator Password 25
Using the Configuration Overview Page 26

Physical Connection

To connect your device:

1. Connect the power cord to the device, then plug the power cord into an electrical outlet.
2. Connect one end of a Category 5 or better Ethernet cable to the Ethernet port in the back of the device. Connect the other end of the cable to a correctly configured network port.
3. If you purchased and installed the Fax Hardware Kit, connect the device to a correctly configured telephone line.
4. Power on the device.

Initial Setup at the Control Panel

THE INSTALLATION WIZARD

The first time that you power on the device, the Installation Wizard starts. The wizard prompts you with a series of questions to help you configure the following basic settings for your device:

- Current date and time
- Local time zone
- Certification, system access level, SMTP, and LDAP
- Language
- Units of Measurement

CONFIGURATION REPORT

After you complete the Installation Wizard, you can obtain a Configuration Report. The Configuration Report lists the current settings for the device.

PRINTING THE CONFIGURATION REPORT

To print a configuration report:

1. At the device control panel, log in as Administrator, For details, refer to Administrator Access at the Control Panel.
2. Touch **Settings > Device Status**.
3. Touch **Print Reports > Printer Reports**.
4. Touch **Configuration Report**, then touch **Print**.

Administrator Access at the Control Panel

To configure the device from the control panel, log in as Administrator.

To log in as Administrator:

1. At the device control panel, Production Print EIP UI is displayed. Press **Home** button.
2. Touch **Log In**.
3. Type **admin**.
4. Type the administrator password, then touch **Log In**.

Note: The original password is the device serial number. When the administrator password is set to the device serial number, administrator functions are not accessible. If the administrator password is set to the device serial number, at the next administrator login attempt, you are prompted to change the administrator password. After you change the administrator password, you have full access to administrator privileges.

To log out, touch **Log Out**. On the new screen, touch **Log Out**.

LOCKING OR UNLOCKING THE DEVICE

To lock or unlock the device:

1. At the device control panel, log in as Administrator. For details, refer to Administrator Access at the Control Panel.
2. Touch **Settings > Device > Authentication/Accounting > Authentication/Security Settings > Administrator Settings**.
3. Enter the Administrator ID and Administrator Password.
4. Touch **OK**.

Manually Setting the Ethernet Interface Speed

The device Ethernet interface detects the speed of your network automatically. If your network is connected to another auto-sensing device, such as a hub, it is possible that the hub does not detect the correct speed. To ensure that the device has detected the correct speed of your network, refer to the Configuration Report. To view the Configuration Report, refer to Printing the Configuration Report.

To set the device Ethernet interface speed manually:

1. At the device control panel, log in as Administrator, for details, refer to Administrator Access at the Control Panel.
2. Touch **Settings > Device > Network Settings > Protocol Settings**.
3. Touch **Ethernet Settings**.
4. Touch **Ethernet - Rated Speed**.
5. To match the speed set on your hub or switch, select the speed.
6. Touch **Energy Efficient Ethernet**.
7. Touch **Enabled**, then touch **OK**.

ASSIGNING A NETWORK ADDRESS

By default, the device acquires a network address from a DHCP server automatically. To assign a static IP address, configure DNS server settings, or configure other TCP/IP settings, refer to TCP/IP.

Viewing Services and Options

To view the services and options that are enabled or installed:

1. At the device control panel, press the **Home** button, then touch **Settings > Device Status**.
2. Touch **Details > Device Configuration**.

   The Device Configuration screen appears.

Embedded Web Server

The Embedded Web Server allows you to configure and administer the device from a Web browser on any computer.

ACCESSING THE EMBEDDED WEB SERVER

Before you begin:

- Ensure that TCP/IP and HTTP are enabled. A TCP/IP or HTTP connection is required to access the Embedded Web Server. For details, refer to Enabling TCP/IP.
- To determine the device IP address, do one of the following:
  - Obtain a Configuration Report. For details, refer to Printing the Configuration Report.
  - At the control panel, press **Home** button.

To access the Embedded Web Server:

1. At your computer, open a Web browser.
2. Type the device IP address in the address field. Press **Enter**. The Status page of the Embedded Web Server appears.
   - You can access the device using a combination of the host name and the domain name as the Internet address. A DNS (Domain Name System) is required. The DNS server requires that the device host name is registered.
   - To specify a port number, for the IP address, type **:** and the port number.
3. If prompted, type the user name and password for the administrator account, then click **Sign in**.

Note: The default administrator user name is **admin** and the original password is the device serial number. When the administrator password is set to the device serial number, administrator functions are not accessible. If the administrator password is set to the device serial number, at the next administrator login attempt, you are prompted to change the administrator password. After you change the administrator password, you have full access to administrator privileges.

Enabling Services and Options

Some services and options are disabled by default. To enable these special services and options, use the device control panel or the Embedded Web Server.

ENABLING SERVICES AND OPTIONS AT THE CONTROL PANEL

To enable services and options at the device control panel:

1. At the device control panel, log in as Administrator, For details, refer to Administrator Access at the Control Panel.
2. Touch **Device > Maintenance**.
3. Touch **Software Options**.
4. Type the code, then touch **Restart**.

ENABLING FEATURES IN THE EMBEDDED WEB SERVER

To enable services and options in the Embedded Web Server:

1. In the Embedded Web Server, click **System > Security > Unique Function Code Settings**.
2. For Unique Function Code, type the required information.
3. Click **Save**.

ENABLING FEATURES AT THE CONTROL PANEL

1. At the control panel, touch **Log In**.
2. At the key operator login screen, select **More Characters** located at the bottom of the screen.
3. Select the asterisk (*****) from More Characters.

   In the Admin's Login ID field, the asterisk (*) will appear next to the **Admin's Login ID**.
4. Select **Standard Characters** and enter the required Unique Function Code (SFR Key).
   Ensure that the asterisk (*) precedes the code.
5. Click **Login**.

   The machine reboots automatically.

Changing the System Administrator Password

For security purposes, after you configure the device, it is recommended that you change the default system administrator password. Store the password in a secure location.

To change the Administrator password:

1. In the Embedded Web Server, click **Permissions**. In User Accounts area, click **admin**.
2. In User Details area, to change the login credentials, click **Change Password**.
3. In Change Password area, type the Current Password and New Password.
4. Retype the password.
5. Click **Save**.

Using the Configuration Overview Page

In the Embedded Web Server, the Configuration Overview page provides shortcuts to commonly accessed pages on the Home tab. To access the Configuration Overview page, click **Device Information > Details**, then in Configuration area, click **Check Status**.

ASSIGNING A NAME AND LOCATION TO THE DEVICE

On the Description page, you can assign a name and location to the device for future reference.

To assign a device name and location:

1. In the Embedded Web Server, login as Administrator, click **Home** tab, then in Device Information area, click **Details**.
2. For Device Name, type a name for the device.
3. For Device Location field, type the Location, Latitude, and Longitude of the device.
4. In the System Administrator field, type the Administrator contact information and the device email address, as needed.
5. Click **Save**.

Network Connectivity

This chapter contains:

Connecting to a Wireless Network 28
Wi-Fi Direct 31
NFC 33
USB 34
Universal Print 35
ThinPrint 36
TCP/IP 37
SNMP 42
LPD 45
Raw TCP/IP Printing 46
SMTP 47
LDAP 50
POP3 52
HTTP 53
Proxy Server 54
IPP 55
Universal Plug and Play Discovery 56
SSDP 57
WebDAV 58
WSD 59
FTP 60
Bonjour Multicast DNS 61
AirPrint 62
Mopria® 64
SOAP 65

Connecting to a Wireless Network

Note:

- If the printer is connected to your wired network, you can configure wireless settings in the Embedded Web Server.
- Before you begin, purchase and install the Xerox® Wireless Network Adapter. For information on installing the Wireless Network Adapter, refer to the User Guide for your printer model.

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

Note:

- The printer uses separate IP settings for wired and wireless connections. For more information, refer to IP.
- 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 your Web browser address field, type the new IP address or host name of your printer.

CONFIGURING WI-FI FROM THE EMBEDDED WEB SERVER

To configure Wi-Fi from the Embedded Web Server, do the following:

1. Connect the printer to a wired network.
2. In the Embedded Web Server, log in as administrator, then click **Network > Wi-Fi**.

Note: Wi-Fi is available after you install the Xerox® Wireless Network Adapter.

1. To enable Wi-Fi, click the **Enable** toggle button.
2. Enter the Network Name.
3. Click **Operating Frequency Band**, then select an option.
4. For SSID, type the SSID for the network to which you want to connect.
5. In the TCP/IP Settings area, configure the settings for IPv4, IPv6, and DNS.

Note: The printer uses separate IP settings for wired and wireless network connections. For details, refer to IP.

1. In the Security Settings area, click **Encryption**, then select a mode of encryption.
2. For the selected mode of encryption, configure the security settings.
   - For WEP:
     - To activate a transmit key, click **Transmit Key**.
     - For each Transmit Key that you select, type values into the corresponding fields.
   - For both WPA2 Personal and Mixed Mode Personal, type the network passcode in the Passcode field and the Retype Passcode field.

- For both WPA2 Enterprise and Mixed Mode Enterprise:
  - Click **Authentication Method**, then select the authentication method for your wireless network.
  - For Root Certificate, upload a Root Certificate.
  - Type values for EAP Identity, Login Name, and Password.

Note: For EAP_TLS Network implementation, the Device Default Certificate cannot be used as a Client Certificate. Generate a Client Certificate, then install the certificate on the printer.

3. Click **Save**.
4. For the new settings to take effect, restart the printer.
5. Disconnect the printer from the wired network.

CONNECTING TO A WI-FI NETWORK AT THE CONTROL PANEL

To connect to a Wi-Fi network at the control panel:

1. At the printer control panel, press the **Home** button.
2. Log in as administrator. For details, refer to Administrator Access at the Control Panel.
3. Touch **Device > Network Settings > Wireless LAN Setting > Common Settings**.
4. To enable the Wi-Fi feature, touch **Enable** toggle button.
5. To connect automatically to an existing Wi-Fi network:
   a. Touch **Wi-Fi Connection Settings**.
   b. In the list of available Wi-Fi networks, touch the required network.

Note: If the required Wi-Fi network is not listed, or if the required network uses WPS, configure the connection manually.

   c. If needed, to log in to the network, type the password.
   d. To select a Wi-Fi frequency band, touch **Operating Frequency Band**, then select an option.

Note: The Wi-Fi frequency band is set to AUTO by default.

   e. Touch **OK**.
6. To connect manually to a Wi-Fi Network:
   a. Touch **Wi-Fi Connection Settings > Manual Settings**.
   b. In the first field, type a name for the Wi-Fi network.
   c. To enter the SSID for the network, touch **SSID**, then touch **OK**.
   d. Touch **Encryption Setting**, then select an option.
   e. For a WPS setup with a Push Button Connection (PBC), enable **WPS (Push Button)**.
   f. Touch **Start**.

DISABLING WIRELESS NETWORKING FROM THE EMBEDDED WEB SERVER

Note: Wireless networking is available only on printers with the optional Wireless Network Adapter installed.

1. In the Embedded Web Server, log in as administrator, then click **Network > Wi-Fi**.
2. Click the **Enable** toggle button.
3. Click **Save**.
4. To activate your changes, at the prompt, click **Restart Now**.

DISABLING WIRELESS NETWORKING FROM THE CONTROL PANEL

You can disable the wireless network from the printer control panel.

Note: Wireless networking is available only on printers with the optional Wireless Network Adapter installed.

To disable wireless networking from the Control Panel:

1. At the printer control panel, press the **Home** button.
2. Log in as administrator. For details, refer to Administrator Access at the Control Panel.
3. To open the Wi-Fi menu, touch **Device > Network Settings > Wireless LAN Settings > Common Settings**.
4. To toggle Wi-Fi from On to Off, touch the **Enable** or **Disable** toggle button.
5. Touch **OK**.
6. Press the **Home** button.
7. For the setting to take effect, at the prompt, touch **Restart Now**.

Wi-Fi Direct

A Wi-Fi Direct network connection enables devices to connect with each other without requiring a wireless access point. You can connect to your printer from a Wi-Fi mobile device such as a tablet, computer, or smart phone.

A Wi-Fi Direct connection does not require manual configuration.

Note:

- Wireless networking is available only on printers that have the optional Wireless Network Adapter installed.
- The Wi-Fi Direct connection is disabled by default.

To configure Wi-Fi Direct from the Embedded Web Server:

1. In the Embedded Web Server, log in as administrator, then click **Network**.
2. click **Wi-Fi Direct**.
3. To enable Wi-Fi Direct, click the **Enable** toggle button.
4. Click **Group Role**, then select an option from the menu.
   - To set the printer to configure the Group Role automatically:
     - Select **Auto**.
     - For Device Name, type a name for the printer.
   - To set the printer as Group Owner for a Wi-Fi Direct group, similar to a wireless access point:
     - Select **Group Owner**.
     - In the Group Owner area, type the information for SSID and Passphrase.
5. For DHCP Server:
   - Type the IP Address and Subnet Mask.
   - For IP Address Lease Time, type the number of minutes.
6. Click **Save**.

To configure Wi-Fi Direct at the control panel:

1. At the printer control panel, press the **Home** button.
2. Log in as administrator.
3. Touch **Settings > Device > Network Settings > Wireless LAN Settings > Wi-Fi Direct Settings**.
4. For Wi-Fi Direct, touch the enable toggle button.
5. Touch **Setup**.
6. Touch **Group Settings**, then select an option.
7. If needed, touch **SSID Suffix**, then type a suffix.
8. If you selected Group Owner as the Group Settings, in the Passphrase field, enter an eight-character passcode.
9. Touch **OK**.

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

NFC

Near Field Communication (NFC) is a technology that enable devices to communicate when they are within 10 centimeters of each other.

You can use NFC to obtain the network interface to establish a TCP/IP connection between your mobile device and the printer.

Note:

- Currently, Xerox® PrimeLink® C9200 Series Printers only support NFC with Android-based mobile devices.
- To print wirelessly after you enable NFC, install the Xerox Print Utility application on your Android device. The application is available in Google Play Store.
- For NFC to function properly, first enable NFC on the printer, then enable the application in your mobile device.

To enable NFC:

1. In the Embedded Web Server, log in as a system administrator, then click **Network > NFC**.
2. To enable NFC, enable the toggle button.
3. Click **Save**.
4. Select **Restart Later** or **Restart Now**.

   If Restart Later is selected, click **Close**.

Tip: If the NFC icon does not light up when the toggle button is set to enable, ensure all plug-ins are enabled. In the Embedded Web Server, log in as a system administrator. Click **System > Plug-in Settings**, then enable the toggle button for **Embedded Plug-ins**.

USB

The printer provides multiple USB ports. The exact number varies, depending on the printer model. All models have the following two USB ports:

- One host port on the front of the printer
- One target port on the back of the printer

In the Embedded Web Server, the USB configuration window provides two toggle buttons for enabling USB:

- **Enable**: This toggle button enables and disables all the USB ports at the same time.
- **USB Port**: This toggle button enables and disables only the target port on the back of the printer.

To configure USB:

1. In the Embedded Web Server, log in as administrator, then click **Network**.
2. Click **USB**.
3. Enable a port.
   - To enable USB communication on all USB ports, click the **Enable** toggle button.
   - To enable the target USB port on the back of the printer, click the **USB Port** toggle button.

Note: To use the target USB port on the back of the printer, click both the **Enable** toggle button and the **USB Port** toggle button.

1. To enable Printer Job Language, click the **PJL** toggle button.
2. Click **Print Mode**, then select a mode.
3. For Auto Job Timeout, type the amount of time in seconds that the printer becomes inactive, before cancelling the print job.
4. Click **Adobe Communication Protocol**, then select a protocol.
5. To enable PostScript® Wait Timeout (RAW Mode), click the toggle button.
6. Click **Save**.

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

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.

UNIVERSAL PRINT

To enable Universal Print:

1. In the Embedded Web Server, click **Network > Mobile Printing > Universal Print**.
2. For Universal Print, select **Enabled**,
3. Click **Save**.

ThinPrint

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 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.

CONFIGURING A THINPRINT

To configure your printer as a ThinPrint:

1. In the Embedded Web Server, click **Network > Protocols > ThinPrint**.
2. For ThinPrint Printing, select **Enabled**.
3. 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.
4. For Packet Size, enter the value.
   The packet size determines the size of the unit for transferring the printing data.
5. The default TCP Port is 4000. To use a different port, in the Port Number field, type a port number.
6. To enable Printer Job Language, click the **PJL** toggle button.
7. To use TBCP Filter, select **Enabled**.
8. Enter the Timeout value in seconds.

TCP/IP

Transmission Control Protocol (TCP) and Internet Protocol (IP) are two protocols within the Internet Protocol Suite. IP manages the transmission of messages from computer to computer, while TCP manages the actual end-to-end connections.

ENABLING TCP/IP

Note: TCP/IP is enabled by default. If you disable TCP/IP, to access the Embedded Web Server, at the device control panel, enable TCP/IP.

To enable TCP/IP:

1. At the device control panel, log in as Administrator. For details, refer to Administrator Access at the Control Panel.
2. Touch **Settings > Device > Network Settings > Protocol Settings**.
3. Touch **TCP/IP - Common Settings**.
4. Select the item you want to change.
5. Touch **IPv4 Mode** or **IPv6 Mode**. To enable both IPv4 and IPv6, touch **Dual Stack**.

CONFIGURING TCP/IP SETTINGS AT THE CONTROL PANEL

Manually Configuring an IPv4 Network Address

To configure an IPv4 network address:

1. At the device control panel, log in as Administrator. For details, refer to Administrator Access at the Control Panel.
2. Touch **Settings > Device > Network Setting > Protocol Settings**.
3. Select **TCP-IP Network Settings**.
4. Select **IPv4 - IP Address Resolution**.
5. Touch **Static**, then touch **Ok**.
6. Touch **IPv4 - IP Address**.
7. Using the touch-screen keypad, type the static IP address, then touch **OK**.
8. Touch **IPv4 - Subnet Mask**.
9. Using the touch-screen keypad, type the subnet mask, then touch **OK**.
10. Touch **IPv4 - Gateway Address**.
11. Using the touch-screen keypad, type the gateway address, then touch **OK**.

Manually Configuring an IPv6 Network Address

To configure an IPv6 network address:

1. At the device control panel, log in as Administrator. For details, refer to Administrator Access at the Control Panel.
2. Touch **Settings > Device > Network Settings > Protocol Settings**.
3. Touch **TCP/IP - Network Settings**.
4. Touch **IPv6 Address Manual Configuration**.
5. Touch **Enabled**.
6. Touch **Manually Configured IPv6 Address**.
7. Using the touch-screen keypad, type the static IP address, then touch **OK**.
8. Touch **Manually Configured IPv6 Address Prefix**.
9. Using the touch-screen keypad, type the prefix, then touch **OK**.
10. Touch **Manually Configured IPv6 Address Gateway**.
11. Using the touch-screen keypad, type the gateway address, then touch **OK**.

Configuring IPv4 Dynamic Address Settings

To configure IPv4 dynamic address settings:

1. At the device control panel, log in as Administrator. For details, refer to Administrator Access at the Control Panel.
2. Touch **Settings > Device > Network Settings > Protocol Settings**.
3. Touch **TCP/IP - Network Settings**.
4. Touch **IPv4 - IP Address Resolution**.
5. Touch **DHCP**, **BOOTP**, **DHCP/AutoIP**, or **STATIC**, then touch **Save**.

Configuring IPv6 Dynamic Address Settings

To configure IPv6 dynamic address settings at the control panel:

1. At the device control panel, log in as Administrator, press the **Home** button. For details, refer to Administrator Access at the Control Panel.
2. Touch **Settings > Device > Network Settings > Protocol Settings**.
3. Touch **TCP/IP-Network Settings**.
4. Touch **IPv6 Address Manual Configuration**.
5. Touch **Disabled**.
6. To view the acquired IPv6 address information, touch **Automatically Configured IPv6 Address**.

Configuring DNS and DDNS Settings

Domain Name System (DNS) and Dynamic Domain Name System (DDNS) are systems that map host names to IP addresses.

To configure DNS settings at the control panel:

1. At the device control panel, log in as Administrator. For details, refer to Administrator Access at the Control Panel.
2. Touch **System Settings > Device > Network Setting > Protocol Settings**.
3. Touch **TCP/IP - Network Settings**.
4. Touch **IPv4 DNS Server Setup** or **IPv6 DNS Server Setup**.
5. Do one of the following:
   - To allow your DHCP server to provide the DNS server address, touch **Get IP Address from DHCP**. Touch **Enabled**.
   - To provide the DNS server address manually, touch **Preferred DNS Server IP Address**. Type the DNS server address, then touch **OK**.

CONFIGURING TCP/IP SETTINGS IN THE EMBEDDED WEB SERVER

If your device has a valid network address, you can configure TCP/IP settings in the Embedded Web Server.

Configuring Settings for IPv4

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

Note: If both IPv4 and IPv6 are disabled, you cannot access the Embedded Web Server. Before you can access the Embedded Web Server, at the device control panel, re-enable TCP/IP. Disabling TCP/IP or changing the IP address disables any dependent protocols.

To configure settings for IPv4:

1. In the Embedded Web Server, click **Network > Ethernet > IPv4**.

   Note: IPv4 is enabled by default.
2. To make changes, touch **Edit**.
3. From the IP Address Resolution menu, select the method for obtaining a dynamic IP address, or to define a static IP address, select **Static**.
4. If you selected Static, type the appropriate information in the following fields: IP Address, Subnet Mask, and Gateway Address.

   Note: If you select BOOTP or DHCP, you cannot change the IP Address, Subnet Mask, or Gateway Address.
5. Click **Save**.

DNS Configuration for IPv4

To configure settings for IPv4:

1. In the Embedded Web Server, click **Network > Ethernet > DNS Configuration**.

2. To allow your DHCP server to provide the DNS server address, in the DNS Configuration area, for Obtain DNS Server Address Automatically, select **Enabled**. To provide the DNS server address manually, clear the check box. For Preferred DNS Server, Alternate DNS Server 1, and Alternate DNS Server 2, type the appropriate IP addresses.

   Note: If DHCP or BOOTP is the IP Address Resolution setting, you cannot change the Domain Name, Primary DNS Server, Alternate DNS Server 1, and Alternate DNS Server 2 settings.

3. To register the device host name in the DNS server, for Dynamic DNS Registration (DDNS), select **Enabled**. To replace existing entries in the DNS server, select **Overwrite**.

   Note: If your DNS Server does not support dynamic updates, you do not need to enable DDNS.

4. To instruct the device to generate a list of search domains, for Generate Domain Search List Automatically, select **Enabled**. If this option is disabled, type the domain names.
5. For Connection Timeout, type the number of seconds allowed until the device stops attempting to connect to the server.
6. Click **Save**.

Configuring Settings for 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 the request with a router advertisement packet containing network-layer configuration parameters.

Note:

- IPv6 is optional. You can use IPv6 in addition to, or in place of, IPv4. If both protocols are disabled, you cannot access the Embedded Web Server. The host name is the same for IPv4 and IPv6. If you change the host name for IPv6, the host name also changes for IPv4.
- If both IPv4 and IPv6 are disabled, you cannot access the Embedded Web Server. Before you can access the Embedded Web Server, at the device control panel, re-enable TCP/IP. If you disable TCP/IP or change the IP address, any dependent protocols are disabled.

To configure settings for IPv6:

1. In the Embedded Web Server, click **Network > Ethernet > IPv6**.
2. For IP Mode, select **IPv6**, or to use both IPv4 and IPv6, select **Dual Stack** under Common. By default, IPv6 is disabled.
3. Type a unique Host Name for the device.
4. To assign an address manually, for Enable Manual Address, select **Enabled**. Type the IP Address and Gateway Address.
5. To allow your DHCP server to assign an IP address to the device, select **Get Configuration Data**.
6. Click **Save**.

DNS Configuration for IPv6

To configure settings for IPv6:

1. In the Embedded WebServer, click **Network > Ethernet > DNS Configuration**.
2. Select a method for obtaining the DNS server address:
   - To allow the DHCP server to provide the DNS server address automatically, for Get IP Address from DHCPv6–Lite, select **Enabled**.
   - To specify the DNS server addresses manually, for DHCPv6–Lite, select **Disabled**. Type the IP addresses of the Preferred DNS Server, the DNS Server Address 1, and the DNS Server Address 2.
3. To register the device host name in the DNS server, for Dynamic DNS Registration, select **Enabled**. To replace the existing DNS entry, for Dynamic DNS Registration, select **Overwrite**.
4. To generate the domain search list automatically, for Generate Domain Search List Automatically, select **Enabled**.
5. For Domain Name 1, Domain Name 2, and Domain Name 3, type the domain names.
6. For Connection Timeout, type the number of seconds allowed until the device stops attempting to connect to the server.
7. For DNS Encryption, select an option.
8. Click **Save**.

Zero-Configuration Networking

To support zero-configuration networking, the printer assigns a self-signed address automatically. The self-signed address is for IPv4, IPv6, or both, for a dual-stack configuration. If the printer cannot connect to a DHCP server to obtain an IP address, the printer assigns itself a Link-Local address.

SNMP

Simple Network Management Protocol (SNMP) is used in network management systems to monitor network-attached devices for conditions that require administrative attention. SNMP consists of a set of standards for network management, including an application layer, a database schema, and a set of data objects. Agents, or software modules, reside in the SNMPv3 engine of the device. A manager is an SNMPv3 management application such as OpenView, that is used to monitor and configure devices on the network. The agent responds to read (GET) requests and write (SET) requests from the manager. The agent can generate alert messages, or traps, based on certain events.

You can configure SNMP settings in the Embedded Web Server. You can enable or disable Authentication Failure Generic Traps on the device. To create an encrypted channel for secure device management, you can enable SNMPv3.

ENABLING SNMP

To enable SNMP:

1. In the Embedded Web Server, click **Network > Protocol > SNMP**.
2. For SNMP, select **Enabled**.
3. Click **Save**.

CONFIGURING SNMP

To configure SNMP settings:

1. In the Embedded Web Server, click **Network > Protocols > SNMP**.
2. For SNMP Properties, select **Enable SNMP v1/v2c Protocols** or **Enable SNMP v3 Protocol**.
   To use SNMPv3, enable and configure HTTPS.
3. To allow remote management servers to change SNMP settings on the device, select **Allow Write**.
4. To instruct the device to generate a trap for every SNMP request received by the device that contains an invalid community name, for Authentication Failure Generic Traps, select **Enabled**.
5. Click **Save**.

Editing SNMP v1/v2c Properties

Note:

- For security purposes, Xerox recommends that you change the SNMP v1/v2c public and private community names from the default values.
- Ensure that the **GET** or **SET** community names in each application that uses SNMP to communicate with this device match the corresponding names on the device.

To edit SNMP v1/v2c properties:

1. In the Embedded Web Server, click **Properties > Connectivity > Protocols > SNMP Configuration**.
2. For SNMP Properties, click **Edit SNMP v1/v2c Properties**.

3. For Community Name (Read Only), type a name up to 256 characters, or use the default value of `public`.

   GET returns the password for the **SNMP GET** requests to the device. Applications that use SNMP to obtain information from the device, such as the Embedded Web Server, use this password.

4. For Community Name (Read / Write), type a name up to 256 characters, or use the default value of `private`.

   SET returns the password for the **SNMP SET** requests to the device. Applications that use SNMP to set information on the device use this password.

5. For Trap Community Name, type a name up to 256 characters for the default, or use the default value of `SNMP_TRAP`.

   Note: The Default Trap Community Name is used to specify the default community name for all traps generated by this device. The Trap Community Name specified for each individual trap destination address can override the Default Trap Community Name. The Trap Community Name for one address can differ from the Trap Community Name specified for another address.

6. For the System Administrator Name field, type the administrator login credentials.
7. Click **Save**.

Editing SNMP v3 Settings

Note: Before you can enable SNMPv3, ensure that a digital certificate is installed on the device and that HTTPS is enabled. For details, refer to Installing a Digital Certificate and Enabling HTTP.

To edit SNMP v3 properties:

1. In the Embedded Web Server, click **Network > Protocols > SNMP**.
2. For SNMP Properties, click **SNMP v3**.
3. To create the administrator account, for Administrator Account, click **Account Enabled**.
4. Type an Authentication Password, then confirm it.
   The Authentication Password must be at least eight characters in length and can include any characters, except control characters. The Authentication Password is used to generate a key for authentication.
5. Type a Encryption Password, then to confirm, type the Privacy Password again.
   The Privacy Password is used for encryption of SNMPv3 data. The password used for data encryption must match the password for the server.
6. For Print Drivers Account, click **Account Enabled**.
7. To reset the password, for Reset to default Password, click **Reset**.
8. Click **Save**.

Adding IP Trap Destination Addresses

To configure IP trap destinations:

1. In the Embedded Web Server, click **Network > Protocol > SNMP > SNMP v1/v2/v3**.
2. At the bottom of the page, click **Available**.
3. For Trap Destination Addresses, click **Add UDP IPv4 Address** or **Add UDP IPv6 Address**.

4. Type the IP address of the host running the SNMP manager application that is to receive traps.

   Note: Port 162 is the port for UDP and is the default port for traps. Select v1 or v2c based on which protocol the trap-receiving system supports.

5. For Traps, select the type of traps that the SNMP manager receives.
6. Click **Save**.

LPD

The Line Printer Daemon (LPD) protocol is used to provide print spooling and network print-server functionality for operating systems such as HP-UX, Linux®, and MAC OS X.

Note: For information on setting up print queues on your client system, refer to the documentation for your client system.

ENABLING LPD

To enable the LPD protocol:

1. In the Embedded Web Server, click **Network > Protocol > LPD**.
2. For LPD, select **Enabled**.

   Note: Disabling LPD affects clients printing to the device over TCP/IP using the LPR printing port.
3. Click **Save**.

CONFIGURING LPD

To configure the Line Printer Daemon protocol:

1. In the Embedded Web Server, click **Network > Protocol > LPD**.
2. Type an LPD port number or use the default port number, 515.
3. For Connection Timeout, type the timeout information.
4. For Maximum Number of Sessions, type a number.
5. If required, for TCP-MSS Mode, select **Enabled**.
6. If TCP-MSS mode is enabled, for IPv4, type the IP addresses for Subnet 1, Subnet 2, and Subnet 3.

   Note: TCP-MSS settings are common for LPD and Port 9100.
7. To use TBCP Filter, select **Enabled**.
8. Click **Print Mode**, select an option.
9. To enable PJL, select **Enabled**.
10. Select Character Encoding from the list.
11. Click **Save**.

Raw TCP/IP Printing

Raw TCP/IP is a printing method used to open a TCP socket-level connection over Port 9100. This connection is used to stream a print-ready file to the device input buffer. The connection closes after sensing an End-Of-Job character in the PDL or after the 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 device. In Windows, the Standard TCP/IP port is port 9100.

ENABLING PORT 9100

Note: Before you enable Port 9100, enable TCP/IP.

To enable port 9100:

1. In the Embedded Web Server, click **Network > Protocols > Port 9100**.
2. For Port 9100, select **Enabled**.
3. Click **Save**.

CONFIGURING PORT 9100

To configure port 9100:

1. In the Embedded Web Server, click **Network > Protocols > Port 9100**.
2. If necessary, for TCP-MSS Mode, select **Enabled**.

Note: TCP-MSS settings are common for LPD and Port 9100.

3. If TCP-MSS mode is enabled, for IPv4, type the IP addresses for Subnet 1, Subnet 2, and Subnet 3.
4. Ensure that the TCP Port Number is set to 9100.
5. To set the number of seconds before the device processes a job with an End-of-Job character, set the End of Job Timeout to the needed number of seconds between 0–65535. The default time is 300 seconds.
6. To use TBCP Filter, select **Enabled**.
7. Click **Print Mode**, select an option.
8. To enable PJL, select **Enabled**.
9. Click **Save**.

SMTP

The device email feature uses Simple Mail Transfer Protocol (SMTP) to deliver scanned images and Internet Fax jobs through email. After you enable SMTP, the email button is enabled on the device control panel.

CONFIGURING SMTP SERVER SETTINGS

To configure SMTP server settings:

1. In the Embedded Web Server, click **Network > Protocols > SMTP**.
   To configure the printer for OAuth 2.0 email with Microsoft 365 Exchange Online, refer to Email Setup with Xerox Device Code Flow Workgroup Email. Continue if not configuring the printer for OAuth 2.0 email with Microsoft 365 Exchange Online.
2. Type the SMTP server IP address or host name.
3. Type the port numbers for sending email, sending Internet Fax, and for receiving email. The default port number is 25.
4. For SMTP - SSL/TLS Communication, select an option.
5. To configure Email Send Authentication, select **On**.
6. Type the Device's Email Address.
7. Click **Save**.

CONFIGURING OPTIONAL SMTP SETTINGS

To configure optional SMTP settings:

- To improve transmission speed, you can set messages for fragmentation 2–500 times. To enable message fragmentation, for Split Send, select **Enabled**.
- To set the number of fragments per message, for Maximum Split Count, type a value 2–500.
- To select how the email jobs are split, for Split Send Method, select one of the following:
  - **Split into Pages**: If you select this option, the mail client does not reassemble the job on receipt.
  - **Split by Data Size**: If you select this option, the mail client is required to reassemble the job on receipt.
- To define a maximum message size for messages with attachments, for Maximum Data Size per Email type a value 512–20480 Kbytes. The default size is 10240 Kbytes.
- To set a maximum job size, for Maximum Total Data Size, type a value 512–2000000 Kbytes.
- To have the device authenticate itself using the Login Name and Password set up on this page, for Login Credentials for the Device to access the SMTP Server to send automated Emails, select an option:
  - **None**: If you select this option, the device does not provide authentication credentials to the SMTP server.
  - **SMTP AUTH**: If you select this option, type the Login Name and Password, then retype the password.
- If authentication is enabled and the device is configured to require users to log in before they can access email, to use the credentials of the user to access the SMTP server, for Login Credentials for Email Send, select **Remotely Authenticated User**. To allow the field to default to the same setting that you selected for sending automated email messages, select **System**.

- For When Remotely Authenticated User Fails to Log In, select an option:
  - **Cancel Email Send**: This option cancels the email transfer.
  - **Relogin using System Data**: This option allows the device to log in the user using stored credentials. If login is successful, the device sends the email.
- Click **Apply**.

PERFORMING AN SMTP SERVER CONNECTION TEST

To perform the connection test:

1. In the Embedded Web Server, click **Network > Protocols > SMTP > Connection Test**.
2. In the Connection Test Email area, type your email address.
3. Click **Start**.

You can view the test result in the Email Delivery Status area. You can find the email that was sent from the device in the email for the Connection Test Email address that you provided.

EMAIL SETUP WITH XEROX® DEVICE CODE FLOW WORKGROUP EMAIL

The supported account types are Outlook Only, Microsoft 365 Personal, Microsoft 365 Business or School.

PRE-SETUP FOR MICROSOFT 365 BUSINESS OR SCHOOL ACCOUNTS

1. If the email account that you wish to use to sign-in to the Xerox® Device Code Flow Workgroup Email application belongs to a business or a school, your Microsoft tenant administrator must consent to the Xerox® Device Code Flow Workgroup Email application by visiting https://www.xerox.com/oauth2-email-admin-consent.
2. After consenting to the Xerox® Device Code Flow Workgroup Email application, your Microsoft tenant administrator may also assign only one or more email accounts to the Xerox® Device Code Flow Workgroup Email application. Contact your Microsoft tenant administrator on how this is accomplished.

REGISTERING THE PRINTER FOR OAUTH 2.0 EMAIL

1. In the Embedded Web Server, click **Network > Protocols > SMTP**.
2. On the SMTP page, click **Service Provider**, then select **Exchange Online / Outlook.com**.
3. Click **Save** and follow the instructions on the screen to register the printer for email.

Note: The other settings like the SMTP server address or ports for sending email, Microsoft Entra Endpoint Settings, and Exchange Online/Outlook.com SMTP Client Settings can remain default or may be edited, if required. Below are the default values.

- **Host Name**: login.microsoftonline.com
- **Device Code Path**: oauth2/v2.0/devicecode
- **Token Path**: oauth2/v2.0/token
- **Tenant**: common
- **Client ID**: ef070a3a-4ded-4bed-b03e-81d33fd61f9b

- **Scope**: https://outlook.office.com/SMTP.Send offline_access openid email

4. A code will be generated. Copy the code and follow the instructions on the screen to sign-in to the Xerox® Device Code Flow Workgroup Email application to register the printer for email.
5. After successful registration, the printer may need a reboot. After the reboot, device is ready to send emails.

Note: The email account that will be used to authenticate with Microsoft to sign-in to the Xerox® Device Code Flow Workgroup Email application shall be the From address that will be used for both user-initiated and device-initiated jobs (Email Alerts, Fax Forwarding to Email (if available), and Internet Fax (if available)).

Note: TCP port 587 should not be blocked by the network of the customer.

Note: POP3 protocol does not support OAuth 2.0 Authentication.

Note: If the From address is edited at the control panel to something different than that email account that is used to register for email, then the email job will be deleted.

LDAP

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

CONFIGURING LDAP SERVER SETTINGS

To configure LDAP server settings:

1. In the Embedded Web Server, click **Network > Protocols > LDAP > LDAP Server/Directory**.
2. For Server Information, type the backup LDAP server addresses and port numbers.
   The default port number is 389.
3. For LDAP Server, select the type of LDAP server.
4. In the Additional Setting area, specify settings, as needed:
   a. For Search Directory Root, type the search directory root path using Base DN format.
   b. For Login Credentials to Search Entries, select **Remotely Authenticated User** or **System**.
   c. If necessary, type the login name, then type and retype the password.
   d. For Maximum Number of Search Results, type the maximum number of addresses that can be returned matching the search criteria. Type a number between 5 and 100.
   e. For Search Timeout, select **Use LDAP Server Timeout** or **Specify Timeout**. If you select **Specify Timeout**, type a duration between 5 and 120 seconds.
   f. If your primary LDAP server is connected to other LDAP servers, to include the servers in your searches, for LDAP Referrals, select **Enabled**.
   g. For LDAP Referral Hop Limit, type the maximum number of consecutive LDAP referrals. Specify a limit between 1 and 5.
5. In the Name Search Condition area, select an option if necessary:
   - **Mapped Name Field**: This option specifies how the fields are mapped.
   - **Surname and Given Name Fields**: This option searches for the last name and first name of the user.
6. Click **Save**.

DEFINING USER MAPPINGS

LDAP servers provide different results to search queries depending on how user data is mapped. Editing the mapping allows you to fine-tune server search results.

Note: If you are using Internet Fax, ensure that the Internet Fax field is not set to No attribute type that can be used. This setting prevents the LDAP Address Book from appearing on the Internet Fax screen on the device control panel. For the Internet Fax setting, select **Mail**.

To define LDAP user mappings:

1. In the Embedded Web Server, click **Network > Protocols > LDAP > LDAP User Mappings**.

   The information that you entered on the LDAP Server tab is summarized in the Server Information area.

2. To send a test query, in the User Name field, type the name of the user for whom you want to search, then click **Search**.
   Any matching user information appears.

3. Click **Save**.

CONFIGURING LDAP CUSTOM FILTERS

To configure LDAP filters:

1. In the Embedded Web Server, click **Properties > Connectivity > Protocols > LDAP > Custom Filters**.
2. In the User ID Query Filter field, type the LDAP search string or filter that you want to apply.

   Note:

   - The filter defines a series of conditions that the LDAP search must fulfill to return the information you want.
   - The search string should be formatted as LDAP objects inside of parentheses. For example, to find the user with a sAMAccountName of Bob, type `(objectClass=user) (sAMAccountName=Bob)`.

3. For Email Address Book Filter, select **Enable Filter**.
4. In the Email Address Book Filter field, type the LDAP search string or filter that you want to apply.

   Note: Format the search string as LDAP objects placed inside parentheses. For example, to find all users that have an email attribute `(mail enabled)`, type `(objectClass=user) (mail=*)`.

5. For Fax Address Book Filter, select **Enable Filter**.
   Type the LDAP search string or filter that you want to apply.
6. For Internet Fax Address Book Filter, select **Enable Filter**.
   Type the LDAP search string or filter that you want to apply.
7. Click **Save**.

PERFORMING AN LDAP CONNECTION TEST

To perform the LDAP connection test:

1. In the Embedded Web Server, click **Network > Protocols > LDAP > Connection Test**.
2. Type a name for the test.
3. Click **Search**.

The test results appear in Search Result area.

POP3

Post Office Protocol, version 3 (POP3) allows email clients to retrieve email from remote servers over TCP/IP on network port 110. This device uses POP3 for the Internet Fax service.

To configure POP3:

1. In the Embedded Web Server, click **Network > Protocols > POP3**.
2. Type the appropriately formatted IP address, host name, and port number.
   The default port number is 110.
3. If required, for POP Receive Password Encryption, select **APOP Authentication**.
4. For User Name, type the name assigned to the device for logging in to the POP3 server.
5. Type a password. Retype the password.
6. To enable POP3 - SSL/TSL Communication, select **Enabled**.
7. For Polling Interval, type a value from 1 through 120 minutes.
   The default value is 10 minutes.
8. Click **Save**.

HTTP

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

ENABLING HTTP

HTTP is enabled by default. If you disable HTTP, before you can access the Embedded Web Server, re-enable HTTP at the device.

To enable HTTP:

1. In the Embedded System, log in as Administrator.
2. Click **Network > Protocols > HTTP**.
3. Touch **Port Status**, select **Enabled** or **Disabled**.

CONFIGURING HTTP SETTINGS

To configure HTTP settings:

1. In the Embedded Web Server, click **Network > Protocols > HTTP**.
2. For Maximum Connection per Port, change the number as needed.
   The default is 8.
3. To use cross-site request forgery protection, for CSRF Protection, select **Enabled**.
4. Type the port number.
   The default is 80.
5. For Secure HTTP Port Number, type the port number. When Secure HTTP is enabled, HTTP traffic is routed to this port.
   The default is 443.
6. For Connection Timeout, type the number of seconds until the connection times out.
7. Set the Alive Timeout to **1** second.
8. Select Device Certificates from the drop-down menu.
9. Click **Save**.

Proxy Server

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

A proxy server has two main purposes:

- The proxy server keeps any devices behind it anonymous for security purposes.
- The proxy server decreases the amount of time needed to access a resource by caching content, such as web pages from a web server.

Note: Proxy server settings are used for Xerox® Remote Print Services, formerly called SMart eSolutions.

To configure proxy server settings:

1. In the Embedded Web Server, click **Network > Protocols > HTTP > Proxy Server**.
2. In the General area, for Use Proxy Server, select **Enabled**.
3. For Proxy Server Setup, select an option:
   - **Same Proxy for All Protocols**: Select this option to apply the same proxy settings for HTTP and HTTPS.
   - **Different Proxy for Each Protocol**: Select this option to apply one proxy setting for HTTP and a different proxy setting for HTTPS.
   - **Use Automatic Proxy Configuration Script**: Select this option to use a specific script that you define.
   - **Automatically Detect Settings**: Select this option to detect proxy settings automatically.
4. For Addresses to Bypass Proxy Server, type any Web addresses or domains that you want to bypass the proxy server.
   For example, type the address of your company intranet site.
5. In the HTTP Server area, type the Server Name and Port Number. The factory default port number is 8080.

   Note: Ensure that the port number that you set for the device matches the port number that the server is configured to use for this proxy.
6. If your proxy server is configured to require authentication, for Authentication, select **Enabled**, then type a Login Name and Password. Retype the password.
7. To use a different proxy server for HTTPS, type the server information in the HTTPS Server area.
   The default port number is 8080.
8. To use an automatic proxy configuration script, type the URL for the script in the Use Automatic Proxy Configuration Script area.
9. Click **Save**.

IPP

Internet Printing Protocol (IPP) is used for remote printing and managing print jobs.

ENABLING IPP

To enable IPP:

1. In the Embedded Web Server, click **Network > Protocols > IPP**.
2. For IPP, select **Enabled**.
3. Click **Save**.

CONFIGURING IPP

To configure IPP printing:

1. In the Embedded Web Server, click **Network > Protocols > IPP**.
2. For Add Port Number (IPP), type the port number for IPP.
3. For Add Port Number (IPPS), type the port number for Secure IPP.
4. To enable the TBCP Filter, select **Enabled**.
5. To allow only one specific user to control or delete any print job, for Access Control, select **Enabled**.
6. To enable the Connection Timeout, select **Enabled**.
7. Type the Connection Timeout period. The default is 60 seconds.
8. Click **Print Mode**, select an option.
9. Click **Save**.

Universal Plug and Play Discovery

The Universal Plug and Play Protocol (UPnP) network protocol allows devices in a TCP/IP network to discover each other. Devices can establish connections for data sharing and communications. You can configure the device to use the Simple Service Discovery Protocol in the UPnP network. For details, refer to SSDP.

ENABLING UPNP

To enable UPnP:

1. In the Embedded Web Server, click **Network > Protocols > UPnP**.
2. For UDP, UPnP Discovery, and SOAP, select **Enabled**.
3. Click **Save**.

CONFIGURING UPNP

To configure UPnP:

1. In the Embedded Web Server, click **Network > Protocols > UPnP**.
2. Type a port number.
   Port 1900 is the standard port for UPnP.
3. Click **Save**.

SSDP

The Simple Service Discovery Protocol (SSDP) can be used in Universal Plug and Play networks. When SSDP is enabled on the printer, the printer advertises itself to other Universal Plug and Play (UPnP) clients in the network. For example, the printer advertises itself to personal computers.

To configure SSDP:

1. In the Embedded Web Server, click **Network > Protocols > SSDP**.
2. For SSDP Port Status, click **Enabled**.
3. For Valid Advertising Period, type an interval value from 60 through 4320 minutes.

   Note: The device advertises itself to other devices in the network using the advertising period. The default is every 180 minutes.

4. For IP Packet TTL, type a value from 1 through 10.

   Note: IP Packet TTL allows the device to reach Universal Plug and Play (UPnP) devices in other subnetworks. The time-to-live (TTL) value specifies the number of routers through which an SSDP message can pass.

5. Click **Save**.

WebDAV

Web-based Distributed Authoring and Versioning (WebDAV) is a set of extensions to HTTP that allow users to edit and manage files collaboratively on remote Web servers. WebDAV enablement is required to use Network Scan Utility 3.

ENABLING WEBDAV

To enable WebDAV:

1. In the Embedded Web Server, click **Network > Protocols > WebDav**.
2. For WebDAV, select **Enabled**.
3. Click **Save**.

CONFIGURING WEBDAV

To configure WebDAV settings:

1. In the Embedded Web Server, click **Network > Protocols > WebDAV**.
2. Type the Port Number.
3. Type the Connection Timeout period.
   The default is 30 seconds.
4. Click **Save**.

WSD

Web Services for Devices (WSD) is technology from Microsoft that provides a standard method for discovering and using network-connected devices. WSD is supported in all of the current Windows and Windows Server operating systems. WSD is one of several supported communication protocols.

ENABLING WSD

To enable the WSD protocol:

1. In the Embedded Web Server, click **Network > Protocols > WSD**.
2. To enable the WSD print service, for Port (Print from Desktop), select **Enabled**.
3. To enable the WSD scan service, for Port (Scan to Desktop), select **Enabled**.
4. Click **Save**.

CONFIGURING WSD

To configure the WSD protocol:

1. In the Embedded Web Server, click **Network > Protocols > WSD**.
2. Edit the following settings as needed:
   - **Port Number**: The default is 80.
   - **TBCP Filter**: To use the filter, select **Enabled**.
   - **Data Receive Timeout**: The default is 30 seconds.
   - **Notification Delivery Timeout**: The default is 8 seconds.
   - **IP Packet TTL**: The default maximum time to live is 1.
   - **Maximum Number of Subscribers**: The default is 50.
   - **PJL**: To enable PJL, select **Enabled**.
   - **Print Mode**: Select the Print Mode from the drop-down menu.
3. Click **Save**.

FTP

File Transport Protocol (FTP) is a standard network protocol that allows you to pass and manipulate files over a TCP/IP network. Several services running on your device, including Network Scanning and Fax, can use FTP as a filing service.

ENABLING FTP

To enable FTP:

1. In the Embedded Web Server, click **Network > Protocols > FTP Client**.
2. For FTP Client, select **Enabled**.
3. Click **Save**.

SETTING UP THE FTP TRANSFER MODE

To set up the FTP transfer mode:

1. In the Embedded Web Server, click **Network > Protocols > FTP Client**.
2. For Transfer Mode, select **Passive Mode** or **Active Mode**.
3. Click **Save**.

ENABLING AND DISABLING A SECURE FTP IN THE EMBEDDED WEB SERVER

1. In the Embedded Web Server or at the control panel, log in as a system administrator.
2. At the key operator login screen, enter the required Unique Function Code (SFR Key), with an asterisk (*) preceding the code. For more information, refer to Enabling Features at the Control Panel.
   - To enable Secure FTP, type `*3035414681`.
   - To disable Secure FTP, type `*3035414680`.

   Note: Ensure that you enter the correct SFR Key to enable or disable Secure FTP.
3. Click **Save**.

   The machine reboots automatically.

Once the system reboot is completed, ensure that you check the configuration report to verify if secure FTP is enabled.

By default, the system software configures secure FTP to use port 22 but the user can change the port number, if needed.

Bonjour Multicast DNS

Bonjour is a zero-configuration networking protocol developed by Apple to allow devices on a LAN to locate each other. When you enable Multicast DNS (Bonjour) on the printer, the device responds to mDNS calls. Any computer that runs the Apple Macintosh operating system Bonjour technology can discover the device on a network. Bonjour and IPP are required for Mopria® Mobile Printing, AirPrint®, and the Mac OS Print Center and Print Setup Utility. To use Bonjour, enable LPD and Raw TCP/IP printing on port 9100. For details, refer to IPP and Raw TCP/IP Printing.

ENABLING BONJOUR

To enable Bonjour:

1. In the Embedded Web Server, click **Network > Protocols > Bonjour**.
2. For Bonjour, select **Enabled**.
3. Click **Save**.

CONFIGURING BONJOUR

To configure Bonjour:

1. In the Embedded Web Server, click **Network > Protocols > Bonjour**.
2. For Host Name and Printer Name, type the appropriate names.
3. To use wide-area Bonjour, for Wide-Area Bonjour, select **Enabled**.
   Wide-area Bonjour allows devices to discover each other even if they are in different subnets on the network.
4. Click **Save**.

AirPrint

AirPrint is a software feature that allows you to print from wired or wireless Apple iOS-based mobile devices and Mac OS-based devices without the need to install a print driver. AirPrint-enabled printers allow you to print or fax directly from a Mac, an iPhone, iPad, or iPod touch.

To use AirPrint, enable and configure IPP and Bonjour.

Note:

- AirPrint and all of required protocols are enabled by default.
- Not all iOS applications support printing using AirPrint.
- Wireless devices must join the same wireless network as the printer. You can connect the printer by its wired network interface.
- The device that submits the AirPrint job must be on the same subnet as the printer. To allow devices to print from different subnets, configure your network to pass multicast DNS traffic.
- AirPrint-enabled printers work with all models of iPad, iPhone 3GS or later, and iPod touch third generation or later, running the latest version of iOS.
- The Mac OS device requires Mac OS 10.7 or later.

CONFIGURING AIRPRINT

To configure AirPrint:

1. In the Embedded Web Server, click **Network > Mobile Printing > AirPrint**.
2. In the General area, for AirPrint, select **Enabled**.
3. To use AirPrint on a USB connection, for USB Connection, select **Enabled**.
4. To specify device information, in the Bonjour area:
   a. For Printer Name, type the name of the printer as you want it to appear on the LAN, Wi-Fi, and Wi-Fi Direct networks.
   b. For Location, type the physical location of the printer.
   c. For Latitude and Longitude, type the geographical coordinates of the printer.
5. To use IPP authentication:
   a. In the IPP Authentication area, for Basic Authentication, select **Enabled**.
   b. Type a user name.
   c. In the Password and Retype Password fields, type a password, then retype the password.
6. To use a digital certificate:
   a. In the Certificate Setting area, click **Edit**.
   b. Create a certificate or upload a signed certificate. For details, refer to Digital Certificates.
7. To configure AirPrint, for software updates:
   a. In the Software Update area, for Manual Upgrade, click **Update**.

b. To check for software updates, in the Software Update area, click **Check Now**.

c. To specify when the printer checks for updates, in the Frequency area, select **Never**, **Daily**, **Weekly**, or **Monthly**.

d. To receive email notifications for the software upgrades, in the Email Notifications area, click **Setup**. In the Email Notification page, type up to three email addresses, then click **Save**.

8. To check life and status for toner, waste, and drum cartridges, in the Consumables area, click **Check Status**. To return to the AirPrint page.
9. To specify what happens when a data error occurs, for Print Job Handling when Data Error Occurs, select **Delete Print Job** or **Force Print Job**.
10. In Software Download area, select **Enabled** or **Disabled** from the list and click **Save**.
11. In Specify File for Software Update area, to browse the file, click **Browse** and click **Start**.
12. Click **Save**.

Mopria®

Mopria® is a software feature that enables users to print from mobile devices without requiring a print driver. To enable printing, users install the Mopria® app or plug-in available from the appropriate app store. When you enable and configure Mopria® on the printer, the required protocols IPP and Bonjour are enabled.

CONFIGURING MOPRIA®

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

Note: To enable printing, install the Mopria® app or plug-in available from the appropriate app store.

To configure Mopria®:

1. In the Embedded Web Server, click **Network > Mobile Printing > Mopria**.
2. Select **Enabled**.
3. Click **Save**.

Note: Mopria cannot be disabled when both the IPP port and Bonjour ports are enabled.

SOAP

Simple Object Access Protocol (SOAP) is an open-standard, platform-independent, XML-based messaging protocol that allows computers and networks that use different operating systems to exchange information. SOAP is used by other network protocols, including Universal Plug and Play Discovery.

To enable SOAP:

1. In the Embedded Web Server, click **Network > Protocols > SOAP**.
2. Select **Enabled**.
3. Click **Save**.

Security

This chapter contains:

Setting Up Access Rights 68
Local Authentication 70
Network Authentication 72
Authentication Using a Card Reader System 75
Authentication Common Access Card (CAC) 80
Controlling Access to Tools and Features 82
Enabling a Software Option 86
Digital Certificates 87
Secure HTTP and SSL/TLS 91
Configuring Domain Filtering 93
S/MIME 94
IPsec 95
802.1X 97
FIPS 140 Data Encryption 98
IP Filtering 99
Unbounded Ports 100
Audit Log 101
Setting System Timeouts 103
PDF Signatures 104
Restricting Access to Job Information 105
Restricting Service Representative Operations 107
USB Port Security 108

Setting Up Access Rights

OVERVIEW

You can control access to the device services and features by setting up authentication, authorization, and personalization.

AUTHENTICATION

Authentication is the process of confirming the identity of a user by comparing information provided by the user, such as user name and password, against another source of user information, such as a Lightweight Directory Access Protocol (LDAP) network directory. Users can be authenticated when accessing the control panel or when accessing the Embedded Web Server.

There are several ways to authenticate a user:

- **Local**: If you have a limited number of users, or do not have access to a Lightweight Directory Access Protocol (LDAP) network directory, you can add user information, such as user names and passwords, to the device internal database. You can then specify tools and feature access for all users. Users are authenticated and authorized when they log in at the control panel.
- **Network**: The device retrieves user information from an LDAP network directory to authenticate and authorize users when they log in at the control panel. Configure LDAP server settings before you configure authentication settings. The device can use any of the following protocols to communicate with your authentication server:

  - Kerberos (Solaris, or Windows 2000/2003)

  - SMB (Windows 2000/2003)

  - LDAP

- **Convenience**: For the Convenience level, users swipe a pre-programmed identification card at the control panel. To use this method, purchase and install a USB card reader and use an authentication server that supports the Xerox® Convenience Authentication API.
- **Card Reader**: To use this feature, purchase and install a magnetic or proximity card reading system, such as Xerox® Secure Access. To access the device, users swipe a pre-programmed identification card.

AUTHORIZATION

Authorization is the process of defining the services and features that users are allowed to access. For example, you can configure the device to allow a user to copy, scan, and fax, but not email. There are two types of authorization:

- **Locally on the Device (Internal Database)**: User login information is stored locally in the device internal User Information Database.
- **Remotely on the Network**: User login information is stored externally in a network database such as an LDAP directory.

PERSONALIZATION

Personalization is the process of customizing services for a specific user. If your network is connected to an LDAP server, the device can look up the home directory and email address for a user when using the Scan to Home or Email scanning features.

Note: Personalization is only available when the device is configured to use network authentication.

CONFIGURING PERMISSIONS FOR PERSONAL FAVORITES

1. In the Embedded Web Server, log in as administrator, then click **Permissions**, then in Roles area, click **Device Operation Roles**.

   Note: Before you can edit or create a Device User Role, the printer requires that you change the administrator password from its default value. If you have already changed the administrator password, you do not need to change it again. For details, refer to Changing the System Administrator Password.

2. For the user role for which you want to configure permissions, click **Edit Permissions**.
3. For Device Control Panel Permissions, select **Custom Permissions**.
4. Click **Setup**.

   The Custom Permissions Settings (Device Control Panel) page opens.

5. Click **Address Book**.
6. For Address Book Permissions, select **Allow**.
7. Click **OK**.
8. On the Custom Permissions Settings (Device Control Panel) page, scroll down and click **Personalization**.
9. For Customize Home Screen, Save Default Settings of Apps, and Edit Feature List, click **Allow**.
10. Click **OK**.
11. Click **Close**.
12. Click **Save**.

Local Authentication

SETTING UP LOCAL AUTHENTICATION

To configure local authentication:

1. In the Embedded Web Server, click **Permission > Authentication and Accounting**.
2. In Authenitication/Accounting Settings, click **Login Method**, then select **Local**.
3. Click **Save**.

DEFINING USER INFORMATION

Before you can define access rights for users, you must define user information. You can add information to, or edit, the device internal User Information Database, or you can specify a network database or LDAP server that contains user information. For details on network authentication and LDAP user information, refer to Network Authentication and LDAP.

EDITING THE USER INFORMATION DATABASE

To edit user information to the user database, refer to Editing the Account Settings for Individual Users.

SPECIFYING LOGIN REQUIREMENTS

To specify password requirements:

1. In the Embedded Web Server, click **Permissions > Authentication and Accounting > Network Accounting**.
2. In the Tracking Information click **Setup**.
3. To display text other than User ID, on the device control panel, in the User ID field, type the text.
4. Enter the Default Value
5. For Ask Users, click **Enabled**.
6. For Mask User ID, select an option:
   - **Enable**: This option shows user ID characters as asterisks on the control panel touch screen.
   - **Disable**: This option shows user ID characters as text on the control panel touch screen.
7. For Failed Access Log, click **Authentication Settings > Advanced Settings**, then click **Enable**. Type the number of allowed login attempts from 1-600. To allow an unlimited number of login attempts, type **0**.

   Note: If the maximum number of allowed attempts is exceeded, the device locks. Restart the device.
8. To allow users to log in without case sensitivity, for Input Settings, select **Non-Case Sensitive**.
9. In the Limit Login Attempts of System Administrator area, type the number of login attempts allowed for the system administrator. You can specify from 1-10 attempts. To allow an unlimited number of login attempts, type **0**.
10. In the Limit Login Attempts of Local User area, type the number of login attempts allowed for the system administrator. You can specify from 1-10 attempts. To allow an unlimited number of login attempts, type **0**.

11. In the Hide User ID area, select **Hide**, **Hide IC Card ID** or **Show**.
12. In Use Same User ID, select **Allow** or **Do Not Allow**.
13. In Disable Inactive Accounts, select **Off** or **On**.
14. In Use Domain Name for Print Client Authentication, select **Off** or **On**.
15. Click **Save**.

Network Authentication

If you have an LDAP server connected to your network, you can configure the device to retrieve user information from the LDAP directory when authenticating a user at the control panel.

SETTING UP NETWORK AUTHENTICATION

To set up network authentication:

1. In the Embedded Web Server, click **Permissions > Authentication and Accounting**.
2. In Authentication/Accounting Settings, for Login Method, select **Remote**, then click **Save**.
3. In Remote Authentication Settings, select **Kerbros** or **LDAP**.

CONFIGURING AUTHENTICATION SERVER SETTINGS FOR KERBEROS

To configure authentication settings for the Kerberos server:

1. In the Embedded Web Server, click **Properties > Security > Remote Authentication Servers > Kerberos Server**.
2. To enable the Kerberos validation services, for Server Certificate Validation, select **Enabled**.
3. For Kerberos Server 1, type the server information:
   a. Type the server name or IP address of your primary server.
   b. Type the Primary Server Port Number.
   c. Type the server name or IP address of your secondary server.
   d. Type the Secondary Server Port Number.
   e. Type the Domain Name of your server.
4. Type the server name, port name, and domain name of any additional Kerberos servers, as needed.
5. Click **Save**.

CONFIGURING AUTHENTICATION SERVER SETTINGS FOR SMB

To configure settings for the SMB server:

1. In the Embedded Web Server, click **Network > Protocols > SMB**.
2. For SMB Server Setup, select an option:
   - Port **Enabled**
   - Get WINS Server Address by DHCP **Disabled**
   - Type Primary WINS Server Address
   - Type Secondary WINS Server Address
   - For NetBios, click enable icon to **Enabled**
3. Click **Save**.

Note: It supports SMB 3.1.1.

CONFIGURING AUTHENTICATION SERVER SETTINGS FOR LDAP

To configure authentication settings for the Lightweight Directory Access Protocol (LDAP):

1. In the Embedded Web Server, login as administrator, click **Network > Protocols > LDAP**.
2. For LDAP, click**LDAP Authentication**.
3. For Authentication Method, select an option:
   - **Direct Authentication**: This method uses the user name and password, which the user types at the control panel, for authentication with the LDAP server.
   - **Authentication of User Attributes**: This method allows you to specify the Attribute of Typed User Name, which the user types at the control panel, and the Attribute of the Login User Name, which the device uses to authenticate the user.
4. If you selected Authentication of User Attributes:
   a. Type the Attribute of Entered User Name. This attribute is the LDAP attribute that corresponds to the information you want the user to type at the control panel. For example, if you want the user to type the mail address, type `mail`. You can type a maximum of 32 characters.
   b. Type the Attribute of Login User Name. This attribute is the login information that is registered on the LDAP server. You can type a maximum of 32 characters.
5. To add text to the user input before authentication, for Use Added Text String, select **Enabled**. For Text String Added to User Name, type the additional text string. For example, you can add your network domain name to the user name, and use this combined string for authentication.
6. Click **Save**.

SETTING THE CONVENIENCE LOGIN METHOD

For Convenience Authentication, the card uses either a magnetic strip or an RFID. A convenience authentication card is different from a Smart Card, which uses an embedded chip. Smart Card typically requires user name and password.

To set the Convenience login method:

1. In the Embedded Web Server, log in as administrator, then click **Permissions > Authentication and Accounting > Login Method**.
2. In Login Method, select **Convenience**.
3. Click **Save**.

   The Convenience Login window appears.
4. In the Server area, type the IP address and Path for the server. Also, define Timeout, Prompt Message, and Prompt Title.
5. To allow users to log in without a card, in the Alternate Login area, select **Allow**.

6. In the Accounting Codes area, select a source for the accounting code:
   - Obtain codes automatically from the server
   - Require users to manually enter codes at the device
7. To save the settings, click **Save**.
8. If you are prompted to restart the printer, click **Restart**.

INSTALLING A USB CARD READER PLUG-IN

The Convenience login method uses a USB card reader. To use the USB card reader, ensure that you install the cardreader_sig.jar plug-in. To obtain the plug-in, follow these steps:

1. Open a Web browser and navigate to www.support.xerox.com.
2. In the search field, type the name of your printer model.
3. In the search results, click the printer name.
4. Click **Drivers & Downloads**.
5. In the Utilities & Applications area, click **USB Card Reader Plug-In**.
6. Follow the instructions to download the file **Cardreader_plugin_with_signature.zip**.

The Cardreader_plugin_with_signature.zip file contains the cardreader_sig.jar file and instructions for how to install the plug-in. To install the cardreader_sig.jar file, follow the instructions.

Authentication Using a Card Reader System

SETTING UP AUTHENTICATION FOR A USB SMART CARD READER SYSTEM

To use the device with a card reader system other than Xerox® Secure Access, you must order and install a card reader kit. The kit includes hardware, software, and instructions for connecting and configuring your card reader system.

Before you begin:

- Install a Kerberos authentication server and configure with user accounts.
- Connect your card reader to the device.

Configure Network Authentication Settings

1. Configure network authentication. For details, refer to Network Authentication.
2. Configure Kerberos server settings. For details, refer to Configuring Authentication Server Settings for Kerberos.

Changing Smart Card Settings in the Embedded Web Server

Adding a Domain Controller

1. To add a domain controller, in the Domain Controller area:
   - Click **Add** or the **Plus** icon (**+**).
   - For Type, select the desired protocol.
   - For Address or Host Name, type the IP address or host name for the domain controller.
   - For Domain, type the domain name for the domain controller.
   - Click **OK**.
2. To validate the certificate returned by the domain controller, in the Validate area, click the **Enable** toggle button.

Setting a Timeout and Synchronizing with a Time Server

1. To set a timeout for the Smart Card reader, in the Options area, locate Timeout.
2. For Timeout, type the number of seconds that the printer waits for a response from the domain controller.
3. To synchronize the Smart Card reader with a time server:
   - In the Options area, click **SNTP**.
   - For Time Server Synchronization, click the **Enable** toggle button.
   - For Time Server Address, type the IP address for the time server.
   - For Time Synchronization Interval, type the number of hours when the Smart Card reader synchronizes with the server.
   - Click **Save**.

Completing the Smart Card Configuration

1. When finished, click **Save**.
2. If prompted to restart the printer, click **Restart**.

Setting Parameters for Login, Logout, and Password

Setting Login Parameters

You can adjust the settings for user logins from the printer control panel, including:

- Login name case-sensitivity
- Number of failed login attempts that are allowed
- If the login name appears on the user interface

To select login parameters:

1. In the Embedded Web Server, log in as administrator, then click **Permissions > Authentication and Accounting**.
2. In the Authentication Settings area, click **Advanced Settings**.
3. If you require a case-sensitive login name, in the Input Settings area, click **User ID for Login**, then select **Case Sensitive**.
4. To set a limit on the number of failed login attempts for users:
   - In the Authentication Settings area, click **Failed Log Access**.
   - To enable tracking of Failed Access Log, click **Enable**.
   - For Failed Attempts, type a number.
   - Click **Save**.
5. To set a limit on the number of failed login attempts for system administrators:
   - In the Authentication Settings area, click **Limit Failed Login Attempts of System Administrators**.
   - To enable tracking of failed login attempts, for Limit Login Attempts of System Administrators, click the **Enable**.
   - If you enabled Limit Login Attempts of System Administrators, for Failed Login Attempts, type a number.
   - Click **Save**.

Setting Logout Parameters

You can set the parameters for logging out from user account on the printer on the printer. You can set an immediate log out, or you can set the printer to display a confirmation message before logging out the users.

To select a logout parameter:

1. In the Embedded Web Server, log in as administrator, then click **Permissions > Authentication and Accounting**.
2. In the Logout Confirmation area, select an option.

Configuring Password Rules

1. In the Embedded Web Server, log in as administrator, then click **Permissions > Authentication and Accounting**, in Authentication Settings area, click **Password Policy**.
2. For Minimum Length, select **Set**.
3. For Number of Characters, type the number of characters allowed for passwords to access the printer.
4. For Maximum Length, type the maximum number of characters allowed for passwords to access the printer.
5. To specify Password Contains User ID, select **Allow** or **Do Not Allow**.
6. To specify Characters in Password, select **Numbers**, **Special Characters**, or **Numbers & Special Characters**.
7. To Change Password at First Login, select **On**.
8. In Rules When Changing Passwords, for Same Consecutive Characters in Old & New Passwords, select **No Restriction** or **Set Restriction**.
9. To set restrict characters in New Password, type the number of characters should be contained.
10. To Reuse Previous Password, select **Allow** or **Do not Allow**.
11. Click **Save**.

Local Authentication Settings for NIST 800-171 Related Functions

To improve critical cybersecurity infrastructure for organizations, the National Institute of Standards and Technology (NIST) in the United States created the Cybersecurity Framework (CSF). The system administrator can change the NIST 800-171r2 compatible settings through the Embedded Web Server. The NIST 800-171r2 related functions include the following features:

- Prevent reuse of user ID
- Auto disablement of user ID
- Password complexity
- Reuse of password
- Temporary password
- User account lock-out

For more information, refer to the User Guide for your printer model.

To configure the local authentication settings, do the following:

1. In the Embedded Web Server, click **Permissions > Authentication and Accounting**, then click **Password Policy**.

   The Passwords Policy page appears.

2. From the Rules When Changing Passwords, configure the following settings for NIST functions as needed:
   - **Same Consecutive Characters in Old & New Passwords**: To restrict the printer from reusing characters from the previous password, select **Set Restrictions**. For Minimum Number of Characters to Restrict, you can specify the minimum number of characters that can be reused, from 1–63. The default setting for this feature is **No Restriction**.
   - **Reuse Previous Password**: To prohibit the reuse of recent passwords, select **Don't Allow**. For Number of Previous Passwords that Cannot be Reused, you can specify the interval before a user can reuse a password, from 1–10. The default setting for this feature is **Allow**.
3. To save the settings, click **Save**.
4. For the new settings to take effect, at the prompt, click **Restart**.

Changing Smart Card Settings at the Control Panel

Enable Smart Card Settings

To enable Smart Card settings:

1. At the device control panel, log in as Administrator, press the **Home** button, For details, refer to Administrator Access at the Control Panel.
2. Touch **Settings > Device > Authentication/Accounting > Authentication/Security Settings > Authentication > User Details Setup > Use of IC Card**.
3. To enable the use of a smart card, touch **On**. To use the public key infrastructure for the certificates, touch **Enabled (PKI Only)**.
4. For Jobs Validated by Card, select **Copy**, **Print**, or **Fax/Scan**, as needed.

   Note: You can select any or all of the available options.
5. Touch **OK**.

Set the Smart Card Certificate Verification Mode

For additional security, you can set the device to validate a Smart Card against certificates stored on the device.

To set the Smart Card verification mode:

1. At the device control panel, log in as Administrator, press the **Home** button, For details, refer to Administrator Access at the Control Panel.
2. Touch **Settings > Device > Authentication / Security Settings > Authentication > User Details Setup > IC Card Certificate Verification**.
3. Touch **Enabled**.

   Note: Configure certificate revocation retrieval settings as necessary.
   - Ensure that the root CA and intermediate CA of the Smart Card certificate are stored on the device.
   - Ensure that the date and time settings on the device are correct for certificate validation.

Set the Smart Card Logout Timing

You can use this feature to set the way the user interfaces with the card reader. You can require the user to leave the Smart Card in the card reader while using the device. Alternatively, you can allow the user to access the system by tapping the Smart Card on the card reader. If the card does not remain in the card reader, the user is required to log out at the control panel.

To set the Smart Card Logout Timing:

1. At the device control panel, log in as Administrator, press the **Home** button, refer to Administrator Access at the Control Panel.
2. Touch **Settings > Device > Authentication/Accounting > Authentication/Security Settings > Authentication > User Details Setup > Contactless IC Card Logout Timing**.
3. Select **Log Out when Card is Removed** or **Log Out from Control Panel**.
4. Touch **OK**.

Authentication Common Access Card (CAC)

AUTHENTICATION COMMON ACCESS CARD (CAC) OVERVIEW

The Common Access Card (CAC) system is part of a Department of Defense initiative to increase the security of its facilities and critical information through the use of smart identification cards. Eventually, all department employees will use CAC cards to gain access to computers, networks, and buildings. In many cases, the department is requesting that same level of authentication at the device level also. When enabled on this device, Department of Defense employees use their CAC card to access the device for scan, fax, or copy functions, providing greater security and device management.



Xerox® CAC Enablement software supports a number of card readers and allows users to authenticate at the device. The card reader is connected to a USB port on the device.

SUPPORTED CARD TYPES

The CAC solution is compatible with most common CAC card types listed below.

- Axalto Pegasus 64K / V2
- Axalto Cyberflex 32K / V1
- Axalto Cyberflex 64K / V2
- Gemplus GemXpresso 64K / V2
- Oberthur 72K / V2
- Oberthur CosmopoIIC 32K / V1
- Oberthur D1 72K / V2 (contact-less and PIV)
- Gemalto GCX4 72K DI
- Oberthur ID One 128 v5.5 Dual
- Gemalto TOPDLGX4 144K

Note: Other card types may function with the Common Access Card (CAC)/Personal Identity Verification (PIV) ID system, but they have not been validated.

SUPPORTED CARD READERS

The following card readers are compatible with the CAC ID system:

- Gemplus GemPC USB SL
- Gemplus GemPC Twin

- SCM Micro SCR3310
- Panasonic ZU 9PS

Other USB CCID-compliant readers may function with the CAC ID system, but have not been validated.

Controlling Access to Tools and Features

CONTROLLING ACCESS FOR ALL USERS

Roles and Levels of Access

The printer recognizes two levels of access.

- **User Accounts**: This access level applies to anyone who has a login account with the printer. The login account can be on the printer or through a network server connected to the printer.
- **Anonymous User Permissions**: This access level applies to anyone using the printer without authentication, such as in a login or authenticated network access.

User Accounts are divided further into Roles. Roles assign privileges to perform tasks with the device. By default, the device defines two roles.

- Basic User: This role can be configured to have full privileges or a subset of privileges.
- System Administrator: This Role has full privileges.

You can edit the privileges assigned to the Basic User Role and create Roles with custom privileges.

Note: Users can belong to only one role.

The device provides two types of Roles.

- Device User Role: This role type defines the general functionality that is available to a user, such as copy, scan, and configuration functions.
- Printing User Role: This role type defines the printing functionality that is available to a user. You can specify times of day that printing is allowed, restrict color printing, or restrict which applications have access to the printer.

Note: More roles are available, depending on the printer settings for Authentication.

Adding a New Device User Role

1. In the Embedded Web Server, log in as administrator, then click **Permissions**, in Roles area, click **Device Operation Roles**.
2. For Device User Roles.
3. To create a role, click the **Plus** icon (**+**), then select **Create New Role**.
4. Type a name for the new Role.
5. Type a short description of the new Role.
6. In the Device Control Panel Permissions area, select the level of functionality that you want to assign to the role.
7. If you clicked Custom Permissions:
   - Click **Setup**.
   - For each application that you want to edit, click the application, select the needed access, then click **Allow**.

- When finished, click **Close**.

8. In the Internet Services Permissions area, select the level of functionality that you want to assign to the role.
9. If you clicked Custom Permissions:
   - Click **Setup**.
   - For each function that you want to edit, click the function, select the needed access, then click **Allow**.
   - When finished, click **Close**.
10. Click **Save**.

Creating a Custom Printing User Role

1. In the Embedded Web Server, log in as administrator, then click **Permissions > Roles > Print Roles**.
2. For Printing User Roles, click the **Plus** icon (**+**).
3. To create a role, select **Create New Role**.
4. Type a name for the new User Role.
5. Type a short description of the new User Role.
6. In the Printing Permissions area, select the level of functionality that you want to assign to the User Role.
7. Click **Save**.

Copying an Existing Device User Role

1. In the Embedded Web Server, log in as administrator, then click **Permissions > Roles > Device User Roles**.
2. For Device User Roles, click the **Plus** icon (**+**).
3. Click **Create New Role from Existing**.
4. Click the menu, then select the role that you want to copy.
5. To add members to the User Role, click **Yes**.
6. Click **Next**.
7. If you clicked Yes to add members:
   - Select the members that you want to add.
   - Click **Done**.
8. Type a name for the new User Role.
9. Type a short description of the new User Role.
10. In the Control Panel Permissions area, select the level of functionality that you want to assign to the role.
11. If you clicked Custom Permissions:
    - Click **Setup**.
    - For each application that you want to edit, click the application, select the needed access, then click **Allow**.
    - When finished, click **Save**.

12. In the Internet Services Permissions area, select the level of functionality that you want to assign to the Custom Printing User role.
13. If you clicked Custom Permissions:
    - Click **Setup**.
    - For each function that you want to edit, click the function, select the needed access, then click **Allow**.
    - When finished, click **Close**.
14. Click **Save**.

Copying an Existing Printing User Role

1. In the Embedded Web Server, log in as administrator, then click **Permissions > Roles > Print Roles**.
2. For Printing User Roles, click the **Plus** icon (**+**).
3. Click **Create New Role from Existing**.
4. Click the menu, then select the role that you want to copy.
5. To add members to the User Role, click **Yes**.
6. If you clicked Yes to add members:
    - Select the members that you want to add.
    - Click **Done**.
7. Type a name for the new User Role.
8. Type a short description of the new User Role.
9. In the Printing Permissions area, select the level of functionality that you want to assign to the role.
10. Click **Save**.

Editing a Device Operation Roles

1. In the Embedded Web Server, log in as administrator, then click **Permissions > Roles > Device Operations Roles**.
2. For the Role that you want to edit, click **Edit Permissions**.
3. Edit the settings as needed, then click **Save**.

Adding Members to a Role

1. In the Embedded Web Server, log in as administrator, then click **Permissions**.
2. In the User Accounts area, click the user to add to the Role.
3. To add the user to a Device Operation Role, in the Roles area, click **Device Operation Role**.
4. Select the Role where you want to add the user, then click **OK**.
5. To add the user to a Print Role, in the Roles area, click **Print Role**.
6. Select the Role where you want to add the user, then click **OK**.

Removing Members from a Role

To remove a member from a Role, use the steps for adding a member to a Role, then move the user to a different role. For details, refer to Adding Members to a Role.

Editing Anonymous User Permissions

1. In the Embedded Web Server, log in as administrator, then click **Permissions > Anonymous User Permissions > Edit Anonymous User Permissions**.
2. To edit the Device Operations:
   - Click **Device Operations**
   - Configure the settings as needed, then click **OK**.
3. To edit the Printing User Role functions:
   - Click **Printing User Role**.
   - Configure the settings as needed, then click **OK**.

Enabling a Software Option

You can use the Software Option feature to enable optional, purchased software features on your device.

To enable a Software Options:

1. In the Embedded Web Server, log in as administrator, then click **System > Security**.

   Note: The Software Option feature is visible only when HTTPS is enabled. For details, refer to Configuring HTTP Settings.

2. In the Security area, click **Software Options**.
3. For Software Options, type the authorization key that was provided with your purchased software kit.
4. Click **Save**.

Digital Certificates

A digital certificate must be installed on the device before you can enable secure HTTP (SSL). A digital certificate is a set of data used to verify the identity of the holder or sender of the certificate. A certificate includes the following data:

- Information about the person, organization, or computer to which the certificate is issued, including the name, location, email address, and other contact information.
- Certificate serial number
- Certificate expiration date
- Name of the certificate authority (CA) that issued the certificate
- A public key
- The digital signature of a certificate authority

INSTALLING A DIGITAL CERTIFICATE

There are three ways to install a certificate on the device:

- Create a Self-Signed Certificate. A Self-Signed Certificate is the result when the device creates its own certificate, signs it, and creates a public key for the certificate to be used in SSL encryption.
- Create a request to have a certificate authority (CA), or a server functioning as a certificate authority sign a certificate and then upload the certificate to the device. An example of a server functioning as a CA is Windows Server running Certificate Services.
- Install a trusted root certificate created by a CA.

Note: Installing a self-signed certificate is less secure than installing a certificate signed by a trusted CA. However, if you do not have a server functioning as a certificate authority, this is your only option.

CREATING A SELF-SIGNED CERTIFICATE

1. If necessary, enable S/MIME capability for the self-signed certificate. For details, refer to Assigning a Name and Location to the Device.
2. In the Embedded Web Server, click **System > Security**, in the Certificates area, click **Certificate Settings**.
3. Click **Create New Certificate**.
4. Select **Generate Self-Signed Certificate**.
5. Select a Digital Signature Algorithm.
6. Select a Public Key Size and type the name of the Issuer.
7. For Validity Period, type the number of days, **1-9999**, until the certificate expires.
8. Click **Start**.

CREATING A REQUEST

To create a request:

1. In the Embedded Web Server, click **System > Security**, in the Certificates area, click **Certificate Settings**.
2. Click **Create**.
3. Select **Create Certificate Signing Request (CSR)**.
4. Fill out the form with the Digital Signature Algorithm, Public Key Size or Elliptic Curve, 2-Letter Country Code, State/Province Name, Locality Name, Organization Name Organization Unit, and Common Name.
5. Click **Start**.
6. Values from the form are used to generate a Certificate Signing Request.
7. When the process is complete, you are prompted to save the Certificate Signing Request. Right-click the link and save the **csr.pem** file to your computer.
8. Email the file to a trusted certificate authority for signing.

Note: If you want to use SSL/TLS for SMTP communication, for SMTP - SSL / TLS Communication, select a method that your server supports.

UPLOADING A CERTIFICATE

When a signed certificate is received back from a trusted certificate authority (CA), you can upload the certificate to the device. You can also upload certificates, root certificates, and intermediate CA certificates to establish a complete chain of trust.

To upload a certificate:

1. In the Embedded Web Server, click **System > Security**, in the Certificates area, click **Certificate Settings**.
2. Click **Import**.
3. If the certificate is password-protected, type the password, then retype the password.
4. Click **Browse**, navigate to the signed certificate in .crt format, then click **Open** or **Choose**.
5. Click **Start**.

Note: The signed certificate must match the CSR created by the device.

MANAGING CERTIFICATES

To view information about the certificates installed on the device, or specify the certificate to use for S/MIME, SSL, and IPSEC:

1. In the Embedded Web Server, click **System > Security** in Certificates Area, click **Certificate Settings**.
2. To filter the display, for Category, Certificate Purpose, and Certificate Order, select the appropriate options.
3. Click **Display the list**.
4. Select a certificate from the list to view Certificate Details.
5. To set the certificate as the primary certificate, click **Use this certificate**. If this option is not available, then the selected certificate has expired or is not valid. All certificates in the certification path (chain of trust) must be installed on the device and must be valid.
6. To remove the certificate, select the certificate, then click **Delete**.

7. To save the certificate to your computer, click the certificate and in Certificate Details area, click **Export**.

CERTIFICATE REVOCATION RETRIEVAL SETTINGS

To configure certificate revocation retrieval settings:

1. In the Embedded Web Server, click **System > Security > Certificate Revocation Settings**.
2. In the General area, for Level of Certificate Verification, select an option:
   - **Low**: The revocation status of certificates is not checked. The device verifies that the certificate has not expired and that the certificate issuer and signature are valid.
   - **Medium**: The revocation status of certificates is checked. If the certificate status cannot be obtained due to a network error, the certificate is still considered valid.
   - **High**: The revocation status of certificates is checked. The certificate is only considered valid after successfully verifying that the certificate has not been revoked.
3. Select the Retrieval of Certificate Status, **By Retrieving CRL** or **By OCSP**.
   - If you select **By OCSP**:
     1. In the OCSP area, for Send Query to OCSP Responder With, select **URL as Specified in Certificate** or **URL as Specified by Administrator**.
     2. For URL of OCSP Responder, type the required URL.
     3. For OCSP Communication Timeout, type the time in seconds that the device waits for information about certificate revocation. The permitted range is 5–60 seconds.
   - If you select **By Retrieving CRL**:
     1. If necessary, in the CRL area, for Auto Retrieval of CRL, select **Enabled**.
     2. For CRL Retrieval Timeout, type the time in seconds that the device waits for information about certificate revocation. The permitted range is 5-60 seconds.
4. Click **Save**.

ENABLING AUTOMATIC SELF-SIGNED CERTIFICATES

When no Device Certificate is available, this feature creates a self-signed certificate, automatically.

1. In the Embedded Web Server, log in as administrator, then click **System > Security**.
2. In the Certificates area, click **Automatic Self-Signed Certificate Creation**.
3. Select **On**, then click **Save**.

ENABLING CERTIFICATE PATH VALIDATION

1. In the Embedded Web Server, log in as administrator, then click **System > Security**.
2. In the Certificates area, click **Certificate Path Validation**.
3. Select **On**, then click **Save**.

CONFIGURING THE PRINTER FOR IC OR SMART CARDS

1. In the Embedded Web Server, log in as administrator, then click **System > Security**.
2. In the Certificates area, click **PKI Functions of IC Cards**.
3. Select **On**, then click **Save**.
4. In the Certificates area, click **IC Card Certificate**.
5. Toggle **Enable**.
6. Enter Object Identifier of Authentication Certificate code.
7. Enter Object Identifier of Signing Certificate code.
8. Enter Object Identifier of Encryption Certificate code.
9. Click **Save**.

For more information about configuring a Common Access Card system on your device, go to www.support.xerox.com, enter your printer name, then click **Documentation**. Select and download the documentation required.

Secure HTTP and SSL/TLS

You can encrypt all data sent over HTTP by establishing an encrypted SSL connection. You can enable SSL encryption for the following services:

- Configuring the device in the Embedded Web Server
- Printing from the Embedded Web Server
- Printing using IPP
- Managing scan templates
- Network scanning
- Network accounting

Before you begin:

- Install a digital certificate. For details, refer to Installing a Digital Certificate.
- Ensure that the date and time on the device are configured correctly. The date and time are used to set the start time for self-signed certificates.

CONFIGURING SETTINGS FOR SSL/TLS

After configuration, the latest version of software supports TLS 1.3. Changes to the TLS version require a device restart.

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.

1. In the Embedded Web Server, log in as administrator, then click **System > Security**.
2. In the Network Security area, click **SSL/TLS Settings**.
3. Select at least one SSL/TLS protocol.
4. To enable SSL/TLS communication with HTTP, for HTTP – SSL/TLS Communication, click the **Enable** toggle button.
5. To specify a device certificate for the server, click **Device Certificate – Server**, then select a certificate.
6. If needed, for HTTP – SSL/TLS Port Number, type a port number.
7. To enable SSL/TLS communication with LDAP, for LDAP – SSL/TLS Communication, click the **Enable** toggle button.
8. To enable SSL/TLS communication with SMTP, click **SMTP – SSL/TLS Communication**, then select an option.
9. To enable SSL/TLS communication with POP3, for POP3 – SSL/TLS Communication, click the **Enable** toggle button.
10. To enable SSL/TLS communication with ThinPrint, for ThinPrint – SSL/TLS Communication, click the **Enable** toggle button.
11. To specify a device certificate for the client, click **Device Certificate – Client**, then select a certificate.
12. To verify certificates on a remote server, for Verify Remote Server Certificate, click the **Enable** toggle button.

13. Click **Save**.

Configuring Domain Filtering

You can specify up to 50 domains to allow or block.

To configure domain filtering:

1. In the Embedded Web Server, log in as administrator, then click **System > Security**.
2. In the Network Security area, click **Domain Filtering**.
3. To allow specific domains, click **Allow Domains**.
   - Enter up to 50 domains to allow.
   - To delete domains from the list, click the **Trash** icon.
4. To block specific domains, click **Block Domains**.
   - Enter up to 50 domains to block.
   - To delete domains from the list, click the **Trash** icon.
5. To disable domain filtering, select **Off**.
6. When finished, click **Save**.

S/MIME

Secure/Multipurpose Internet Mail Extensions (S/MIME) is a standard for public key encryption and signing of email encapsulated in MIME.

Before you begin:

- Enable SSL/TLS.
- Install an S/MIME certificate and all certificates in the certification path (chain of trust) for the S/MIME certificate. The S/MIME certificate must be in PKCS #12 format, and the email address in the certificate must be the same as the device email address.
- Enable S/MIME Communication on the SSL/TLS Settings page.

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 for the following protocols:

- DHCP v4/v6 (TCP and UDP)
- DNS (TCP and UDP)
- FTP (TCP)
- HTTP (Scan Out, TCP port 80)
- HTTPS (Scan Out, TCP port 443)
- HTTPS (Web Server, TCP port 443)
- ICMP v4/v6
- IPP (TCP port 631)
- LPR Print (TCP port 515)
- Port 9100 Print (TCP port 9100)
- SMTP (TCP/UDP port 25)
- SNMP (TCP/UDP port 161)
- SNMP Traps (TCP/UDP port 162)
- WS-Discovery (UDP port 3702)
- Up to 10 additional services

CONFIGURING IPSEC

Note: Before you can enable IPSec, ensure the HTTP (SSL) is enabled with an installed digital certificate.

To configure Internet Protocol security communications:

1. In the Embedded Web Server, click **Network > Protocols > IPSec**.
2. For Protocol, select **Enabled**.
3. For IKE Authentication Method, select **Preshared Key** or **Digital Signature**.
4. If you selected Preshared Key, type the Preshared Key, then to verify, retype the key.
5. For IKE SA Lifetime and IPSec SA Lifetime, type the values in minutes:
   - IKE SA Lifetime: 5–28800 minutes
   - IPSec SA Lifetime: 300–172800 minutes

   Note: Ensure that you set the IPSec SA Lifetime to a shorter period of time than the setting for IKE SA Lifetime.
6. Select the DH Group type.
7. If necessary, enable PFS.

8. Enter the Specific Destination IPv4 Address and the Specific Destination IPv6 Address.
9. To restrict the device from communicating with devices that are not using IPSec, for Communicate with Non-IPsec Device, select **Disabled**.
10. Click **Save**.

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 device 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 to be used in an 802.1X-secured network.

Before you begin:

- Ensure your 802.1X authentication server and authentication switch are available on the network.
- Determine the authentication method supported by the server.
- Create a user name and password on your authentication server.
- Ensure that the device can be offline for several minutes. Changing and applying 802.1X settings causes the device to restart.

CONFIGURING 802.1X

To configure 802.1x network settings:

1. In the Embedded Web Server, log in as administrator, then click **Network**.
2. In the Connections area, click **Ethernet**.
3. In the 802.1X area, click **Setup**.
4. For Enable 802.1X, click the toggle button.
5. Click **Authentication Method**, then select an option.

   Note: EAP-TTLS is available if the device is configured to use EAP-TTLS.

6. For Certificate Verification, click the toggle button.
7. For the login credentials, type values for User Name (Device Name), Password, and Retype Password.
8. Click **Save**.

FIPS 140 Data Encryption

All data that is stored on and transmitted by the device is encrypted. Some services and protocols, such as SMB and the PDF Direct Print service, do not use an encryption method that complies with government standard FIPS 140. You can warn users with a control panel message when data is about to be transmitted that is not encrypted to FIPS 140 standard. For details, refer to the device Security White Paper at the www.xerox.com/support.

To enable the data encryption warning message:

1. In the Embedded Web Server, click **System > Security**, in Network Security area, click **FIPS 140**.
2. For FIPS 140, select **On**.
3. Click **Save**.

Note: FIPS 140 encryption does not apply to the SMB protocol or to the PDF Direct Print Service.

Note: Support for FIPS 140 is compliant with the SFTP protocol.

IP Filtering

You can prevent unauthorized network access by only allowing data to be transmitted to and from specific IP addresses and ports.

CREATING AN IP FILTER RULE

To create an IP filter rule:

1. In the Embedded Web Server, click **System > Security > IP Filtering**.
2. For IPv4 Filtering or IPv6 Filtering, select **Enabled**.
3. For the option that you enabled, click **Add**.
4. In the Allowed IP Address / Subnet Mask area, type the Source IP Address / Subnet Mask, click **Add**. This is the IP address of the computer or device that you want to allow to access the printer.
5. For Source IP Mask, type a number for the filter rule.

   For IPv4, the range of 0–32 corresponds to the 32-bit binary number that comprises IP addresses. 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.

   For IPv6, the range of 0–128 corresponds to the 128-bit binary number that comprises IP addresses. For example, a mask of /64 represents a 64-bit mask, which defines a single IPv6 subnet.
6. Click **Save**, then follow the prompts to restart the device.
7. Refresh your browser, then navigate back to the IP Filtering page.
8. For IP Filter Rule List, select the rule that you created in the first part of the process.
9. Select your rule in the list, then click **Save**.

To edit or delete an existing rule, select the rule, then click **Edit** or **Delete**.

Note: To edit or delete an existing rule, click **Edit** or **Delete**.

Unbounded Ports

The unbounded port feature provides printer security by allowing you to register the ports that are permitted to communicate with the device.

ADDING AN UNBOUNDED PORT

To add a port that is allowed to communicate with the device:

1. In the Embedded Web Server, click **System > Security**, in the Network Security area, click **Unbounded Port**.
2. Click **Add**.
3. Type the port number.
4. For Port Location, select **Source** or **Destination**.
5. For Protocol, select **TCP** or **UDP**.
6. Click **Save**.

EDITING AN UNBOUNDED PORT

To edit an unbounded port:

1. In the Embedded Web Server, click **System > Security > Unbounded Port**.
2. Select an item in the Unbounded Port List, then click **Edit**.
3. Edit the port number, destination, and protocol, as needed.
4. Click **Save**.

DELETING AN UNBOUNDED PORT

To delete an unbounded port:

1. In the Embedded Web Server, click **System > Security > Unbounded Port**.
2. Select an item in the Unbounded Port List, then click **Delete**.
3. Click **Save**.

Audit Log

When the Audit Log feature is enabled, the device begins recording events that happen on the device. You can download the Audit Log as a tab-delimited text file and review it to find security breaches and assess the device security.

ENABLING AUDIT LOG

Note: Secure HTTP (SSL) must be enabled before you can enable the Audit Log. For details, refer to Secure HTTP and SSL/TLS.

To enable the Audit Log:

1. In the Embedded Web Server, click **System > Logs > Audit Log**.
2. For Audit Log, select **Enabled**.
3. Click **Save**.

SAVING AN AUDIT LOG

1. In the Embedded Web Server, click **System > Logs > Audit Log**.
2. For Export Audit Log, click **Export**.
   It will be saved as **auditfile.txt** file to your computer automatically.
3. Open the file in an application that can read a tab-delimited text file.

INTERPRETING THE AUDIT LOG

The Audit Log is formatted into columns:

- **Log ID:** A unique value that identifies the event.
- **Date:** The date that the event happened in mm/dd/yy format.
- **Time:** The time that the event happened in hh:mm:ss format.
- **Audit Event ID:** The type of event. The number corresponds to a unique description.
- **Logged Events:** An abbreviated description of the type of event.
- **User Name:** User Name, Job Name, Computer Name, Device Name, Folder Name, or Accounting Account ID (when Network Accounting is enabled).
- **Description:** More information about the Logged Event. When the Logged Event is System Status for example, one of the following can appear:
  - Started normally (cold start)
  - Started normally (warm start)
  - Shutdown requested
  - Image Overwriting started
- **Optionally Logged Items:** Other information recorded when the event occurs, such as log in and authentication access method.

Note:

- For a Network Scanning scan job, an audit log entry is recorded for each network destination within the job.
- For Email jobs, an audit log entry is recorded for each SMTP recipient within the job.
- To record user names in the Audit Log, configure network authentication.

Setting System Timeouts

1. In the Embedded Web Server, log in as administrator, then click **System > Timeouts**.
2. In the Reset Device Control Panel area, for System Timeout, type the number of seconds that the printer remains idle before the control panel goes into Standby mode.
3. In the Reset Device Website area, for Device Website Timeout, type the number of minutes that the printer remains idle before the Embedded Web Server goes into Standby mode.
4. Click **Save**.

PDF Signatures

You can add a digital signature to PDF documents that are created by the device scan feature. The signature uses the information in an S/MIME digital certificate.

Before you begin:

- Install an S/MIME digital certificate.
- Enable secure HTTP (SSL) and S/MIME communication. For details, refer to Secure HTTP and SSL/TLS and S/MIME.

To set digital signatures:

1. In the Embedded Web Server, click **Apps > Email > PDF Signature Settings**.
   PDF Signature Settings are also available in **Apps > Scan > PDF Signature Settings**.
2. For PDF Signature, select an option from the list.
3. For PDF Signature Hash Algorithm, select an algorithm.
4. For Signing Certificate, select **Device Certificate** or **IC Card Certificate**.
5. For **Device Certificate**, select an email address for the device certificate.
6. Click **Save**.

Restricting Access to Job Information

You can control how job information displays at the control panel when the user touches the **Jobs**.

HIDING OR PASSWORD PROTECTING COMPLETED JOB INFORMATION

To control access to completed job information:

1. In the Embedded Web Server, login as Administrator, click **Jobs > Job Settings > Completed Jobs View**.
2. For Completed Jobs View, select an option:
   - **Allow Job Veiwing at All Times**: This option users to view completed jobs
   - **Require Login to View Jobs**: This option allows users to view completed jobs only when they are logged in.
   - **Hide**: This option prevents users from seeing completed job information.
3. If you select Require Login to View Jobs, for Access To, select an option:
   - **All Jobs**: This option allows users to view all completed jobs.
   - **Jobs Run By Logged-in User Only**: This option allows users to view only jobs completed by logged-in users.
4. For Hide Job Details, select an option:
   - **Yes**: This option allows users to view only basic information for completed jobs.
   - **No**: This option allows users to view all information for completed jobs.
5. Click **Save**.

HIDING ACTIVE JOB INFORMATION

To hide or show active job information:

1. In the Embedded Web Server, Login as Administrator, then click **Jobs** tab, in Jobs area select **Active Jobs**.
2. For Hide Job Details, select an option:
   - To hide job details, select **Yes**.
   - To show job details, select **No**.
3. Click **Save**.

ALLOWING OR RESTRICTING JOB OPERATIONS

To control the job operations that a user can perform:

1. In the Embedded Web Server, login as Administrator click **Jobs > Job Status Default > Job Operation Restrictions**.
2. For Pause / Cancel, select **All Users**, **Administrator Only**, or **Job Owner and Administrator**.
3. For Continue / Edit Scan, select **All Users** or **Job Owner and Administrator**.
4. For Continue / Edit Print, select **All Users** or **Job Owner and Administrator**.
5. For Promote Print Job, select **All Users** or **Job Owner and Administrator**.

6. Click **Save**.

Restricting Service Representative Operations

You can allow a service representative full access to the device, or you can restrict access to the following operations:

- Delete all data
- Image log control
- Print universal unique ID
- Data encryption
- Encryption key for confidential data
- Service representative restricted operation
- SSL / TLS settings
- S/MIME settings
- IPsec settings
- System administrator settings
- Maximum login attempts by the system administrator
- Overwrite hard drive
- Creating or changing users with system administrator rights
- Changing SNMPv3 settings

If you restrict access, you can specify a password for the service representative operations.

Caution:

- If you lose the system administrator user ID and password, and need to recover the device, a repair can be required.
- If you lose the system administrator user ID and password, you cannot change these restrictions.
- If you lose the password, the service representative cannot perform maintenance if an error occurs on the device.

SETTING UP SERVICE REPRESENTATIVE RESTRICTIONS

To restrict the access of a service representative:

1. In the Embedded Web Server, click **System > Security > Service Representative Operation Settings**.
2. For Operation Restriction, select **Enabled**.
3. To set a Maintenance password, type and retype the password.
4. Click **Save**.

USB Port Security

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

ENABLING OR DISABLING USB PORTS

1. In the Embedded Web Server, log in as administrator, click **System**, then in General area, click **USB**.
2. To enable or disable a USB port, for USB Port, click the toggle button.
3. For Serial Number to Display During Plug and Play area, select **USB's Media Serial Number**.
4. For Device Front, toggle the **Enable** icon for USB-A (Standard).
5. For Device Rear, toggle the **Enable** icon for USB-A and USB-B.
6. For USB-B, toggle the **Enable** icon.
7. For PJL, toggle the **Enable** icon.
8. For Print Mode, select an option from the print mode.
9. For Auto Eject Time, enter the eject time from 5 through 1275 seconds.
10. For Adobe Communication Protocol, select an option from the list.
11. For PostScript Wait Timeout (RAW Mode), toggle the **Enable** icon.
12. Click **Save**.

Note: Disabling a USB port also disables a USB card reader connected to the port.

Printing

This chapter contains:

General Printer Settings 110
Language Emulation Settings 113
Managing Banner Page Printing Options 115
Print Service Settings 117
UNIX®, Linux®, and AS/400 Printing 120

General Printer Settings

CHANGING THE TRAY SETTINGS

The tray settings determine how the printer manages the paper trays.

- Tray Mode: This option determines if users are prompted to confirm or modify paper settings when they insert a paper tray into the printer. There are three modes: Fully Adjustable, Dedicated, and Bypass.
  - In Fully Adjustable mode, users can change the paper settings at the control panel each time they insert a paper tray into the printer, or insert paper into the Bypass Tray.
  - In Purpose-Specific mode, only a system administrator can use the Embedded Web Server or control panel to change the settings for paper features. When a printer tray is set to Dedicated mode, users cannot change the tray settings.
  - In Bypass mode, the printer prompts users to confirm or modify paper settings when paper is loaded into the Bypass Tray. If the Bypass Tray contains paper, Bypass mode sets the Bypass Tray as the default tray for all print jobs without a specified tray.
- Auto Paper Select: This option designates a tray as available for all jobs that use the type of paper in the tray, and for print jobs that do not specify a tray.
- Priority: This option sets a hierarchy for the paper trays. When more than one tray has Auto Select enabled and contains paper that matches the job, the printer uses the highest priority tray. When the Priority 1 tray is empty, the printer uses the Priority 2 tray, and so on, until all trays are empty or refilled.

To change the tray settings from the printer control panel:

1. At the printer control panel, log in as administrator, then press the **Home** button.
2. Touch **Device > Paper Trays**.
3. Select a tray.
4. To set the level of restriction on the paper tray, touch **Tray Mode** and select an option.
5. If you selected Dedicated for Tray Mode, configure the paper size, type, and color.
6. To allow the printer to select which paper tray to use, for Auto Select, enable the toggle button.
7. To select a priority level for this paper tray, for Priority, to increment priority, touch the **Plus** icon (**+**) or to decrement the priority, touch the **Minus** icon (**–**).
8. Touch **OK**.

To change the tray settings from the Embedded Web Server:

1. In the Embedded Web Server, log in as administrator, then click **Home**.
2. In the Trays area, click a tray icon.
3. To set the level of restriction on the paper tray, click **Tray Mode**, then select an option.
4. If you enabled **Purpose-Specific Tray Mode**, configure the paper size, type, and color.
5. To allow the printer to select which paper tray to use, for Auto Paper Select, click the **Enable** toggle button.
6. To enable Auto Tray Switching, select **Enabled**.

7. To select a priority level for the paper tray, click **Priority**, then select an option.
8. Click **Save**.

CONFIGURING POLICIES FOR PRINT JOBS

The printer provides the following policies for print jobs:

- Auto Job Promotion: This policy manages jobs that cannot start because the needed paper is not available. When Print Around is off, the printer blocks all print jobs until the resource is available. When Print Around is on, a print job is held for resources, and other jobs that do not need the same resource are allowed to print.
- Stored Print Jobs: This policy allows you to set a minimum length of for passcodes that are assigned to stored jobs, and to delete stored jobs after a specified period.

To configure general polices for print jobs:

1. In the Embedded Web Server, log in as the system administrator, then click **Jobs > Job Settings**.
2. In the Auto Job Promotion area:
   - To enable Print Around, click the **Enable** toggle button.
   - To delete held jobs, select **Automatically Delete Held Jobs**, then click **On**.
   - In the Held Job Retention Period, specify the amount of time that the printer holds a job for attention before it deletes the job from the queue.
3. To show or hide the jobs, for Active Jobs View and Completed Job View, select **On** or **Off** from the option.
4. In the Stored Print Job Settings area:
   - To set a minimum length for passcodes assigned to stored jobs, for Minimum Number of Passcode Digits, type a number.
   - Configure the time period that the printer waits before it deletes the stored jobs.
5. To enable the Printer Lockout, click **Edit**, then click **Enable** toggle button. Choose the Printer Lockout Time accordingly, then click **Save**.
6. To notify job completion by Email, click **Edit**, select the jobs, then click **Save**.
7. Click **Save**.

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.

To enable Print From USB:

1. In the Embedded Web Server, log in as administrator, then click **Apps > USB**.
2. In the Enable Feature area, for Print, select **Enable**.
3. To activate the changes, at the prompt, click **Restart Now**.

SETTING PAPER SIZE PREFERENCES

1. In the Embedded Web Server, log in as administrator, then click **System > Measurements**.
2. Select **Inches** or **Millimeters**.

Language Emulation Settings

The device can be used with SAP® Enterprise Resource Planning (ERP) software applications. In the SAP® environment, users and automated processes create documents to support business functions. For example, to dispatch goods from a warehouse requires packing lists and goods labels. To support users and processes, you can create up to 20 logical printers. Each logical printer has print settings for the different documents produced.

CONFIGURING POSTSCRIPT LANGUAGE EMULATIONS

To configure PostScript language emulations:

1. In the Embedded Web Server, click **System > Language Emulations > PostScript**.
2. For Logical Printer Number, type a number, then click **Edit**.
3. In the PostScript Logical Printer Settings area, set the printer settings as needed.
4. For Memory Settings, select **Factory Settings** or **Logical Printer Number**.
5. Set the user details, then enable the native mode of the print driver, as needed.
6. Click **Save**.

CONFIGURING PCL® 6/5E LANGUAGE EMULATIONS

To configure PCL® 6/5e language emulations:

1. In the Embedded Web Server, click **System > Language Emulations > PCL 6/5e**.
2. In the PLC 6/5e Settings area, set the printer settings as needed.
3. Click **Save**.

CONFIGURING TIFF AND JPEG LANGUAGE EMULATIONS

To configure TIFF and JPEG language emulations:

1. In the Embedded Web Server, click **System > Language Emulations > TIFF/JPEG**.
2. For Logical Printer Number, type a number, then click **Edit**.
3. In the TIFF/JPEG Logical Printer Settings area, set the printer settings as needed.
4. For Memory Settings, select **Factory Settings** or **Logical Printer Number**.
5. Click **Save**.

CONFIGURING HP-GL/2 LANGUAGE EMULATIONS

To configure HP-GL/2 language emulations:

1. In the Embedded Web Server, click **System > Language Emulations > HP/GL-2**.
2. For Logical Printer Number, type a number, then click **Edit**.
3. In the HP-GL/2 Logical Printer Settings area, set the printer settings as needed.

4. For Memory Settings, select **Factory Settings** or **Logical Printer Number**.
5. Click **Save**.

CONFIGURING PDF LANGUAGE EMULATIONS

To configure PDF language emulations:

1. In the Embedded Web Server, click **System > Language Emulations > PDF**.
2. For Switch Decomposer, select **PDS Bridge** or **PS**.
3. In Quantity, enter a value from 1 through 999.
4. Select Paper Size from the drop-down menu.
   The default setting is **Auto Detect**.
5. Select Output Color from the drop-down menu.
   The default setting is **Auto Detect**.
6. To print on the sides, select **1 Sided** or **2 Sided**.
7. Select Printer Mode from the drop-down menu.
   The default setting is **Standard**.
8. For Collated, select **On** or **Off**.
9. To protect the file, enter the Password.
10. 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.

Note: For a banner page to print, banner page printing must be enabled in the print driver. Banner page printing must also be enabled at the control panel or in the Embedded Web Server.

ENABLING BANNER PAGE PRINTING IN THE EMBEDDED WEB SERVER

1. In the Embedded Web Server, click **System > Defaults > Print Settings**.
2. In the Banner Pages area, for Sensing Separator Page, select **Enabled**.
3. For Banner Pages, select **Start Page**, **End Page**, or **Start Page & End Page**.
4. For Banner Page Tray, select the tray from which the banner page prints.
5. To allow banner page printing to be enabled from the print driver, for Allow Print Driver to Override, select **Enabled**.
6. Click **Save**.

ENABLING BANNER PAGE PRINTING FROM THE CONTROL PANEL

To enable banner page printing from the control panel:

1. At the device control panel, log in as Administrator, press the **Home** button. For details, refer to Administrator Access at the Control Panel.
2. Touch **Device > System Settings > App Settings > Print Settings > Other Settings**.
3. Touch **Banner Pages**.
4. Touch **Start Page**, **End Page** or **Start Page & End Page**.
5. To allow banner page printing to be enabled or disabled from the print driver, touch **Allow Print Driver to Override**.
6. Touch **Ok**.

ENABLING BANNER PAGE PRINTING IN THE XEROX VERSION 3 PRINT DRIVER

To enable banner page printing in the print driver:

1. In the Windows Control Panel, locate the printer.
2. Right-click the printer, then select **Printing preferences**.
3. Click the **Advanced** tab.
4. To enable banner page printing, for Job ID, select **Print ID on a Banner Page**, **Print ID in Margins - First Page Only**, or **Print ID in Margins - All Pages**. To disable banner page printing, select **Disable Job ID**.
5. Click **OK**.

Note: If banner page printing is disabled through the Embedded Web Server or at the device control panel, setting the print driver to print banner pages has no effect.

ENABLING BANNER PAGE PRINTING IN THE XEROX VERSION 4 PRINT DRIVER

Before you begin, install the Xerox® version 4 print driver, and the Xerox® Print Experience application.

Note: The Xerox® version 4 print driver is available on Windows 8 and later.

To enable banner page printing:

1. In the Windows Control Panel, locate the printer.
2. Right-click the printer, then select **Printing preferences**.
3. Click the **Advanced** button.
4. Click the **Document** tab.
5. To enable banner page printing, for Job Identification, select **Print ID in Margins - First Page Only**, **Print ID in Margins - All Pages**, or **Print ID on a Banner Page**. To disable banner page printing, select **Disable Job ID**.
6. Click **OK**, then click **OK**.

Note: If banner page printing is disabled through the Embedded Web Server or at the printer control panel, setting the print driver to print banner pages has no effect.

Print Service Settings

ALLOCATING MEMORY FOR PRINT SETTINGS

1. At the device control panel, log in as Administrator, press the **Home** button. For details, refer to Administrator Access at the Control Panel.
2. Touch **Settings > Device > System Settings > App Settings > Print Settings > Allocate Memory**.
3. Touch an option. You can change settings for the following features:
   - PostScript Memory
   - HP-GL/2 Auto Layout Memory
   - Job Ticket Memory
   - Receiving Buffer - LPD
   - Receiving Buffer - IPP
4. Specify the amount of memory allocated to the selected feature.
5. Touch **OK**.

CONFIGURING OTHER TYPES OF PRINT SETTINGS

1. At the device control panel, log in as Administrator, press the **Home** button. For details, refer to Administrator Access at the Control Panel.
2. Touch **Settings > Device > App Settings > Print Settings > Other Settings**.

3. Touch a selection. You can change settings for the following features:
   - **Print Area**: To print beyond the standard page margins, touch **Extended**.
   - **Substitute Tray**: Specify an action for the device to take when the device runs out of a specific size paper. Options include **Display Message**, **Use Larger Size**, **Use Closest Size**, **Select Tray 5**, **Switch Size Series**, or **Page Layout**.
   - **Prioritize Bypass Tray**: To instruct the device to print from the Bypass Tray, touch **Enabled**.
   - **Paper Type Mismatch**: Specify an action for the device to take when the paper type loaded in the tray does not match the defined paper type. Options include **Print**, **Display Confirmation Screen**, or **Display Paper Supply Screen**.
   - **Unregistered Forms**: Set a print option for instances in which a form that is specified for printing in a form data file is not registered on the device. If you select **Print**, only the data prints because the specified form is not present. The setting is added to the print settings menu when there is a print specification from the host computer.
   - **Resume Job After Print Error**: To cancel a print job automatically when an error occurs, touch **Job Resumes Automatically**. To display a control panel prompt that requires a user to cancel the job manually, touch **Resume by User**.
   - **When Paper Jam Occurs**: To continue printing a job after clearing a paper jam, touch **Resume Job after Jam Clearance**. To cancel the print job, touch **Delete Job**.
   - **Print User ID**: You can print the User ID for a user on the page. To set location where the User ID prints on the page, touch **Top Left**, **Top Right**, **Bottom Left**, or **Bottom Right**. If you use one of these options to specify a User ID, specify the same User ID in the print driver. To prevent the User ID from printing, touch **Off**.
   - **Sensing Separator Page**: To instruct the device not to print on separator pages during a print job, touch **Enabled**. To instruct the device to ignore separator pages, touch **Disabled**.
   - **Banner Pages**: To print an identifying page before each print job, touch **Start Page**. To print an identifying page after each print job, touch **End Page**. To print identifying pages before and after each print job, touch **Start Page & End Page**.
   - **Banner Page Offset**: Banner page offset can help distinguish print jobs from one another. To offset the banner page from the print job pages, touch **Offset**. If you do not want to offset the banner page from the print job pages, touch **No Offset**.
   - **Banner Page Tray**: Select the paper tray loaded with the paper that you want to use for printing banner pages.
   - **PostScript Default Color**: To set the default color option for PostScript print jobs, touch **Color** or **Black & White**.
   - **PostScript Paper Supply**: Select a paper supply option for PostScript print jobs. To allow the device to select the paper tray, touch **Auto Select**. To allow the user to select the paper tray, touch **Select Paper Tray**.
   - **PostScript Font Absence**: To specify how jobs are handled when the PostScript font specified in the document is unavailable in the device, touch **Cancel Printing** or **Substitute Font and Print**.
   - **PostScript Font Substitution**: To use an ATC (Avondale Type Co.) font as a substitute font when a specified PostScript font is not present, select **Use ATCx**. If you do not want to use ATCx as the substitute font, select **Do not use ATCx**.

- **LPD Print Queue**: To specify the LPD print sequence, touch **Data Processing Order** or **Job Submission Order**.
- **OCR Font Glyphs (OXSC)**: To specify the glyph used for OCR jobs, select **Backslash** or **Japanese Yen Sign**.

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 do the following tasks:

- Configure and verify the status of network-connected printers.
- Set up a printer on your network. After the printer is installed, you can monitor the operation of the printer.
- Perform maintenance checks and view supplies status at any time.
- Provide a common look and feel across the many different suppliers of UNIX® and Linux® operating systems.

Installing Xerox® Printer Manager

Before you begin, ensure that you have root or superuser privileges to install Xerox® Printer Manager.

1. Download the appropriate package for your operating system.
   a. Go to www.support.xerox.com.
   b. Search for your printer, then open the page for Drivers and Downloads.
   c. Select your operating system, then select an installation package:
   - XeroxOSDPkg-AIXpowerpc-x.xx.xxx.xxxx.rpm for the IBM PowerPC family
   - XeroxOSDPkg-HPUXia64-x.xx.xxx.xxxx.depot.gz to support HP Itanium workstations
   - Xeroxv5Pkg-Linuxi686-x.xx.xxx.xxxx.rpm to support RPM-based 32-bit Linux environments
   - Xeroxv5Pkg-Linuxi686-x.xx.xxx.xxxx.deb to support Debian-based 32-bit Linux environments
   - Xeroxv5Pkg-Linuxx86_64-x.xx.xxx.xxxx.rpm to support RPM-based 64-bit Linux environments
   - Xeroxv5Pkg-Linuxx86_64-x.xx.xxx.xxxx.deb to support Debian-based 64-bit Linux environments
   - XeroxOSDPkg-SunOSi386-x.xx.xxx.xxxx.pkg.gz for Sun Solaris x86 systems
   - XeroxOSDPkg-SunOSsparc-x.xx.xxx.xxxx.pkg.gz for Sun Solaris SPARC systems
2. To install the Xerox Office Standard Driver on your UNIX platform, log in as root, then type the appropriate command for your operating system:
   - AIX: `rpm -U XeroxOSDPkg-AIXpowerpc-x.xx.xxx.xxxx.rpm`
   - HPUX: `swinstall -s XeroxOSDPkg-HPUXia64-x.xx.xxx.xxxx.depot.gz \*`
   - Solaris (x86-based): `pkgadd -d XeroxOSDPkg-SunOSi386-x.xx.xxx.xxxx.pkg`
   - Solaris (SPARC-based): `pkgadd -d XeroxOSDPkg-SunOSsparc-x.xx.xxx.xxxx.pkg`

   The installation process creates a `Xerox` directory in `/opt/Xerox/prtsys`.

3. To install the Xerox Custom Driver on your Linux platform, log in as root, then type the appropriate command for your operating system:
   - Linux (RPM-based): `rpm -U Xeroxv5Pkg-Linuxi686-x.xx.xxx.xxxx.rpm`
   - Linux (Debian-based) `dpkg -i Xeroxv5Pkg-Linuxi686-x.xx.xxx.xxxx.deb`

   The installation process creates a `Xerox` directory in `/opt/Xerox/prtsys`.

Launching Xerox® Printer Manager

To launch Xerox® Printer Manager:

1. On your computer, open a command-line window, then log in with root or superuser privileges.
2. Type `xeroxprtmgr`, then press **Enter**.

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.

To install a Xerox® print driver, refer to Xerox® Printer Manager.

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.

Note: For complete information on CUPS printing capabilities, refer to the *CUPS Software Users Manual* that is available from www.cups.org/documentation.php.

Installing the Xerox® PPD on a Workstation

The Xerox® PPD file for CUPS is available on the Xerox website www.support.xerox.com. Download the file from the Downloads and Drivers page, then follow the instructions for the PPD file.

To install the Xerox® PPD file for CUPS:

1. Download the latest UNIX® PPD file from the Xerox® website.
2. Copy the PPD file into your 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 on your workstation.
3. Follow the instructions that are included with the PPD file.

Adding the Xerox® Printer

To add the Xerox® printer to the CUPS printer list:

1. Verify that the CUPS daemon is running.
2. Open a Web browser, type `http://localhost:631/admin`, then click **Enter**.
3. For User ID, type `root`. For Password, type the root password.
4. Click **Add Printer**, then follow the onscreen prompts to add the printer to the CUPS printer list.

Printing with CUPS

CUPS supports the use of both the System V (lp) and Berkeley (lpr) printing commands.

- To print to a specific printer in System V, type: **lp -dprinter filename**, then click **Enter**.
- To print to a specific printer in Berkeley, type: **lpr -Pprinter filename**, then click **Enter**.

AS/400 FOR IBM POWER SYSTEMS

Xerox provides Workstation Customization Object (WSCO) files to support IBM iV6R1 or later. A Work Station Customization Object is a lookup table that the host print transform (HPT) uses to translate AS/400 commands into the equivalent PCL code for a specific printer. A WSCO can modify many features including paper input tray, 1-sided or 2-sided printing, characters per inch, lines per inch, landscape or portrait orientation, fonts, and margins.

The XTOOLS library provides a source WSCO for each supported Xerox® printer or device. The library and installation instructions are available from www.support.xerox.com. For your device, select the download for the IBM AS/400 operating system. Unzip the downloaded `XTOOLSxxxx.zip` file, then follow the instructions to install the library.

Note:

- The host print transform only works on files that are of the type AFPDS and SCS. PIDS-formatted printer files must be recreated as type AFPDS to use the WSCO for printing.
- You must have IOSYSCFG permissions to create a device description or a remote queue.
- For details on AS/400, refer to the IBM AS/400 Printing V (Red Book), available on the IBM website.

Installing the WSCO and Setting up Print Queues

For detailed instructions on installing the library and setting up print queues, refer to the installation instructions that are included with the library.

Copying

This chapter contains:

Confirming the Position of Document Guides 124
Setting a Default Image Gradation Mode 125
Specifying Default Copy Settings 126
Copy Control 127
Configuring Presets for Original Page Sizes 128
Reduce and Enlarge Presets 129
Defining Custom Colors 130

Confirming the Position of Document Guides

Document Guides Position Confirmation provides a confirmation message when you change the position of the paper guides to Letter width. If enabled, when you change the guides to Letter, then start a scan, copy, or fax job, a confirmation message appears on the printer control panel. When you change the paper-width guides to A4 or other settings, a confirmation message does not appear.

To enable the Document Guides Position Confirmation:

1. In the Embedded Web Server, log in as administrator, then click **System > Defaults**.
2. In the Common area, click **Check Document Guides Position**.
3. Select **On**.
4. Click **Save**.

Setting a Default Image Gradation Mode

The printer provides two methods of optimizing gradient shades in images. The Photo Image Pseudo Gradation Mode setting provides the following options.

- **Error Diffusion**: This option is a method of halftoning used to smooth the gradients in an image. Use this method for images that are printed.
- **Dither**: This option is a method of randomizing pixels to smooth the gradients in an image. Use this method for images that are displayed on a screen.

To select a method of optimizing gradients in images:

1. In the Embedded Web Server, log in as administrator, then click **System > Defaults**.
2. In the Common area, click **Photo Image Pseudo Gradation Mode**.
3. Click **All Except Copy Job**, then select an option.
4. Click **Save**.

Specifying Default Copy Settings

To specify the default copy settings that users see at the control panel:

1. At the device control panel, log in as Administrator, press the **Home** button, For details, refer to Administrator Access at the Control Panel.
2. Touch **Settings > Customize Apps > Copy > Default Settings**.
3. Touch the desired setting. For details on copy settings, refer to the *Xerox® PrimeLink® C9265/C9275/C9281 Series Color Multifunction Printer User Guide*.
4. Make the required changes to the setting.

Copy Control

To control copy settings:

1. At the device control panel, log in as Administrator, press the **Home** button, For details, refer to Administrator Access at the Control Panel.
2. Touch **Settings > Device > App Settings > Copy Settings**.
3. Touch **Copy Controls**.
4. Touch a setting in the list.
5. Make the required changes.

Configuring Presets for Original Page Sizes

You can define up to 14 presets for the size of original pages.

To configure the preset sizes for original pages:

1. In the Embedded Web Server, log in as administrator, then click **Apps > Copy**.
2. In the Presets area, click a preset size.
3. Select a unit of measure.
4. Select a page dimension.
5. Click **Save**.

Reduce and Enlarge Presets

To change the presets for reducing or enlarging images:

1. At the device control panel, log in as Administrator, press the **Home** button, For details, refer to Administrator Access at the Control Panel.
2. Touch **Settings > Device > App Settings > Copy Settings**.
3. Touch **Reduce / Enlarge Presets**.
4. Make the required changes to the preset.

Defining Custom Colors

To define custom colors:

1. At the device control panel, log in as Administrator, press the **Home** button, For details, refer to Administrator Access at the Control Panel.
2. Touch **Settings > Device > App Settings > Copy Settings**.
3. Touch **Custom Colors**.
4. Touch a custom color in the list.
5. To increase or decrease the values for Yellow, Magenta, or Cyan, touch **+** or **-**.
6. Touch **OK**.

Scanning

This chapter contains:

Configuring General Scan Service Settings 132
Setting Up Scanning to an FTP Server 133
Setting Up Scanning to an SFTP Server 134
Setting Up Scanning to an Email Address 135
Scanning to a Folder on the Device 136
Managing Folders and Scanned Files 137
Scanning to an Email Address 139
Scanning to a USB Drive 141
Job Flow Sheets 142
Enabling Network Scan Utility 3 145

Configuring General Scan Service Settings

SETTING SCAN DEFAULTS

To define scanning default settings for all users:

1. At the device control panel, log in as Administrator, press the **Home** button, For details, refer to Administrator Access at the Control Panel.
2. Touch **Settings > Device > App Settings > Scan Settings > Scan Defaults**.
3. Touch a default setting, then touch **OK**.

CONFIGURING OTHER SCAN SETTINGS

To define other scanning settings for all users:

1. At the device control panel, log in as Administrator, press the **Home** button, refer to Administrator Access at the Control Panel.
2. Touch **Settings > Device > System Settings > Scan Settings > Other Settings**.
3. Make the appropriate change, then touch **OK**.

SETTING SCAN TO PC DEFAULTS

To define default Scan to PC settings for all users:

1. At the device control panel, log in as Administrator, press the **Home** button, For details, refer to Administrator Access at the Control Panel.
2. Touch **Settings > Device > Scan Settings > Scan to PC Defaults**.
3. In the list, touch a default setting.
4. Change the following settings as needed:
   - **Transfer Protocol**: Touch **FTP**, **SMB**, or **SMB (UNC Format)**.
   - **Login Credential to Access Destination**: To use the user name and password of the remotely authenticated user for login, touch **Remotely Authenticated User**.
   - **User Name for FTP Scan**: If you select Remotely Authenticated User for the Login Credential to Access Destination setting:
     - To use only the user name for login, touch **User Name Only**.
     - To use the full login credential name for the user, which includes the domain name, touch **Add Domain Name**.

Setting Up Scanning to an FTP Server

Before you set up scanning to an FTP Server, ensure that the server has the proper software installed and configured.

1. In the Embedded Web Server, log in as administrator, then click **Address Book**.
2. To associate the FTP server with a contact, click a contact name.
3. For FTP, click the **FTP**, then enter the following information:
   - **Name**: Enter the name that you want to appear in the Address Book.
   - **Type**: Select the network connection type.
   - **IP Address/Host Name: Port**: Enter the IP address or host name of your FTP server, then enter the default port number. In the next field, enter the default port number for FTP. Use the default port number 21, or select a number from the range provided.
   - **Save Location**: Enter the path of the folder on the FTP server. For example, to save the scanned files to a folder named `colorscans` inside the scans folder, type `scans/colorscans`.
   - **User Name**: Enter a user name corresponding to a user account on the FTP server.
   - **Password**: Enter the password corresponding to the user account on the FTP server.
   - **Retype Password**: Enter your login password again.

Note: After you complete the process, scanning to the FTP server is enabled.

Setting Up Scanning to an SFTP Server

Before you set up scanning to an SFTP Server, ensure that the server has the proper software installed and configured.

1. In the Embedded Web Server, log in as administrator. For details, refer to Administrator Access at the Control Panel.
2. Click **Address Book**.
3. To associate the SFTP server with a contact, click a contact name.
4. On the popup window, click **SFTP**, then enter the following information:
   - **IP Address/Host Name: Port**: Enter the IP address or host name of your SFTP server, then enter the default port number. In the next field, enter the default port number for SFTP. Use the default port number 22, or select a number from the range provided.
   - **Save Location**: Enter the path of the folder on the SFTP server. For example, to save the scanned files to a folder named `colorscans` inside the scans folder, type `scans/colorscans`.
   - **User Name**: Enter a user name corresponding to a user account on the SFTP server.
   - **Password**: Enter the password corresponding to the user account on the SFTP server.
   - **Retype Password**: Enter your login password again.

   Note: After you complete the process, scanning to the SFTP server is enabled.
5. Click **Save**.

Setting Up Scanning to an Email Address

Before you can scan to an email address, configure the printer to communicate with your SMTP email server.

To configure the SMTP server settings:

1. In the Embedded Web Server, log in as administrator, then click **Apps**.
2. In the Installed Apps area, click **Email**.
3. In the SMTP area, click **Setup**.
4. To enable Email Submission, enable the toggle button.
5. Enter or select the following information.
   - In the Device Email area, type an email address to appear in the From field of emails from the printer.
   - In the SMTP Server area, click **Server Address**, then type the IP address or DNS name of the SMTP server.

     If you do not know the IP Address or DNS Name of the SMTP server, click **Select Server from List**.

   Note: This feature requires that specific configurations are made to your network. For details, contact your network administrator.

   - For Outgoing SMTP Port Number, type the default port number required for the SMTP server, or select a number from the range provided. Common default port numbers for SMTP include 25, 465, and 587.

   Note: Ensure that the authentication type is compatible with your SMTP server.
6. Click **OK**.

Scanning to a Folder on the Device

The Store to Folder feature allows users to scan files to folders created on the device hard drive. You can retrieve stored files using the Embedded Web Server. This feature provides network scanning capability without the need to configure a separate server.

Note: To use faxes with this feature, you must purchase and install the Fax Hardware Kit. For details, refer to the instructions included with the kit.

Managing Folders and Scanned Files

CREATING AND EDITING A FOLDER

To create a scan folder on the device hard drive:

1. At the device control panel, press the **Home** button and click **Send from Folder > Create New Folder**.
2. Select an available folder.
3. Type a name for the folder, then click **OK**.
4. On the Check Folder Passcode window, select **On** to set the passcode, then click **OK**.
5. For the Folder Passcode, enter the password and click **OK**.
6. For the Target Operation, select an option:
   - To check the passcode for every job operation, select **All Operation**.
   - To check the passcode when saving or modifying jobs, select **Save (Write)**.
   - To check the passcode when printing or deleting jobs, select **Print / Delete (Read)**.
7. To delete files after they are printed or retrieved, for Delete Files after Print or Retrieve, select **Enabled**.
8. To delete files after the stored file folder date expires, for Delete Expired Files, select **Enabled**.

You can edit and delete folders. You can view a list of the files in a folder.

- To edit or delete a folder, for the folder number, perform one of the following actions:
  - Click on the folder name and type the new name then click **OK**.
  - Click **Delete Folder**, then to confirm the deletion, click **Delete**.

SCHEDULING DELETION OF FILES STORED IN FOLDERS

To minimize disk space consumed by stored files, the device can delete files after a specified time period.

To schedule deletion of files stored in scan folders:

1. At the device control panel, log in as Administrator, press the **Home** button. For details, refer to Administrator Access at the Control Panel.
2. Touch **Device > App Settings > Send from folder**.
3. Touch **File Retention Period**, then touch **On**.
4. Set time retention period.
5. Touch **OK**.

CONFIGURING SCAN FOLDER SERVICE SETTINGS

To configure scan folder settings:

1. At the device control panel, log in as Administrator, press the **Machine Status** button, then touch the **Tools** tab. For details, refer to Administrator Access at the Control Panel.

2. Touch **System Settings > Folder Service Settings**.
3. To change a setting:
   a. Touch an item, then touch **Change Settings**.
   b. Touch an option, then touch **Save**.

   Use this method to change the following settings as needed:

   - **Limit Access to Folder**: Touch **On** or **Off**.
   - **Files Retrieved by Client**: Specify when to delete files that have been retrieved from a folder.
     - To use the folder settings, touch **Delete According to Folder Settings**.
     - To ignore the folder settings and delete files from folders after the files are retrieved, touch **Force Delete**.
   - **File Display Default**: Touch **List** or **Thumbnail**.
   - **Orientation for Stored Print Jobs**: Touch **Portrait** or **Landscape**.
   - **Print and Delete Confirmation Screen**: To display a confirmation message on the touch screen when a file is printed and deleted from a folder, touch **Enabled**.
   - **Quality/File Size for Retrieval**: Select the quality and size that files are compressed to when retrieved from a folder.
   - **Convert Custom Size to Standard Size**: To convert files in folders to a standard size when a fax or Internet Fax is transferred for secure polling, touch **Yes**.
   - **Standard Size Threshold Value**: Specify the standard size for the Convert Custom Size to Standard Size setting.
   - **Internet Fax to Internet Fax**: To allow users to forward files stored in folders using the Internet Fax service, touch **Enabled**.
   - **Internet Fax to Email**: To allow users to forward files stored in folders using the Email service, touch **Enabled**.
4. Touch **Close**.

Scanning to an Email Address

Scanning to an email address sends scanned documents as attachments to email.

For instructions explaining how to use this feature, refer to the User Guide at www.xerox.com/support.

Note: To use faxes with this feature, purchase and install the Fax Hardware Kit. For details, refer to the instructions included with the kit.

CONFIGURING EMAIL SETTINGS

1. At the device control panel, log in as Administrator. For details, refer to Administrator Access at the Control Panel.
2. Touch **App Settings > Scan Settings > Email Control**.
3. Change the following settings as needed:
   - **Maximum Address Entries**: Select the maximum number of email addresses to which a scanned document can be sent. This includes To, Cc, and Bcc fields.
   - **EMail Print Options**: Select the parts of the email that you want to print. Select **Print Attachment Only**, **Attachment, Full Headers & Message**, or **Attachment, Basic Headers & Message**.
   - **Print Error Notification Email**: To print an error report when an email transmission error occurs, touch **On**.
   - **Response to Read Receipts**: To allow the device to respond to a request for a read receipt (MDN) after an email is received, touch **On**.
   - **Display Read Receipts**: To allow the device to request a read receipt (MDN) when an email is sent, touch **On**.
   - **Print Delivery Confirmation Mail**: To print a confirmation report (Delivery Status Notification - DSN response or Mail Delivery Notification - MDN response) for every transmission, touch **On**. To print a report when a transmission fails, touch **Print when delivery fails**.
   - **Maximum Data Size per EMail**: Specify the maximum size of an email that will be split when using the Split by Data Size method.
   - **Maximum Total Data Size**: Specify the maximum size of an email that can be sent.
   - **Maximum Split Count**: Specify the maximum number of splits.
   - **Edit From Field**: To allow any user to edit the From field of an email, touch **Enabled**.
   - **Edit Email Recipients**: To allow users to edit the To, Cc, and Bcc fields of an email, touch **Yes**.

EDITING EMAIL SETTINGS

To edit general email settings in the Embedded Web Server:

1. In the Embedded Web Server, click **Apps > Email > Incoming Email Settings**.

2. Change the email settings as needed:
   - For Receiving Protocol, select **POP3** or **SMTP**.
   - For Incoming Email Print Options, select the parts of the email that you want to print.
   - For Output Destination for Incoming Email, select an option.

Scanning to a USB Drive

The Store to USB feature allows users to scan a document to a USB flash drive using the USB port on the device control panel.

ENABLING SCAN TO USB FUNCTIONALITY

To enable users to scan files to a USB drive:

1. In the Embedded Web Server, click **Apps > USB**.
2. In the Enable Features area, click **Scan** and select **Enabled**.

Job Flow Sheets

You can create a Job Flow to execute a series of actions on a scanned document that is stored in a folder. The actions are defined in a Job Flow Sheet. For example, a Job Flow can print the scanned image and send the image to an FTP repository.

Before you begin, enable ports for SOAP, SNMP, and UDP.

To configure a Job Flow:

- Create a Folder. Refer to Scanning to a Folder on the Device.
- Set up a Job Flow Sheet. Create a sheet, then define the actions for the sheet.
- Link the Job Flow Sheet to the folder.

Note: To use faxes with this feature, you must purchase and install the Fax Hardware Kit. For details, refer to the instructions included with the kit.

SETTING UP A JOB FLOW SHEET

To set up a Job Flow Sheet, create a Job Flow Sheet and define the actions performed by the Job Flow Sheet

Creating a Job Flow Sheet

To create a job flow sheet:

1. In the Embedded Web Server, click **App > Send from Folder**.
2. In the Folder area, click **View**, then click on any folder.
3. Select **Link Job Flow Sheet to Folder** option.
4. On the Link Job Flow Sheet to Folder popup, click **Edit**.
5. On the Job Flow Sheet List popup, click **Add**.
6. To create the Job Flow Sheet, enter the following details:
   - For Job Flow Sheet Name, type a name for the sheet.
   - For Description, type a description for the sheet.
   - For Keyword, type keywords that can help users find the sheet at the control panel.

7. Specify the options for the action that you selected:
   - **Send as Fax**: Type the name and fax number of the recipient, then select the starting rate.

     Type the folder number and the folder passcode.

     If required, for Send Relay Broadcast or Print at Relay Station, select **Enabled**.

     If needed, for Relay Station ID / Broadcast Recipients, F Code, and Password (F Code Communication), type the required information.
   - **Send as Internet Fax**: Type a name and email address for each recipient, then select the Internet fax profile. If required, for Header, select **On**.
   - **Send as Email**: Type the name and email address for each recipient, then select the file format.
   - **Transfer via FTP**, **Transfer via SFTP**, or **Transfer via SMB**: For Name and Server Name, type the required information.
     1. For SMB, type the share name.
     2. Type the login name and password of the folder.
     3. Select the file format.
     4. For **MRC High Compression** and **Optimize for Quick Web View**, select **On**, if needed.
8. Under Print/Email Notification area, set the following:
   - **Print**: Select the **Paper Supply** tray, **Output Destination** tray, **Quantity**, and **2 Sided Printing** options, as needed. If other options are available, select them as needed, for example to use staples.
   - **Email Notification:** Type the email addresses of the recipients, then for When to Notify, select options as needed. For Message, type the message to include in the body of the email.

JOB FLOW SHEET RESTRICTIONS

Actions available for use in a Job Flow Sheet are listed below.

- Print
- Fax
- IP Fax (SIP)
- Internet Fax
- Mail
- FTP
- SFTP
- SMB

There are restrictions on the combination of actions that can be used in a Job Flow Sheet. The table shown here illustrates the availability of various actions.

ACTION	PRINT	FAX	IP FAX (SIP)	INTER-NET FAX	MAIL	FTP/ SFTP	SMB
Fax Documents for Secure Polling	1	1	1	1	1	1	1
Scanning	1	1	1	1	1	1	1
Fax to Folder	1	1	1	1	1	1	1
Internet Fax Received	1	1	2	2	2	1	1
Print Stored	3	3	3	3	3	3	3
1: Always Available 2: Never Available 3: Available depending on System Administrator settings							

LINKING THE JOB FLOW SHEET TO A FOLDER

To link a job flow sheet to a scan folder:

1. In the Embedded Web Server, click **App > Send from Folder**.
2. In the Folder area, click **View**. The list of folder appears.
3. Click on a Folder, then click **Link Job Flow Sheet to Folder**.
4. For the folder to which you want to create a link, click **Edit**.
5. Select your Job Flow Sheet from the list, then click **Link**.
6. Click **Save**.

Enabling Network Scan Utility 3

Network Scan Utility 3 allows you to scan directly to your computer and helps you manage and distribute scanned image files. Before you can use the utility, you must enable SNMP, WebDAV, and SOAP.

To enable port settings to run the Network Scan Utility 3:

1. In the Embedded Web Server, click **Network > Protocols**.
2. For SNMP, WebDAV, and SOAP, select **Enabled**.
3. Click **Save**.

You can now install and use the scan utility.

Faxing

This chapter contains:

Embedded Fax 148
Internet Fax 157
LAN Fax 160
Session Initiation Protocol Fax 161
Printing Fax Reports 164

Embedded Fax

When you send a fax from the device control panel, the document is scanned and transmitted to a fax machine using a dedicated telephone line.

Before you begin:

- Verify that the device has access to a functioning telephone line and has a telephone number assigned to it.
- Install the Fax Hardware Kit and set the country code. For details, refer to the instructions provided with the kit.

You can use some of the scan service settings for faxes:

- To store faxes to folders on the printer, refer to Scanning to a Folder on the Device.
- To send faxes to an email address, configure the email settings. For information, refer to Scanning to an Email Address.
- When faxes are stored in folders, you can specify more actions. For example, the printer can print the fax, send it to an email recipient, then send the fax to a network repository. To perform actions on the stored folder, create a job flow sheet. For information, refer to Job Flow Sheets.

ENABLING EMBEDDED FAX

To enable the embedded fax server:

1. In the Embedded Web Server, click **Apps > Fax**.
2. For Fax, select **Enabled**.

TO SET UP A FAX

To set up a fax:

1. In the Embedded Web Server, login as administrator.
2. Click **Apps > Fax**.
3. In the Fax Line area, click **Edit** and enter the details.
4. For Fax Name, enter a name.
5. For G3 ID, enter the fax number.
6. Select the Dial Type as **Tone** or **10 pps**.
7. Select the G3 Transmission as **Detect Tone** or **Do Not Detect Tone**.
8. Click **Save**.

CONFIGURING FAX COMMON SETTINGS

1. In the Embedded Web Server, log in as administrator.
2. Click **Apps > Fax > Common Settings**.

3. Change the following fax settings as needed:

OPTION	DESCRIPTION
Reconfirm Recipients	Select any one of the following to reconfirm recipients • **Do Not Confirm** • **Always Reconfirm** or • **Reconfirm If Multiple Recipients**
Rotate 90 Degrees	To rotate scanned faxes 90 degrees, click **On**.
Border Limit	If a received fax document is longer than a page, specify the border size around the document to force a page break (0.0–5.0.in)
Auto Reduce on Receipt	To fit a long received fax document on a single page if the document is within the range specified in the Border Limit setting, click **On**.
2 Pages per Slide on Receipt	To print two pages on a single sheet of paper, click **On**.
2 Sided Printing	To print on both sides of a single sheet of paper, click **On**.
Memory Full Procedure	If the device hard disk becomes full while scanning a document, the current job can be aborted and deleted or the partially stored job can be sent. Choose the following: • **Delete Job** • **Run Job with Already Scanned Originals**
Maximum Storage Pages	Set the maximum number of pages that can be stored for a fax document.
Transmission Report - Job Undelivered	To print a report for a failed delivery, for Transmission Report - Job Undelivered, select **On**. If you do not want a report, select **Off**.
Limit Output Destination Usage	To Limit output destination choose any one of the following: • **Off** • **Fax Apps Only**.

ENABLING THE OUTPUT DESTINATION

To separate faxes from other prints, you can send faxes to a specific output tray. To enable the selection of an output tray for faxes:

1. In the Embedded Web Server, login as administrator, then click **Apps > Fax**, then in Incoming Fax Settings area, click **Folder Selector Setup**.

2. Select **Enabled**.
3. Click **Save**.

CONFIGURING FAX CONTROL SETTINGS

1. In the Embedded Web Server, log in as administrator.
2. Click **Apps > Fax > Fax Controls**.

3. Change the following fax settings as needed:

OPTION	DESCRIPTION
G3 Sender ID Fax	To notify G3-ID to recipients, click **On**.
Transmission Interval	Specify how often faxes are transmitted (3–155 seconds). A longer transmission interval increases the total time required to send a broadcast transmission, but allows faxes to be received during that time.
Batch Send	To allow multiple faxes addressed to a single destination to be sent in a single fax transmission whenever possible, click **Yes**. This option reduces transmission costs.
Direct Fax	To allow the device to receive a LAN fax sent from a print driver, select **On**. For details about LAN fax, refer to the *Print Driver Help*.
Activity Report	This report provides a summary of faxes sent and received. By default, this report prints automatically after 100 fax transmissions and receptions. Click **Activity Report**, then perform the following: • Click **Print Activity**, then click **On**. • Click **Print Recipient Information**, then click **First 40 Characters** or **Last 40 Characters**. • Click **Number of Events**, select **100** or **200**.
Broadcast Report	This report acknowledges the transmission of a fax sent to multiple recipients. The Fax app generates this report automatically. Click **Broadcast Report** and select any one of the following: • **On** to enable. • **Off** to disable. • **Print Only When Error Occurs**
Polling/Storage from Remote Devices	To allow remote devices to poll for faxes stored on the printer, click **Allow**.
Simple Log of Sent Fax Documents	Click **Simple Log of Sent Fax Documents**, toggle the **Enable** button, and perform the following: • Click **Transfer Method** to choose **Email** or **SMB**. • Click **Destination (Email)**, select the options, then click **OK**.

CONFIGURE INCOMING FAX SETTINGS

Configure the Incoming Fax Settings in the Embedded Web Server:

1. In the Embedded Web Server, log in as administrator.

2. Click **Apps > Fax > Incoming Fax Settings**.
3. Change the following fax settings as needed:

OPTION	DESCRIPTION
Fax Receiving Mode	Choose Fax receiving mode from the following options: • **Auto Receive** • **Manual Receive**
Block Inbound Faxes	To block unknown fax numbers toggle the **Enable** button. Type up to 50 fax numbers that you want to block.
File Name Format	Select a file format.
Folder Selector by G3 ID	Store faxes based on G3 ID.
Folder Selector Setup	To classify received faxes by line type and store them in folders as specified in the Embedded Web Server, click **Enable**. Locate these folders on classify received faxes by line type and store them in folders as specified in the Embedded Web Server.
Line 1 Output Destination	To select the output destination, select the following options: • **Finisher Top Tray** • **Finisher Tray**

SETTING INCOMING FAX OPTIONS

Reduce/Enlarge Presets

To modify the reduce/enlarge adjustment values available to users:

1. At the device control panel, log in as administrator, press the **Home** button, refer to Administrator Access at the Control Panel.
2. Touch **Device > App Settings > Fax Settings > Reduce/Enlarge Presets**.
3. Choose one of the pre-configured presets or select an item in the list.
4. If you are modifying settings, change the following settings as needed:
   - **Preset %**: Specify the preset magnification values to appear in the Layout Adjustment Screen.
   - **Variable %**: Specify the default magnification value to appear in the Layout Adjustment Screen.

Original Document Size Defaults

To specify default size settings for received faxes:

1. At the device control panel, log in as Administrator, press the **Home** button. For details, refer to Administrator Access at the Control Panel.
2. Touch **Device > App Settings > Fax Settings > Original Size Defaults**.
3. To modify an original document size default setting:
   a. From the list, touch an original document size item.
   b. To select the paper size, touch **A/B Series Size**, **Inch Size**, or **Others**.
   c. Touch a paper size and page orientation.
   d. Touch **OK**.

STORING AND FORWARDING RECEIVED FAXES

You can configure incoming faxes to route automatically to an internal folder. You can configure the printer to send faxes from an internal folder to a destination using one or more of the following methods:

- Print: Print a hard copy of the received fax.
- Send as Fax: Forward the fax to another fax number.
- Send as Internet Fax: Forward the fax to an Internet fax address.
- Send as Email: Forward the fax as an email attachment to an email recipient.
- FTP Transfer: Save the fax to an FTP repository.
- SFTP Transfer: Save the fax to a secure FTP repository.
- SMB Transfer: Save the fax to an SMB repository.
- Email Notification: Send an email notification to selected recipients.

The fax and scanning services share the folder database. To create and name the internal folder to store received faxes, refer to Scanning to a Folder on the Device.

Setting up the Folder to Receive Faxes with Email Notification

Before you begin, create and name a folder to receive the incoming faxes. For details, refer to Scanning to a Folder on the Device.

To set up the folder to receive faxes:

1. In the Embedded Web Server, log in as Administrator.
2. Navigate to **Apps > Send from Folder**.
3. Click **View**.
4. Select an available folder.
5. Provide a folder name and enable any options you like for your fax folder jobs.
6. Select **Save**.
7. Navigate to **Apps > Fax > Incoming Fax Settings**.
8. Enable the Folder Selector Setup.

9. Select **Folder Selector for Line #**.

   Note: # above depends on how many fax lines you have installed in your device.

10. For Folder Selector List, select **Folder Selector for Line 1**, then click **Enabled**.
11. Enter 1–500 number for the folder that you have created to receive faxes.
12. For Link Job Flow Sheet to Folder, select an option and enter the required details from the recipients area.
13. In Print/Email Notification area, select **Email Notification**.
14. Select **On** for When File is Stored.
    a. Enter a message, if required.
    b. Enter at least one email address and click **OK**.
15. Select **Save** twice to complete setup.
16. Go back to **Apps > Send from Folder**.
17. Click **View**.
18. Select the folder with name you just created in Step 5.
19. Click **Link Job Flow Sheet to Folder**.
20. Click **Edit**, then click **Add**.
21. Enter the name in the Job Flow Sheet Name.
22. Click **Save**.
23. From Job Flow Sheet List, select the sheet you just created.
24. Enable Link.
25. Click **Save**, then click **Close**.
26. Click **Save**.

Configuring and Linking Job Flow to Folder at Control Panel

To configure and link the Job Flow to Folder:

1. At the device control panel, log in as Administrator.
2. Go to Home Screen and touch **Send from Folder** app.
3. Touch the folder which is created in Setting up the Folder to Receive Faxes with Email Notification.
4. Touch **Folder Settings**.
5. Touch **Link Job Flow to Folder**.
6. Touch **Select Job Flow Sheet**.
7. Choose the Job Flow Sheet created in Setting up the Folder to Receive Faxes with Email Notification.
8. To see details, touch the information icon of the Job Flow Sheet.
9. In the Details screen, touch **Edit**.
10. Add description as required.

11. Touch **Send as Email**.
12. Add recipient from address book or create new recipient.
13. Select **OK**.
14. Close the Send as Email window.

    The Number of Recipients is populated.
15. Touch **OK**.

    Note: Ensure that the newly created Job Flow Sheet is selected.
16. Touch **OK**.

This process creates a Job Flow Sheet for the faxes received in the incoming fax folder. To manage folders and job flow sheets, refer to Scanning to a Folder on the Device and Job Flow Sheets.

STORING AND FORWARDING FAXES USING FAX IDENTIFIERS

Fax Group 3, which is also known as G3, is an encoding format for fax transmissions. You can use the telephone number of the G3 fax sender to store faxes in a folder on the printer. To store faxes from a known telephone number, create a folder for the number. You can use the asterisk character as a wildcard for a range of numbers. For example, 12312345*, stores faxes received from telephone numbers 1231234500–1231234599. The printer reads wildcard telephone numbers from left-to-right, and non-wildcard numbers from right-to-left. If you set up several folders, you can store faxes from different telephone numbers in different folders.

To use the G3 information for storing faxes, ensure that the devices that send faxes to your printer support the G3 fax protocol. Ensure that you have set up the printer to use embedded fax. For details, refer to Enabling Embedded Fax. Ensure that you have enabled the storing of faxes to a folder by the G3 identifier. For details, refer to Configuring Fax Control Settings.

The storage of faxes using fax identifiers takes priority over the storage of all received faxes in a single folder.

The fax and scanning services share the folder database. To create and name the internal folder to store received faxes, refer to Scanning to a Folder on the Device.

Setting up the Folder to Store Faxes

Before you begin, create and name the internal folder to store received faxes. For information, refer to Scanning to a Folder on the Device.

To set up the folder to receive faxes based on the telephone numbers received in a G3 fax transmission:

1. At the device control panel, log in as administrator, press the **Home** button. For details, refer to Administrator Access at the Control Panel.
2. Touch **Device > App Settings > Fax Settings > Fax Received Options**.
3. Select **Folder selector by G3 ID**.
4. Select an unused number.
5. Select **G3 ID**.
6. Type G3 ID, select **OK**, then select **Folder Number** and click **OK**.

To forward faxes from the folder, create a job flow sheet, then associate the sheet with the folder. For details, refer to Job Flow Sheets.

Internet Fax

Internet Fax allows you to scan a document at the device and send it to a destination using an email address or to receive and print an email with attachments. You can also print a transmission report. Internet Fax enables this functionality without the use of a telephone line.

CONFIGURING INTERNET FAX SETTINGS

Before you begin:

- To transfer emails, configure the POP3 and SMTP settings.
- Configure email and Internet Fax settings. For details, refer to Configuring Email Settings.
- If you want the printer to receive Internet faxes, create an email address for the printer.
- Install the Fax Hardware Kit.

Note:

- Before you enable Internet Fax, ensure that the printer has a valid domain name.
- The Internet Fax service uses many of the same settings as the Scan to Email service.

CONFIGURING INTERNET FAX GENERAL OPTIONS

To configure settings for incoming and outgoing Internet faxes:

1. In the Embedded Web Server, click **Apps > Internet Fax > Internet Fax Controls**.

2. Change the following settings, as needed under Internet Fax Control:
   - To send the Internet fax to an email address using an SMTP server, select **Internet Fax Path**, for Send, select **Via Email Server**. To send to an email address using a fully qualified host name or IP address, select **Direct P2P**. Selecting Direct P2P sends the email as a hostname address, for example, `example.address@device.domain.jp`, or as an IP address, for example, `example.address@[129.249.123.1]`.
   - To select the profile to use to send an Internet Fax broadcast, for Broadcast Profile, select an option:

     TIFF-S: Documents larger than A4 are reduced automatically to A4, 210 x 297 mm (8.27 x 11.69 in.).

     TIFF-F: To specify Superfine for Resolution, or to send A3, 297 x 420 mm (11.69 x 16.54 in.) or B4, 250 x 353 mm (9.84 x 13.9 in.) documents, select this profile.

     TIFF-J: To use JBIG compression, select this profile.
   - For Broadcast Starting Rate, select **G3 Auto**, **Forced 4800 bps**, or **G4 auto** as the default communications mode.
   - To print a delivery confirmation report, for Delivery Confirmation Method, select **Delivery Receipts**. To confirm that the Internet fax was received and processed, select **Read Receipts**. The destination fax machine must support Delivery Status Notification (DSN) or Mail Delivery Notification (MDN).

     To use this setting, select print delivery confirmation as part of your email settings.
   - To select the parts of the Internet fax that you want to print, for Incoming Internet Fax Print Options, select an option. You can choose **Print Attachment Only**, **Print Attachment & Message if it exists**, **Attachment, Basic Headers & Messages**, or **Attachment, Full Headers & Message**.
   - To disallow users from forwarding a fax to a number listed in the fax address book, for No Fax Transfer from Address Book, select **Enabled**.
   - To add a transmission header to a received Internet fax when it is forwarded, under the Transmission Header Text - Fax Transfer, select **Display Header**.
   - To specify the maximum size allowed to forward an Internet fax, for Fax Transfer Maximum Data Size, select Enabled. Type the maximum size from 1–65535 Kbytes.
   - To print an error report when a transmission error occurs, go to Auto Printing of Error Notification Email, select **Save**.
   - To allow the printer to respond to a request for a read receipt (MDN), for Response to Read Receipts, select **Enabled**.
   - To allow the printer to Respond to Read Receipt Requests, for Read Receipts, select **Enabled**.
   - For Subject, type the text that you want to appear in the subject field for the Internet fax.
   - For Message, type the text that you want to appear with the Internet fax.
   - For User, Attachment, or Device Information, select the additional information that you want to send with the Internet fax.
   - For Signature, type the text that you want to appear with the Internet fax.
   - To use Encryption, select **Enabled**.
   - To print a report for a failed delivery, for Transmission Report-Job Undelivered, select **On**. If you do not want a report, select **Off**.

3. Click **Save**.

CONFIGURE INCOMING FAX SETTINGS

Configure the Incoming Fax Settings in the Embedded Web Server:

1. In the Embedded Web Server, log in as administrator.
2. Click **Apps > Fax > Incoming Fax Settings**.
3. Change the following fax settings as needed:

OPTION	DESCRIPTION
Fax Receiving Mode	Choose Fax receiving mode from the following options: • **Auto Receive** • **Manual Receive**
Block Inbound Faxes	To block unknown fax numbers toggle the **Enable** button. Type up to 50 fax numbers that you want to block.
File Name Format	Select a file format.
Folder Selector by G3 ID	Store faxes based on G3 ID.
Folder Selector Setup	To classify received faxes by line type and store them in folders as specified in the Embedded Web Server, click **Enable**. Locate these folders on classify received faxes by line type and store them in folders as specified in the Embedded Web Server.
Line 1 Output Destination	To select the output destination, select the following options: • **Finisher Top Tray** • **Finisher Tray**

INTERNET FAX ADDRESSES

You can store Internet Fax email addresses in the device internal address book or you can configure the device to reference a network LDAP directory.

LAN Fax

Local Area Network (LAN) Fax allows you to send a fax from the print driver on your computer to a fax machine over a telephone line.

Users select the Fax option from their print driver. For details about using or configuring LAN Fax, refer to *Driver Help*.

Session Initiation Protocol Fax

Session Initiation Protocol (SIP) Fax or Fax Over IP (FoIP) Fax, allows you to send and receive fax documents over the Internet to and from another FoIP fax machine or a standard G3 fax machine. If you have an SIP server, you can associate the SIP User Name of the device with a fax number, so that users can type the fax number in a familiar format. If you have a VoIP gateway, the device can communicate with standard G3 fax machines. If necessary, configure SIP server settings, register VoIP gateways, and configure T.38 settings.

Note: Before you begin, purchase and install the Fax over IP (FoIP) Kit.

To enable SIP Fax at the control panel:

1. At the device control panel, log in as Administrator, press the **Home** button. For details, refer to Administrator Access at the Control Panel.
2. Touch **Device > Maintenance**.
3. Touch **Software Options**.
4. To enable SIP Fax, type the software PIN.
5. Touch **Restart**.

ENABLING SIP SETTINGS

For printers equipped with fax over IP, to enable SIP:

1. In the Embedded Web Server, log in as administrator, then click **Apps > Fax**.
2. In the SIP Settings area, click **SIP**.
3. For Enable SIP Port, click **Enable** toggle button.
4. If needed, type a new port number.
5. For Device SIP Address, type the SIP address for the printer.
6. Click **SIP Transport Protocol**, then select an option.
7. To enable or disable the SIP server, click **SIP Server**, then select an option.
8. Click **OK**.

To register the VoIP gateways:

1. In the Embedded Web Server, log in as administrator, then click **Apps > Fax**.
2. In the SIP Settings area, click **SIP**.
3. For Enable SIP Port, click **Enable** toggle button.
4. In the VoIP Gateways area, click **Edit**.
5. Click the first available gateway.
6. For ID Number, type an ID number for the gateway.
7. For Address, type the IP address for the gateway.
8. Click **OK**.
9. If you use multiple VoIP gateways, for each gateway, repeat the steps to register the gateway.

10. When finished, click **Close**.
11. Click **OK**.

To configure domain filtering:

1. In the Embedded Web Server, log in as administrator, then click **Apps > Fax**.
2. In the SIP Settings area, click **SIP**.
3. For Enable SIP Port, click **Enable** toggle button.
4. In the Domain Filtering area, click **Edit**.
5. To allow specific domains, click **Allow Specific Domains**.
   - Enter up to 50 domains to allow.
   - To delete domains from the list, click the **Trash** icon.
6. To block specific domains, click **Block Specific Domains**.
   - Enter up to 50 domains to block.
   - To delete domains from the list, click the **Trash** icon.
7. To disable domain filtering, select **Off**.
8. When finished, click **OK**.

   Note: For domain filtering, you can either allow domains or block domains. The configuration window does not let you list both domains to allow and domains to block at the same time.
9. Ensure that all SIP settings are completed.
10. Click **OK**.

CONFIGURING VOIP GATEWAY REGISTRATION

To send data by VoIP Gateway without using the SIP server, register one or more VoIP gateways. Each entry consists of an ID and a Gateway Address (IP). You can register up to 50 VoIP Gateways.

To register a VoIP Gateway:

1. In the Embedded Web Server, click **Network > Protocols > VoIP Gateway**.
2. To manage VoIP Gateway IDs, perform the appropriate procedure:
   - To register a new VoIP Gateway ID, click **Create**. Type the required information for ID and Gateway Address, then click **Apply**.
   - To revise an existing VoIP Gateway ID, select the appropriate ID, then click **Edit**. Make changes as needed, then click **Apply**.
   - To delete a VoIP Gateway ID, select the appropriate ID, then click **Delete**. To confirm the deletion, at the screen prompt, click **OK**.

CONFIGURING T.38 SETTINGS

1. In the Embedded Web Server, log in as administrator, then click **Apps > Fax**.
2. In the SIP Settings area, click **T.38**.
3. Click **T.38 Transport Protocol**, then select an option.
4. If needed, for UDPTL Listening Port Number, type a new port number.
5. If needed, for TCP Listening Port Number, type a new port number.
6. If needed, for RTP Listening Port Number, type a new port number.
7. Click **OK**.

CONFIGURING SIP SETTINGS AT THE DEVICE CONTROL PANEL

You can change commonly used SIP Fax settings on the Fax Options tab of the control panel. Additionally, you can view and edit the following SIP Fax settings on the Tools tab in System Administrator mode:

- **Fax Screen Default Settings**: Set the Default Fax Screen Tab options, Address Book Speed Dial Numbers, and Transmission Screen options.
- **Fax Default Settings**: Set the Resolution, Original Type, Starting Rate, and other defaults.
- **Fax Control Settings**: Set settings for Re-enter Recipient Data, Transmission Header Text, Rotation, and other fax control settings.
- **Fax Received Options Settings**: Set up folders for received faxes.
- **Output Destination Setup**: Set the appropriate tray for received faxes.
- **Local Terminal Information**: Set the Local Name, Company Logo, G3 SIP Line ID, and other information.

Printing Fax Reports

CONFIGURING REPORTS

The Embedded Web Server allows you to configure three types of reports:

- **Activity Report**: This report provides a summary of faxes sent and received. You can generate this report from the printer control panel. By default, this report prints automatically after 100 fax transmissions and receptions. You can also generate this report manually.
- **Confirmation Report**: This report acknowledges the transmission of a fax sent to a single recipient. The Fax app generates this report automatically.
- **Broadcast Report**: This report acknowledges the transmission of a fax sent to multiple recipients. The Fax app generates this report automatically.

To configure these report:

1. In the Embedded Web Server, log in as administrator, then click **Apps > Fax**.
2. In the Fax Controls area, click **Activity Report**.
   - To enable activity reports, click **Print Activity Report**, then select **On**.
   - Configure the remaining settings as needed.
   - Click **Save**.
3. In the Fax Controls area, click **Broadcast Report**.
   - To enable confirmation reports, click **On**.
   - To get Report Contents, click **Print Only When Error Occurs**, select an option **All Communications** or **Communications with Error**.
   - Click **Save**.

PRINTING A FAX ACTIVITY REPORT

1. At the printer control panel, press the **Home** button.
2. Touch **Device Status > Print Reports > Job Status/Activity Reports**.
3. Touch **Activity Report > Print**.

Accounting

This chapter contains:

Xerox® Standard Accounting Tool..... 166
Network Accounting..... 169
Accounting Using an Auxiliary Device..... 171

Xerox® Standard Accounting Tool

Xerox® Standard Accounting Tool tracks the number of copy, print, scan, and fax jobs for each user. You can set different user limits for each type of job performed. You can reset limits remotely at any time. You can generate reports listing usage data for individual users, groups, or departments.

When Xerox® Standard Accounting Tool is enabled, before users can access services, they are required to log in to the device. Before printing documents from a computer, users are required to provide their account details in the print driver.

Note: If Xerox® Standard Accounting Tool is enabled, you cannot enable other accounting modes.

You can create a maximum of:

- 2499 unique Xerox® Standard Accounting Tool user IDs
- 500 General Accounts
- 499 Group Accounts

You assign all user IDs to one or more group accounts.

Note: Xerox® Standard Accounting Tool settings and account data are stored in the device. It is recommended that you back up settings using the Cloning feature. If Xerox® Standard Accounting Tool settings are lost or deleted, you can restore the settings using the clone backup file.

Before you begin:

- Install print and drivers on all user computers.
- If you require authentication, configure Local Authentication or Network Authentication.

ENABLING XEROX® STANDARD ACCOUNTING

1. In the Embedded Web Server, log in as administrator, then click **Permissions > Authentication and Accounting > Accounting Method**.
2. Select **Xerox Standard Accounting**, click **Save**.
3. In the What to Track window, select a tracking option.
   - **Track All:** This option records all scan, copy, and print activity.
   - **Only Track Color Copies and Prints:** This option records the number of color copies or prints only.
   - **Custom Tracking:** This option allows you to customize the functions to record. Select **Edit** and choose the functions to track, then click **Save**.
4. To block login information from displaying on the screen, for Mask Input, click **Enable**.
5. To save the changes, click **Save**.
6. When prompted to restart the printer, click **Change**.
7. After the printer restarts, log in as an administrator.

CREATING A USER ACCOUNT

1. In the Embedded Web Server, log in as administrator, then click **Permissions**.

2. In the User Accounts area , click **Edit**, then select **Add New Account.**
3. Type the User ID.
4. If the Login/Logout setting is configured to require user passwords, type the password for the user account, then retype the password.
5. Click **Add**.

EDITING THE ACCOUNT SETTINGS FOR INDIVIDUAL USERS

You can configure the following parameters for an individual user:

- Set the type of user for the device. You can select a basic user or an administrator.
- Set the type of user for printing. You can select a basic user or a custom role.
- Reset any personal changes to the home screen on the printer control panel.
- Link the printer to a PC user name to receive status messages.
- Set and reset limits on jobs sent to the printer.
- Designate a From email address for the Scan to Email app.

To edit the account settings for a user:

1. In the Embedded Web Server, log in as administrator, then click **Permissions**.
2. In the User Accounts area, click a user name.
3. In the Roles area:
   - To select between a basic user and an administrator, click **Device Operation Role**, select an option, then click **Save**.
   - To select the role for printing, click **Print Role**, select an option, then click **Save**.
4. To reset any personal changes to the home screen on the printer control panel, in the Personalizations area:
   a. Click **Delete**.
   b. When prompted to confirm, click **Delete**.
5. To designate an email address for the From line in the Scan to Email app, in the Email "From" Address area:
   a. Click **Edit**.
   b. In the Email Address field, type an email address, then click **Save**.

CHANGING A USER PASSWORD

1. In the Embedded Web Server, log in as administrator, then click **Permissions**.
2. Click the user name that you want to change.
3. Click **Change Password**, then type in the new password.
4. Retype the new password.
5. Click **Save**.

DELETING AN ACCOUNT

1. In the Embedded Web Server, log in as administrator, then click **Permissions**.
2. In the User Accounts area, select the user name that you want to change.
3. In the User Details area, click **Delete**.
4. At the confirmation prompt, click **Delete**.

GENERATING AND DOWNLOADING A XEROX® STANDARD ACCOUNTING 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, log in as administrator, then click **Permissions > Authentication and Accounting > Accounting Settings**.
2. Click **Download Xerox Standard Accounting Activity Report**.
3. On the Confirmation window, click **Download**.

   The document is saved automatically as a .csv file in the default download location on your computer hard drive.
4. Click **Cancel**.

RESETTING USAGE LIMITS

When users reach their maximum usage limit, they cannot use that feature until the administrator resets their limit. You can use the Reset option to reset all the usage data to zero.

1. In the Embedded Web Server, log in as administrator, then click **Permissions > Print Roles > Basic Printing User**.
2. Select the User Name and modify the usage limit.

Network Accounting

To enable accounting through a network server:

1. In the Embedded Web Server, log in as administrator, then click **Permissions > Authentication and Accounting > Accounting Method**.
2. Select **Network Accounting**, click **Save**.

To specify a network server to monitor the accounting:

1. In the Limits area, click **Setup**.
2. In the Limits Server area:
   - For Server URL, type a URL for the network server that manages accounting.
   - For Timeout, type the number of seconds that the printer waits idle before it disconnects from the server.
3. In the Jobs to Apply Usage Limits area:
   - To select functions to monitor, click the **Enable** toggle button.
   - If you selected Prints as a function to monitor, in the Job Limit Communication Error Handling section, select an action to perform in response to an error.
4. Click **Save**.

You can configure aspects of the login screen on the control panel. To configure this information:

1. In the Tracking Information area, click **Setup**.
2. To display information for a user, in the User ID area:
   - For Default Label, type the label that appears above the login field on the control panel.
   - For Default Value, type the default login string that appears in the login field on the control panel.
   - To require users to log in to the printer to retrieve usage information, for Ask Users, click the **Enable** toggle button.
   - To prevent login information from appearing on the control panel, for Mask Input, click the **Enable** toggle button.
3. To display information for a General Account, in the Account ID area:
   - For Default Label, type the label that appears above the login field on the control panel.
   - For Default Value, type the default login string that appears in the login field on the control panel.
   - To require users to log in to the printer to retrieve usage information, for Ask Users, click the **Enable** toggle button.
   - To prevent login information from appearing on the control panel, for Mask Input, click the **Enable** toggle button.
4. In the When to Prompt area, click each type of service, then select an option.
5. Click **Save**.

To require a login to retrieve accounting information:

1. In the Information Verification area, for **Enable**, click the toggle button.
2. Click **Verify Print Job**, then select an option.
3. Click **Save**.

Accounting Using an Auxiliary Device

Note: If the login method is set to Simple or Local, you cannot configure the printer to perform accounting functions with an auxiliary device.

To set up accounting with an auxiliary device:

1. In the Embedded Web Server, log in as administrator, then click **Permissions > Authentication and Accounting > Accounting Method**.
2. From the Accounting Method window, select **Auxiliary Device**, then click **Save**.

   The Auxiliary Device window appears.
3. In the Device Type area, select from the following options to use for payment:
   - **Coin/Cash Activated**
   - **Subtractive Card Activated (Example: Pre-paid Card)**
   - **Cumulative Card Activated (Example: Credit Card)**
4. In the Jobs To Track area, click the toggle buttons to select the activities to track. For example, **Copy** or **Print** or both.
5. In the Billing Settings area, click and select from the following options:
   - **Jobs with Insufficient Credit**: You can select from the options **Delete Job Immediately** or **Hold Job**.
   - **Charge Print Jobs**: You can select from the options **Charge by Card Number** or **Do Not Charge by Card Number**.
   - **Print Control with Cumulative Device**: You can select from the options **High Speed Printing** or **Track with Cumulative Device**.
   - **Scan Ahead for Copy Jobs**: You can select from the options **Disabled** or **Enabled**.
6. To save the settings, click **Save**.

Administrator Tools

This chapter contains:

Monitoring Alerts and Status 174
Fault History 175
Activating a Supplies Plan 176
Paper Tray Settings 177
SMart eSolutions 186
Configuring Stored File Settings 192
Retrieving Stored Files 193
Setting Default Touch Screen Settings 194
Taking the Printer Offline 195
Restarting the Device in the Embedded Web Server 196
Changing the Power Saver Settings 197
View Usage and Billing Information 198
Cloning 199
Public Address Book 200
Font Management Utility 203
Customizing Device Contact Information 204
Resetting and Restarting the Printer 205
Updating the Device Software 206
Date and Time Settings 207
Fax Speed Dial Setup Settings 208
Watermarks and Annotations 209
Memory Settings 211
Backup and Restore 212
Printer Management 213

Monitoring Alerts and Status

You can configure alert and status notices to be sent automatically as email messages to one or more recipients.

XEROX VITALS LIGHTBAR (OPTIONAL)

Xerox Vitals Lightbar is a compact, USB-powered LED designed for printers. While managing multiple machines, it provides a quick, at-a-glance status update to help operators stay informed and responsive without checking the UI constantly. It supports upto 64 addressable RGB LEDs and works across most Xerox® Fiery® EX Print Servers. For more information, refer to *Xerox® PrimeLink® C9265/C9275/C9281 Series Printer User Guide*.

SETTING UP JOB COMPLETION ALERTS

To set up job completion alerts for email recipients:

1. In the Embedded Web Server, click **Jobs > Job Settings > Notify Job Completion by Email**.
2. For Recipient Email Address, toggle enable button for **Report**, type up to five addresses for recipients to receive job completion alerts.
3. In the Message field, type the text to appear in the message.
4. For Targeted Jobs, select the types of jobs for which recipients receive notification when a job completes, then click **Save**.
5. For When to Notify, select an option for recipients to receive notification after all job completions or only after job errors occur.
6. Click **Save**.

SETTING UP DEVICE STATUS ALERTS

To set up device alerts for email recipients:

1. In the Embedded Web Server, click **Home** tab, in Notifications area, click **Settings**.
2. For each Recipient's Email Address, from the Send Notice drop-down list, select a notification frequency option.
3. In the Regular Notification Settings area, click **Edit** for each recipient, set the appropriate mail status notification.
4. In the Notice Frequency Settings area, select the notification options for frequency, date, and time.
5. Click **Save**.

Fault History

Use Fault History to view the log of recent printing faults. Faults are recorded in the log whenever the printer fails to print a job due to an error like a paper jam. The fault list appears with a code that identifies the type of fault and the date and time the fault occurred.

VIEWING FAULT HISTORY

1. In the Embedded Web Server, log in as administrator, then click **Home**.
2. For Notifications, click **Settings**.
3. To view a list of recent printer errors, click **Error History**.
4. Click **Close**.

Activating a Supplies Plan

To use a supplies plan, contact your Xerox equipment supplier or Xerox representative for a supplies plan code. To enable your device for a plan, activate the plan at regular intervals. To enter the code:

1. In the Embedded Web Server, click **Home**, in the Supplies area, click **Details**.
2. Go to Advanced Settings area, click **Supplies Plan**, then select **Supplies Plan Activation** or **Plan Conversion**.
3. Type the code.
4. Click **Apply**.
5. To restart the printer, follow the onscreen instructions.

Paper Tray Settings

ACCESSING PAPER TRAY SETTINGS

You can manage which paper options appear on the control panel and on the Paper Tray Settings screen. To access these options:

1. At the device control panel, log in as Administrator, press the **Home** button. For details, refer to Administrator Access at the Control Panel.
2. Touch **Settings > Device > Paper Tray Settings**.

CUSTOM PAPER SETTINGS

From the Paper Tray Settings screen, you can select the Custom Paper Name or Color feature to set a custom name for paper that is loaded in the device. You can use a maximum of 24 characters for each custom paper name.

Note: Use this feature for plain paper, 60–105 g/m^2, only.

To set a custom paper name or color:

1. At the device control panel, log in as Administrator, then access the **Paper Tray Settings** screen. For details, refer to Accessing Paper Tray Settings.

2. Select **Common Settings > Custom Paper Settings**, then change the following settings:
   - **Name**: Set name for the custom paper.
   - **Paper Type**: Select the paper type to be set to the custom paper.

     You can name Custom Type 1 to 5, and Custom Paper Color 1 to 5 using up to 24 characters, comprised of letters, numbers, and symbols, for each type and color. For example, you can use a name that shows the usage, such as `Color` for colored paper, and `Covers` for bond paper.
   - **Paper Weight**: Select the paper weight to be set to the custom paper.
   - **Adjust Alignment**: Select the alignment adjustment setting registered in Manual Alignment.
   - **Adjust Paper Curl**: Select the correction type registered in paper curl. To adjust the curl as an Administrator, refer to Creating a Custom Curl Profile as Administrator.
   - **Adjust Image Transfer**: Specify the percentage of the voltage value to be applied numerically or adjust it using sample print. It enables setting for the optimal image transfer value for the custom paper when the image is not transferred in the optimal image condition to paper.
   - **Adjust Regi-Loop**: When performing skew adjustment for the pre-register feed, the adjustment value can be set for each user paper. The adjustment value for the pre-register feed can be set in the range of –9 to 9 mm, in 0.3 mm increments.
   - **Side Shifting**: This function sets to adjust for side shift operation and running misalignment.
   - **Fold Position Adjustment**: Select the adjustment value registered in Adjust Finisher.
   - **Adjust Image Transfer for Trial Edge**: Adjust the voltage ratio of the second transfer roll in the transfer unit. When using heavy weight paper, if uneven colors due to transfer failure occurs only at the back edge of the paper, adjusting the voltage ratio of the second transfer roll may improve the transfer failure.

   Note: If the voltage of the second transfer roll is high or too low for the paper to be used, it may cause transfer failure. If a transfer failure occurs, change this number to adjust the voltage ratio.
   - **Adjust Image Transfer for Trial Edge**: Adjust the voltage ratio of the second transfer roll in the transfer unit. When using heavy weight paper, if uneven colors due to transfer failure occurs only at the back edge of the paper, adjusting the voltage ratio of the second transfer roll may improve the transfer failure.
   - **Adjust Image Transfer for Trial Edge**: Adjust the voltage ratio of the second transfer roll in the transfer unit. When using heavy weight paper, if uneven colors due to transfer failure occurs only at the back edge of the paper, adjusting the voltage ratio of the second transfer roll may improve the transfer failure.
   - **Adjust Fusing Temperature**: Adjust the fusing unit temperature. if the toner peels off the paper, increasing the temperature may improve it.

   Note:
     - If you decrease the temperature too much, the toner on the high density images is not fused enough and it may peel off from the paper.
     - If the temperature is raised too high when printing on the light weight paper, a paper jam may occur in the fusing and peeling section.

- When changing the settings, check the print results. Return the value to default Zero after printing, because the environmental condition is always different.

- **Adjust Fusing Speed**: If printer defects such as image distortion, image stretching, or image shrinking occur in the image on the later half of the paper, adjusting the speed of fusing unit may improve the printing defects. When the image is shrinking, speed the fusing unit up and when it is stretching, slow the fusing unit down.
- **Adjust Primary Transfer Current Y/ Adjust Primary Transfer Current M/ Adjust Primary Transfer Current C/ Adjust Primary Transfer Current K**: Adjust the voltage ratio of the first transfer roll in the transfer unit. If blurring, white streaks, after image ghosting occur due to poor transfer, adjust the voltage ratio of the first transfer roll in the transfer unit improves the transfer failure.
  1. Increase the voltage ratio when blurring occurs in the image on the paper edge (an area about 10 mm).
  2. Decrease the voltage ratio when the white streaks or after image ghosting occur in the halftone area.
- **Adjust Fusing Nip Pressure**: If the toner is removed, increase the value to increase the pressure of the fusing unit.

Note:

- Use the function when it is not improved even adjusting fusing temperature.
- A guideline for improving toner peeling on envelopes from two to four. If the adjustment value is too large, paper may be skewed.

- **Glass Mode**: Reduces the speed and produces a glossy output.
- **Adjust Air Volume for Feeder Fan**: Increase the air volume of the conveyor fan when the short paper (A4, Post Cards), thick paper, or curled paper is easily jammed.

Note: Adjust step by step. If the air volume is too large, another trouble may occur.

ESTABLISHING START-UP ATTRIBUTES

You can change and set the paper tray attributes that appear on the control panel when the device starts.

To modify the paper tray attributes that are available at start up:

1. At the device control panel, log in as Administrator, then access the **Paper Tray Settings** screen. For details, refer to Accessing Paper Tray Settings.
2. Select **Common Settings > Change Paper Settings During Loading**.
3. Touch **Enabled** or **Disabled**.

PAPER TYPE PRIORITY

You can define the priority of the trays to use when paper of the same size and the same orientation is set in multiple trays for automatic tray selection.

- **Auto Paper Selection**: A paper tray that contains the appropriate paper is selected automatically by the Xerox device for copying or printing.
- **Paper Type Setting**: The Paper Type setting is prioritized over the paper tray priority settings. If different paper types appear in the same priority sequence, the paper is determined by the paper tray priority sequence. A tray that contains a paper type set to Auto Paper Off is not included in the automatic tray selection.

Note: Not all print servers adhere to the Paper Type Priority feature setting.

Setting Paper Type Priority

To set paper type priority:

1. At the device control panel, log in as Administrator, then access the **Paper Tray Settings** screen. For details, refer to Accessing Paper Tray Settings.
2. Touch **Common Settings > Paper Type Priority**.
3. Select the option you need. The following table lists the current default settings for the paper type priority.

ITEM	CURRENT SETTING
Plain	First
Plain reloaded	Auto paper Off
Recycled	Second
Bond	Third
Blank Side	Auto paper off
Custom type 1	Auto paper off
Custom type 2	Auto paper off
Custom type 3	Auto paper off
Custom type 4	Auto paper off
Custom type 5	Auto paper off

4. Select a feature.
5. Touch **OK**.

SETTING PAPER TRAY ATTRIBUTES

From the Paper Tray Settings area, you can set the size and type of paper loaded in the trays.

To set paper tray attributes:

1. At the control panel, access **Paper Tray Settings**. For details, refer to Accessing Paper Tray Settings.
2. Select the tray that you want to change.
3. Select the paper type, paper size, and paper color. For Auto Paper Select, select the color.

4. Touch **OK**.

SETTING UP A DEDICATED PAPER TRAY

Users can load only a specific size and type of paper into a dedicated paper tray. When they use the printer, users are prompted to load the specified paper into the tray. If the specified paper is not used, the printer reports an error.

You can set the following trays as dedicated paper trays:

- Trays 1–4
- Trays 6 and 7 for the High Capacity Feeder or Oversized High Capacity Feeder

To set up a dedicated paper tray to use a particular size and type of paper:

1. At the control panel, access **Paper Tray Settings**. For details, refer to Accessing Paper Tray Settings.
2. Select the tray that you want to set up as a dedicated paper tray.
3. Select the paper type, paper size, and paper color.
4. Enable **Purpose-Specific Tray**.
5. Touch **OK**.

CHANGING PAPER SETTINGS DURING TRAY LOADING

To set the paper tray attribute options that are available when paper is loaded:

1. At the device control panel, log in as Administrator, then access the **Paper Tray Settings** screen. For details, refer to Accessing Paper Tray Settings.
2. Select **Change Paper Settings During Loading**.
3. Select **Off** or **On**.

ESTABLISHING BYPASS TRAY DEFAULTS

The Paper Tray Settings area allows you to define up to 20 paper sizes that appear when Tray 5 (Bypass) is loaded and in what order the paper sizes appear.

You can load the following paper sizes in Tray 5:

- A/B Series Size: A3, A4, A5, A6, JIS B4, JIS B5, and JIS B6
- Inch Size includes: 13 x 19 in., 13 x 18 in., 12.6 x 19.2 in., 12 x 18 in., 11 x 17 in., 11 x 15 in., 8.5 x 14 in., 8.5 x 13 in., 8.5 x 11 in., 8 x 10 in., 7.25 x 10.5 in., 5.5 x 8.5 in., and 5 x 7 in.
- Others: SRA3, A4 Oversized, 9 x 11 in., 215 x 315 mm, 8K, 16K, 100 x 148 mm, 148 x 200 mm, 4 x 6 in.
- Envelope Size Includes: Chou 3, Kaku 2, C4, and C5
- Custom Size: Includes paper sizes up to Banner 330 x 660 mm (13 x 26 in.)

To define and set the paper sizes that appear when Tray 5 is loaded with paper:

1. At the control panel, access **Paper Tray Settings**. For details, refer to Accessing Paper Tray Settings.

2. Touch **Tray 5 - Standard Size Defaults**.
3. Select the paper size that you want. Select from **A/B Series Size**, **Inch Size**, **Others**, or **Manual Size Input**.
4. Touch **OK**.

CUSTOMIZING THE PAPER SUPPLY SCREEN

Use this feature to specify whether the options Usage or Size Detection appear on the Paper Supply screen.

To define the paper tray attributes that appear on the Paper Supply screen:

1. At the device control panel, log in as Administrator, then access **Paper Tray Settings**. For details, refer to Accessing Paper Tray Settings.
2. Select **Common Settings > Customize Paper Supply Screen**.
3. Select the needed option:
   - **Disabled**: This option hides the items that are specified in the Paper Size setting.
   - **Size Detection**: This option shows the setting for the Paper Size setting.
   - **Usage (Auto Paper Select)**: This option shows the setting for the Auto Paper Select setting.

PAPER TRAY PRIORITY

Set the priority of the trays to use when paper of the same size and the same orientation is set in the multiple trays or print data does not include the paper tray information for automatic tray selection.

Auto Paper selection means that a tray containing the appropriate paper is selected automatically by the device for copying or printing. This setting applies to Trays 1 to 4 and 6 (optional). You cannot apply this setting to Tray 5.

Note: Not all Print Servers (DFEs) adhere to this feature setting.

Setting Paper Tray Priority

To set the paper tray priority:

1. At the control panel, access **Paper Tray Settings**. For details, refer to Accessing Paper Tray Settings.
2. Select the desired tray for priority.
3. Touch **Priority**.
4. Touch each tray, then set the corresponding priority, or exclude the tray from automatic switching.

Note: If you include tray 5 in your priority list, it must be the last tray in your priority settings.

5. After you have set the priority for all trays, touch **OK**.

MANAGING AUTOMATIC TRAY SWITCHING

From the Paper Tray Settings area, you can set the alternative tray or paper to use when the paper runs out in the selected tray.

Note: Not all print servers adhere to the Auto Tray Switching feature setting.

To manage automatic tray-switching controls:

1. At the control panel, access **Paper Tray Settings**. For details, refer to Accessing Paper Tray Settings.
2. Touch **Common Settings > Auto Tray Switching Control**.
3. To change a setting:

   a. Touch an option, then touch **OK**.

   Use this method to change the following settings:

   - **Auto Tray Switching**: Touch **Enable during Auto Select** or **Enable for Same Paper Type/Color**. If you select Enable during Auto Select, the printer switches the tray when a user selects Auto Select in the Copy screen or selects Paper Select in the print driver.
   - **Targeted Paper Type (Copy Jobs)**: Touch **According to Priority Assigned** or **Selected Paper Type Only**. If you select According to Priority Assigned, the paper type is determined according to the settings in Paper Type Priority. If you select Selected Paper Type Only, you can specify the paper type.
   - **Targeted Paper Color (Copy Jobs)**: To determine the alternative color to use, touch **All Colors** or **Selected Color Only**.

Note: If you set a tray to Exclude from Auto Tray Switching in Paper Tray Priority, the tray is not included in automatic tray switching.

The device does not switch the tray automatically in the following cases:

- Tray 5 is selected
- The tray that contains paper other than plain paper, recycled paper, or plain reload paper is selected
- The tray that contains paper that is set as Auto Paper Off in Paper Type Priority is selected.

IMAGE QUALITY

When copying or printing a document, the device applies the image-quality settings that are defined in the Paper Tray Attributes area of the control panel. The type of paper that is set in Paper Tray Attributes and the image-quality processing method that is specified for that type of paper control the amount of ink transfer, speed, and fuser temperature applied.

Note: The image-quality setting for these paper types changes the weight range that appears for each paper type.

Specifying Image Quality Settings

To optimize the image quality of the output, select the media weight range to apply to a print or copy job.

To specify image quality settings:

1. At the device control panel, log in as Administrator, and then access the Paper Tray Settings screen.

   For details, refer to Accessing Paper Tray Settings.

2. To navigate the menu, use the up and down arrow keys, then touch **Common Settings > Image Quality**.
3. Select the paper type that you want to change.

   The Image Quality settings for the paper type that you selected appear. The settings represent the media weight range.

4. Select a different setting, then touch **OK**.

Note: For all custom paper types, the options available include **Plain A**, **Plain B**, **Plain C**, and **Plain D** paper. For more information, refer to Article ID: KB0427162 Unable to Program Paper Tray with Desired GSM Range from Paper Type Selection Menu.

NVM ADJUSTMENTS REQUIRED FOR GBC ADVANCEDPUNCH PRO (APP) SOFTWARE VERSION

If you encounter paper jams in GBC AdvancedPunch Pro, then check the GBC Software version and adjust the NVM values according to the table. To find the GBC APP software version, refer to *GBC user interface*.

GBC SOFTWARE NVM	NVM SETTINGS
769–401	**0**: Software Version lower than 18.13 **1**: Software Version 18.13 or higher

PAPER CATALOG

The paper catalog allows you to define a unified set of stocks for an entire fleet of devices. The system administrator defines the paper stocks on the print server. The most commonly used paper stocks appear at the top of the list in the paper catalog. When loading media in a paper tray, the user can use the paper catalog to assign a specific paper stock to the tray. When submitting a print job or copy job, the user can use the paper catalog to choose a specific paper stock for the job.

The EFI configuration for paper catalog allows you to store up to 400 paper catalog types.

To be available for use, the paper catalog must be enabled. You can enable or disable paper catalog at the control panel or in the Embedded Web Server using the following codes:

- Enable: `*3151333451`
- Disable: `*3151333450`

Note: When typing the code, be sure to include the asterisk (*).

For enablement instructions, refer to Enabling Services and Options.

For details and setup instructions, refer to www.efi.com.

Assigning a Paper Stock to a Tray Using Paper Catalog

To assign a paper stock to a tray using the Paper Catalog:

1. Send a CSV file through the JDF to the appropriate location on the Print Server (DFE).

   The stock list in the CSV file replaces the Stock Library and is transferred to the device for use during tray programming.

2. Open the paper tray and load the paper stock.
3. Close the paper tray and touch **Paper Catalog** on the device control panel touch screen.
4. Select the appropriate paper stock from the list and touch **OK**.

   The control panel touch screen shows the paper stock type loaded in the tray.

5. Touch **Confirm**.

   The stock is associated with the tray and the association is reflected in the tray settings on the Print Server (DFE).

SMart eSolutions

Note: SMart eSolutions is called Xerox® Remote Print Services now. For more information, refer to Xerox Remote Print Services.

SMART ESOLUTIONS OVERVIEW

SMart eSolutions is a collection of features and services that automates and simplifies the administration of Xerox® devices. These features include:

- Meter Assistant: The Xerox® MeterAssistant® provides Automatic Meter Reading (AMR). AMR automatically submits billing meter reading data that is used for customer billing purposes.
- Supplies Assistant: The Xerox® SuppliesAssistant® provides Automatic Supplies Replenishment (ASR). ASR proactively orders device components such as toner.
- Maintenance Assistant: The Maintenance Assistant provides Automatic Information Forwarding (AIF). AIF provides usage counters and fault conditions for Xerox technicians to manage device support requirements.

Note: Specific enablement and support of remote services features varies according to Xerox® device model, configuration, and operating company.

SMart eSolutions is enabled via a secure internet connection between the printer and Xerox using Secure Socket Layer (SSL) protocols and 256-bit encryption. Only device performance information is sent to Xerox through the secure connection.

CONFIGURATION PLANNING

NO.	TASK	INFO FROM TASK (IF RELEVANT)	
1	Verify that you have authorized Internet connectivity for the device and that the device is physically connected to the network.		
2	Print a Configuration Report and record the device IP address. Refer to Printing the Configuration Report.		
3	For information on DNS Settings, refer to Configuring TCP/IP Settings in the Embedded Web Server. DHCP Server automatically provides DNS information, or complete the following sections, where relevant:		
	a. DNS Server Address:		
	b. Alternate DNS Server Address 1: (if required)		
	c. Alternate DNS Server Address 2: (if required)		
	d. Domain Name:		
	e. Dynamic DNS Registration Used: (if required)		
	f. Connection Timeout: (if required)		

NO.	TASK	INFO FROM TASK (IF RELEVANT)	
4	Confirm HTTP Proxy Server (if used) is configured to allow access to HTTP/HTTPS ports 80 and 443. For details, refer to Proxy Server.		
5	HTTP Proxy Server Address:		
6	HTTP Proxy Server Port:		
7	HTTP Proxy Server Authentication Account (if used):		
	a. User Name:		
	b. Password:		
8	Confirm Firewall Proxy Server (if used) is configured to allow access to HTTP/HTTPS ports 80 and 443.		

CONFIGURING SMART ESOLUTIONS

Enrolling and Setting up Communication

To enable SMart eSolutions and set up communications:

1. In the Embedded Web Server, click **System > SMart eSolutions**.
2. For SMart eSolutions Enablement, select **Enabled**.
3. For Daily Upload Time, click **Settings** in the Upload Schedule area, enter the time of day for communication transmissions to occur between the device and the communication server.
4. For Payload Type, in the Transmission Data area, click **Payload**, select an option.
5. To test the communication between your device and the Xerox server, click **Test Connection**.

   The screen changes to simulate communication transmission. The screen changes a second time to confirm success or failure of the test.
6. Click **OK**.

Setting Up Email Notification

To set up email notifications:

1. In the Embedded Web Server, click **System > SMart eSolutions > Settings** go to Email Notifications area.
2. For Email Addresses, click in a field, then type an email address. You can specify up to five email addresses.
3. For Send Notification, select notification options, as needed.
4. Click **OK**.

Setting Up Software Updates

To set up software updates:

1. In the Embedded Web Server, click **System > Software Update**.
2. To allow software updates, for Software Updates, select **Enabled**.
3. For When should the Device check for updates?, select the update frequency.
4. To set up notifications for the software updates:
   a. For Whom to notify if an update is available?, click **Setup**.
   b. For Email Address, click a field, then type an email address.
   You can specify up to three email addresses.
   c. Click **OK**.

Terminating the SMart eSolutions Service

To terminate the service:

1. In the Embedded Web Server, click **System > SMart eSolutions > Disable**.
2. Select the person who is trying to disable this feature.
3. Type a reason for disabling the service.
4. Click **Disable**.

After you request the service termination, one more data transmission occurs.

VIEWING SMART ESOLUTIONS INFORMATION

Uploading Smart eSolutions Data

1. In the Embedded Web Server, log in as administrator, then click **System > Smart eSolutions**.
2. Click **Download Data**.

   The document is saved automatically as a .csv file in the default download location on your computer hard drive.

TROUBLESHOOTING

If you are experiencing problems with the SMart eSolutions setup, review the following information for assistance.

For more information on SMart eSolutions, refer to Xerox Remote Print Services.

A Xerox® Remote Services Security White Paper is available at https://security.business.xerox.com/en-us/documents/white-papers/.

Troubleshooting Internet Access Problems

If you are using a proxy server or firewall to control access to the Internet, verify the settings.

Verifying Connectivity with the Proxy Server

To verify connectivity with the proxy server, use a computer connected to the same subnet as the device.

Note:

- To confirm your settings, use the information that you gathered on the installation worksheet.
- Your network can use the host name for devices that include the proxy server. The use of host names requires a name service, such as DNS. If you are not using DNS, identify the proxy server by its IP address.

1. On your computer, open a command prompt.
2. At the command prompt, use the ping command to ping the IP address of the proxy server.

   No reply to the ping command indicates that there are network connectivity issues between the device and the proxy server.
3. If there is no reply to the ping command, investigate the issue.
   - Verify the information entered on the device, especially the default gateway.
   - Verify the proxy server address.
   - Verify that the default HTTP (80) and HTTPS (443) ports are not blocked at the proxy server.
   - Determine whether the proxy server requires authentication. If authentication is required, obtain the user name and password. In the Embedded Web Server, type the information for the proxy server.
   - Verify the proxy server IP address and the port number. If your network is using DNS and host names, verify the host name or the fully qualified domain name of the proxy server.
   - If the proxy server was provided instead of an IP address, at the control panel, ensure that DNS is enabled.

Verifying the Firewall Settings

A firewall can block access to the Internet. Verify the following information with the IT Administrator:

- The firewall rules are set to allow the device access to the Internet.
- The firewall does not require a user name and password for outbound access.
- The firewall does not block the standard HTTP (80) and HTTPS (443) ports.

Verifying the Network Device Addresses

A firewall, proxy server, and DNS server are not the same thing. It is possible for the same physical host to perform more than one or all of the functions. However, usually these functions are not on the same host. If the same IP address is given for more than one of these functions, verify with your IT administrator that this information is correct.

Troubleshooting Incorrect Proxy Server Settings

Finding the Proxy Server in Windows

You can find the proxy settings with a Windows computer, then use the settings on your device. To find the proxy server settings:

1. On a Windows computer, open the control panel in classic view.

2. Click **Internet Options**.
3. Click the **Control Panel > Network and Internet > Internet Options** tab, then click **Connection and LAN Setting**.
   The address and port number for the proxy server used by your computer appear in this window.
4. If a proxy server is enabled, click **Advanced**.
   The Proxy Settings window shows the proxy servers used for each protocol.
5. Enter the proxy settings into your device using the Embedded Web Server. For details, refer to Proxy Server.

Finding the Proxy Server in Mac OSX

You can find the proxy settings with a Macintosh computer, then use the settings on your device. To find the proxy server settings:

1. At a Mac OS® X desktop, click the Apple icon, then **System Preferences**.
2. Click **Network**.
3. Click the network adapter that is in use, then click **Configure**.
4. Click the **Proxies** tab. If your computer is configured to connect to the Internet through a proxy server, the server address and port number appear here.

Enter the proxy settings into your device using the Embedded Web Server. For details, refer to Proxy Server.

Troubleshooting Incorrect DNS Settings

To verify the DNS Settings:

1. On a Windows computer on the same subnet as the device, open a command prompt.
2. To display the IP configuration information, at the prompt, type `ipconfig/all`.
3. Write down the connection-specific DNS suffix, which is the domain name. Write down the IP addresses of the DNS servers.
4. To verify connectivity, type `ping`, then type the IP address of the DNS server. If there is network connectivity, the server replies to the ping command.
5. To verify connectivity with the default router, type `ping`, then type the IP address of the default gateway. If there is network connectivity, the gateway replies to the ping command.

Use the information to verify the DNS server and default gateway settings on your device. For details, refer to TCP/IP.

Unconfirmed Support for SMart eSolutions

Note: This service is available for US-registered accounts only.

To perform a device eligibility test:

1. Access the site: www.accounts.xerox.com/meters/amr-capability-test.jsf.
2. For Enter the machine serial number, type the device serial number.

3. To indicate whether the device is in a network area, select **Yes** or **No**.

   Note: To support SMart eSolutions, the device must be connected to the network.

4. Click **Submit**.
   A status message appears confirming that your device is eligible or not eligible for SMart eSolutions capabilities.

5. If necessary, to enter another serial number, click **Clear Form**.

Connectivity Failed Following Device Restart

After a device restart or software update, ensure that the device is still communicating with the Xerox host. Ensure the communication even if you performed a clone of the device settings. Verify the connectivity settings, validate, and test communication as described in this document.

Configuring Stored File Settings

To configure stored file settings:

1. At the control panel, press the **Home** button.
2. Touch **Settings > Device > App Settings > Job Settings**.
3. To change a setting, touch **Save**.
   Use this method to change the following settings:
   - **File Retention Period**: To minimize the disk space consumed by stored files, the printer can delete files after a specified time period. Touch **On**, then select the number of days to retain files are kept before deletion, and time that are deleted, then click **OK**.
   - **Stored Job Retention Period**: Touch **On**, then select how long print files stored on the printer are kept before being deleted. To keep files until the date specified in the Expiration Date for Files in Folder setting, touch **Same Expiration Date as Files in Folder**. To delete jobs every time the printer is powered off, for Power Off Deletes Jobs, touch **Yes**.
   - **Display Default of Stored Print Job List**: Touch **List** or **Thumbnail**.
   - **Print Job Confirmation Screen**: Touch **Enabled** or **Disabled**. When Disabled is selected, stored files are deleted after they are printed.
   - **Preview Generation**: Set the preview generation to **On** or **Off**.
   - **Duration for Preview Generation**: To specify the length of time for the preview to display, touch **Limited**, then specify the length of time between 10 and 900 seconds. To specify an unlimited time for the preview, select **No Limit**.
   - **Minimum Passcode Length for Stored Jobs**: Specify the minimum number of allowed password digits between 0 and 12 for password-protected print jobs.
   - **Print Order for All Selected Files**: Specify the order in which files are printed when a user prints all stored files.

Retrieving Stored Files

To specify the settings for retrieving stored files:

1. In the Embedded Web Server, login as administrator, click **Network > Protocols > HTTP**.
2. If needed, for Retrieve Scanned Files / Files in Folder, select **Retrieve only when proxy is bypassed and HTTP/1.1 is used**.
3. For Retrieve Scanned Files / Files in Folder with HTTP/1.1, in Internet Services Settings area, click **Enable** toggle button.

Setting Default Touch Screen Settings

To set the default touch screen settings:

1. At the control panel, press **Home**.
2. To set the control panel default screens and buttons, touch **Settings > Device > System Settings > Screen / Button Settings**.
3. To change a setting:
   a. Touch an option, then touch **OK**.
   b. Use this method to change the following settings:
   - **Screen Default**: Set the screen that appears when the printer is powered on.
   - **Home Screen Default**: Set the screen that appears when the Services button is pressed.
   - **Screen After Auto Clear**: Set the service screen that appears when a certain amount of inactive time has passed for the Auto Clear feature. To revert to the last service screen used, touch **Last Selection Screen**, or to revert to the main Services screen, press the **Home** button.
   - **Auto Display of Login Screen**: To set the screen to prompt users automatically to log in when authentication is configured, touch **On**.
   - **Services Home**: Specify the service icons that appear when a user presses the Services Home button.
   - **Display One-Touch Buttons**: To set one touch buttons, click **Enable**.
   - **User name on login Icon**: To set given user name, select **Shorten** or **Do not Shorten**.
   - **Job Type on Job Status Screen**: Specify the types of jobs that appear when the Job Status button is pressed.
   - **Default Language**: Set the default language for the control panel.
   - **Screen Brightness**: Adjust the brightness of the screen.
   - **Reconfirm Email Recipient**: If you do not want users to reconfirm email recipients, touch **Do not Confirm**. To require users to retype recipient addresses when they send an email, touch **Always Reconfirm Recipient** or **Reconfirm if Multiple Recipients**.
   - **Reconfirm Fax Recipient**: To require users to retype recipient addresses when they send a fax, touch **Always Reconfirm Recipient** or **Reconfirm if Multiple Recipients**.
   - **Display Warning Screen After Inserting USB**: Select the screen that appears when a user inserts a USB drive in the Xerox device.
   - **Display Supplies Screen**: Select when the consumables screen is displayed.
   - **Keyboard Input Restriction**: Set the restriction to **Off** or **On (ASCII Only)**.
   - **Effect of holding Down +/- Buttons**: To enable or disable fast scrolling, touch **Change Value Continuously** or **Change Value Once**.
   - **Disable Notification Messages**: To disable notification messages, touch **Enable**.
   - **Message Display Time**: To set the duration of the message to be displayed.
   - **Foot Switch Action on Preview Screen**: To specify which button works when Foot Switch is pressed on the preview screen that shows. This setting applies only when Foot Switch is connected to device.

Taking the Printer Offline

To prevent the printer from either sending or receiving jobs over the network, you can take the printer offline. While the printer is not processing jobs, you can perform printer maintenance. When the printer is offline, any services, such as Network Scanning, are unavailable.

Note: Taking the printer offline does not power off the printer.

To take the printer offline:

1. At the control panel, press the **Home** button.
2. Touch **Settings > Device Status > Print Mode**.
3. Touch toggle switch icon to **Disable** Online to enable printer offline.

Restarting the Device in the Embedded Web Server

To restart the device using the Embedded Web Server:

1. In the Embedded Web Server, click **Home** tab, then click **Support**.
2. At the bottom of the Support page, click **Restart Device**, then click **Restart**.

Note: Restarting the device can take up to five minutes. During this time, network access is not available.

Changing the Power Saver Settings

The Power Saver feature has two modes:

- Low Power: After remaining inactive for a preset time, the printer enters Low Power mode.
- Sleep: After entering Low Power mode and remaining inactive for another preset time, the printer enters Sleep mode.

To change the power saver settings:

1. In the Embedded Web Server, click **System > Power Saver**.
2. For Time to Low Power Mode, type a time between 1 and 120 minutes.
3. For Time to Sleep Mode, type a time between 1 and 120 minutes.
4. To schedule a power-off time, for Scheduled Power Off, select **On**, then type the time for the power off.
5. For Sleep Mode Settings, select **Prioritize Power Saver** or **Prioritize Wake Up Time**.
6. For Enter Power Saver After Printing Ends, select **Immediately After Auto Printing Ends** or **According to Power Saver Timer Settings**.
7. For Power Saver Deactivation, select **Deactivate all**, **Deactivate Partially as Required**, or **Deactivate Partially When Printing / Job Auto Processing**.
8. For Auto Power Off, select **On** or **Off**.
9. For Smart WelcomEyes, click **Enable** toggle button, then click **Enable** toggle button for Exit Power Saver by Smart WelcomEyes.
10. For Smart WelcomEyes and Exit Power Saver by Smart WelcomEyes, click **Enable** toggle buttons.
11. Click **Save**.

View Usage and Billing Information

BILLING INFORMATION

The Billing Information page shows the count for pages printed or generated in black and white or color for billing purposes.

1. In the Embedded Web Server, click **Home** in Billing/Usage area, click **Details**.

   The list of pages printed or generated by device appears.

2. When finished viewing the information, click **Close**.

USAGE COUNTERS

The Usage Counters page displays the total number of pages printed or generated by the device.

1. In the Embedded Web Server, click **Home** in Billing/Usage area, click **Details**.
2. For Usage Counters, click **Usage Counters**.
   A detailed list of pages printed or generated by the device appears.

ENABLING THE BILLING IMPRESSION MODE

The Billing Impression Mode (BIM) feature defines how the printer accounts for impressions made on oversized pages, for example, on Tabloid or Ledger 279 x 432 mm (11 x 17 in.). With BIM enabled, oversized prints are counted as two Letter prints that measure 215.9 x 279.4 mm (8.5 x 11 in.).

To enable BIM, contact your Xerox® service representative, and request an activation code. To enable BIM on the printer:

1. In the Embedded Web Server, click **Home** in Billing/Usage area, then click **Details**.

   The list of pages printed or generated by device appears.

2. For Impression Mode, click **Impression Mode**.
3. Type the PIN activation code.
4. Click **Apply**.

Cloning

Cloning allows you to save your current printer configuration and app 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.

Note: Disable FIPS 140 mode before you install a clone file. For details, refer to FIPS 140.

To determine the software version:

1. In the Embedded Web Server, click **System**.
2. Click **Software Update**.
3. In the Software Update area, view the current version.

CREATING A CLONE FILE

1. In the Embedded Web Server, login as administrator, then click **Home**.
2. In the Quick Links area, click **Cloning**.
3. Click **Create**.
4. In the Create Clone File area, select the apps and features that you want to include in the clone file.

   Note: To include Personal Favorites in the exported clone file, include Address Book, Authentication, Authorization, Accounting, and Personalization among the selected features.
5. Click **Create**.
6. Save the downloaded file to a selected location.
7. Click **Close**.

INSTALLING A CLONE FILE

1. In the Embedded Web Server, login as administrator, click **Home**.
2. In the Quick Links area, click **Cloning**.
3. Click **Install**.
4. Click **Select**.
5. Navigate to the location of the clone file, select it, then click **Open**.
6. Click **Install**.
7. Click **OK**.

XEROX® DEVICE MANAGER CLONING FEATURE

These printers support the Xerox® Device Manager cloning feature. The cloning feature allows delivery of a clone file to the device with credentials for authentication. For more information on how to use the cloning feature, refer to *Xerox® Device Manager* documentation.

Public Address Book

The Public Address book stores email addresses, internet fax addresses, and fax numbers.

Note: An Internet Fax Address is the email address of an Internet fax machine.

ADDRESS BOOK OPTIONS

Based on your network and device configuration, you can use the following methods to manage your email addresses and fax numbers:

- LDAP Directory: If your network is connected to an LDAP server, you can configure the printer to look up addresses from the LDAP directory.
- Public Address Book: If you do not have an LDAP server, you can use the Public Address Book to store fax device phone numbers, Internet fax addresses, and email addresses on the device.
- LAN Fax Address Book: The LAN Fax feature has a separate directory for storing and managing addresses. For details, refer to the print driver help.

You can configure the device to access an LDAP directory, and a Public Address Book. If you have both methods configured, users can choose to use either address book.

EDITING THE PUBLIC ADDRESS BOOK AS A CSV FILE

If you have many addresses to manage, you can create a list of addresses in a spreadsheet application. You then save the information as comma-separated values in a file with a **.csv** file extension, then upload the file to the printer.

The printer recognizes the second row in the CSV file as the first data entry. The first row contains headings for the data in each column. The default column heading names are Name, Email Address, Fax Number, and Internet Fax Address. Other columns in the file contain data for other services and features, for example network drives.

NAME	EMAIL ADDRESS	FAX NUMBER	INTERNET FAX ADDRESS
Jim Smith	jim.smith@corp.com	1234567898	faxmachine.one@corp.com
Matt Lukas	Matt.Lukas@corp.com	4566544985	faxmachine.two@corp.com
Richard Allen	richard.allen@corp.com	7899877754	faxmachine.three@corp.com

Downloading a Sample CSV File

To download a sample file:

1. In the Embedded Web Server, click the **Address Book** tab.
2. In the Address Book area, click **Download Template**.
3. To reconfirm template download, click **Download**.

   A **.csv** format file gets downloaded in your computer.

Downloading a Sample CSV File with Headings Only

To download a file that contains sample headings:

1. In the Embedded Web Server, click the **Address Book** tab.
2. In the Address Book area, click **Export to Address Book**.
3. Click **Export**.
4. To save the file to your computer, follow the on-screen instructions.

IMPORTING AN ADDRESS BOOK FILE

To import an Address Book file:

1. In the Embedded Web Server, click **Address Book**.
2. In the Address Book area, click **Import Address Book**.
3. To import a new address book file, in the Import Address Book File area, click **Browse**.
4. Select the file with the **.csv** file extension, then click **Open**.
5. For First row of the .CSV file, select **Column headings** or **Recipient data**. If you downloaded and edited a sample CSV file, select **Column headings**.
6. Click **Next**.
7. On the Import page, in the Imported Heading column, select the labels from your imported file that you want to map to the labels in the Address Book.
8. Click **Import**.

ADDING, EDITING, AND DELETING ADDRESS BOOK ENTRIES

Adding a Name

To add a name to the Address Book:

1. In the Embedded Web Server, click the **Address Book** tab.
2. In the Address Book area, click **Add > New Contact**.
3. Edit the fields in the New Contact area.
4. Click **Save**.

Editing a Name

To edit a name in the Address Book:

1. In the Embedded Web Server, click the **Address Book** tab.
2. Next to the name you want to edit.
3. Edit the fields in the New Contact area and provide more detailed information.
4. Click **Save**.

Deleting a Name

To delete a name from the Address Book:

1. In the Embedded Web Server, click the **Address Book** tab.
2. For the name that you want to delete, click **Delete**.
3. To confirm the deletion, click **Delete**.

Deleting All Names

To delete all names from the Address Book:

1. In the Embedded Web Server, click the **Address Book** tab.
2. In the Address Book area, click **Tools > Delete All Contacts**.
3. To confirm the deletion, click **Delete**.

Importing Address Book Data

You can copy the Address Book data from files that are exported from other devices, and save the files to your computer as comma-separated values files. To import an Address Book file from another device:

1. In the Embedded Web Server, click Address Book, then click **Tools**.
2. Click **Import Address Book**.
3. To import a new address book file, for Import Address Book Data, click **Browse**.
4. Select the CSV file, then click **Open**.
5. Select **Add to Existing** to add new contacts or **Overwrite** by deleting all the existing contact for importing the address book
6. Click **Import**.

Exporting Address Book Data

You can export the Address Book from your printer for use on another device. To export the Address Book to a comma-separated values file:

1. In the Embedded Web Server, click **Address Book**.
2. In the Address Book area, click **Tools > Export Address Book**.
3. Click **Export**.
4. To save the exported file, follow the onscreen instructions.

Font Management Utility

The Xerox® Font Management Utility is a utility that allows you to manage fonts for one or more printers on your network. You can use the font management utility to download your company branded fonts or unicode fonts to support multiple languages on your printer. You can add, delete, or export fonts. You can select printers in the utility printer list that you want to display.

To download Xerox® Font Management Utility, go to www.support.xerox.com, enter your product, name, then select **Drivers & 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.

Customizing Device Contact Information

The support page in the Embedded Web Server displays contact information for service and supplies and for the system administrator. You can customize this information to display your company contact information.

To add custom information:

1. In the Embedded Web Server, click **Home** tab, then click **Support**.
2. Click **Edit**.
3. Update the fields as needed, then click **Save**.

XEROX ONLINE SUPPORT

Note: If your network uses a proxy server, configure the Proxy Server settings of the printer to ensure that the printer can connect to the Internet.

To enable Connect to Xerox Online Support:

1. In the Embedded Web Server, click **Home**.
2. In the Quick Links area, click **Support**.
3. In the Options area, click **Online Support**.

Resetting and Restarting the Printer

RESTARTING THE PRINTER AT THE CONTROL PANEL

Using the Software Resets feature to restart the printer is faster and wastes fewer consumables than powering the printer on and off. Restarting the printer can take up to five minutes during which time the Embedded Web Server is not available.

1. Ensure that the printer is in the ready state.
2. Press and release the Power button.
3. Touch **Restart**.
4. On the confirmation screen, touch **Restart**.

Updating the Device Software

When Xerox releases a new version of device software or firmware, you can update your device to incorporate the new fixes and improvements.

Before you begin:

- Determine the current device software version.
- Download the latest software update file for your device model in **.bin** format from the Drivers and Downloads page.

DETERMINING THE CURRENT SOFTWARE VERSION

1. In the Embedded Web Server, click **System > Software Update**.
2. To verify the software version, go to Software Update area.

UPDATING THE SOFTWARE

1. In the Embedded Web Server, click **System > Software**.
2. For Software Update, click **Check Now**.
3. Refresh your browser and navigate to **System > Software**.
4. In the Specify File for Software Update area, click **Browse**. Locate and select the software upgrade file with the **.bin** format.
5. Click **Open**.
6. Click **Start** to Install Software. The file is sent to the device.

   After the software is installed, the device restarts.
7. To verify the updated software version, check the configuration report.

Date and Time Settings

When you set up the printer for the first time, you are asked to set the date and time. To change the date and time after the initial setup, use the control panel to change the settings. You can use the date and time settings to do the following tasks:

- Enable Network Time Protocol (NTP) synchronization
- Set other timing functions for the printer

To change date and time settings:

1. At the control panel, press the **Home** button.
2. Touch **Settings > Device > System Settings > System Clock/Timers**.
3. Select an option, then touch **OK**.
   As needed, use this method to change the following settings:
   - **Date**: Set the date format and date.
   - **Time**: Set the time using a 12-hour or 24-hour format.
   - **NTP Time Synchronization**: If you have a Network Time Protocol (NTP) server, set the clock in the printer to **On** to synchronize with your NTP server.
   - **Time Synchronization Interval**: Specify how often, 1–500 hours, the printer connects to the NTP server.
   - **Time Server Address**: Specify the NTP server address.
   - **Auto Clear**: Specify the amount of inactive time before the control panel resets to the default screen.
   - **Auto Job Release**: Set Auto Job Release to **On**, 1–240 seconds, or **Off**.
   - **Specify Auto Print Time**: Set the time period to start the next print job after you operate the control panel.
   - **Printer Lockout**: To set up printer lockout, use the Embedded Web Server. Refer to Locking the Printer.
   - **Time Zone**: Set the time difference from GMT.
   - **Daylight Savings**: Set the daylight savings time, if necessary. During daylight savings time, the printer increments the clock forward by one hour automatically.
   - **Warmer Mode**: To prevent condensation, touch **On** to enable warmer mode, touch **Auto Start** to operate the warmer mode automatically.
   - **Print on Demand Duration** Set the time from 0–255 minutes.

Fax Speed Dial Setup Settings

To set up and administer the Fax Speed Dial feature:

1. In the Embedded Web Server, login as Administrator.
2. Click **Address Book**.
3. Under All Contacts, select **Fax**.
4. Select **Add New Contact**, enter the required information, then click **Save**.

Watermarks and Annotations

A watermark inhibits the replication of a document by adding text or a background pattern to the printed page. You can configure watermarks to print dates, unique IDs, background patterns, or default text. Additionally, you can set watermarks to print according to the job type.

Annotations are customizable text strings that are printed on the document, similar to watermarks. If you want to create a custom annotation not found in the default selections, you can set a text string and then apply one of the four preset templates to the text string. When annotations are enabled, they print according to the layout template associated with the job type.

CREATING A WATERMARK

To set up the watermark appearance and enable a forced watermark:

1. In the Embedded Web Server, click **System > Security**, then in File Security area, click **Watermark**.
2. In the Watermark area, specify the date format and watermark appearance.
3. In the Force Watermark area, select the jobs that require a watermark on the output, select **On**.
4. Click **Save**.

CREATING A UNIVERSAL UNIQUE ID

To print the Universal Unique ID number in the watermark:

1. In the Embedded Web Server, click **System > Security**, then in the File Security area, touch **Print Universal Unique ID**.
2. For Print Universal Unique ID, select **Enabled**.
3. Use the position adjustments to choose where you want the unique ID to print on the page.
4. Choose the print position for side 2 of the page.
5. Click **Save**.

FORCED ANNOTATIONS

Forced annotations allow you to create text strings for custom watermarks. You can create up to eight strings with a maximum of 64 characters. Once the string is created, you can apply a layout template to the watermark.

Creating Annotation Text Strings

1. In the Embedded Web Server, click **System > Security**, then in the File Security area, click **Edit** under Create Text String.
2. Type up to 8 annotation text strings with a maximum of 64 characters each.
3. Click **Save**.

Applying Layouts to Text Strings

To apply a template to an annotation text string:

1. In the Embedded Web Server, click **System > Security**, then in File Security area, click **Force Annotation**.
2. To apply the template to the annotation text string for one of the available types of jobs, click **Save**.
3. In the Layout Template area, click **Edit** select one of the preset templates.
4. Click **Save**.

Deleting Layout Templates

To delete layout templates:

1. In the Embedded Web Server, click **System > Security**, then in File Security area, click **Force Annotation** then in the Layout Template area, click **Edit > Delete Layout Template**.
2. In the Layout Template List area, select the templates that you want to delete.
3. Click **Delete**.

Memory Settings

To increase performance, you can allocate memory away from unused ports or you can allocate more memory to heavily used ports.

1. In the Embedded Web Server, click **System > Defaults**, then in the Print Settings Area area, click **Allocate Memory**.
2. For IPP, click **No Spooling** or **Spool**.
3. Under Job Ticket Memory, specify the amount of memory.
4. Click **Save**.

Backup and Restore

You can back up your device and, if needed, restore the settings to the device. The backup process creates a file that is stored on the device. Each time you back up the device, the backup file is overwritten. The process backs up the following data:

- Network connectivity and security settings
- Local user accounting settings
- Address book entries
- Information about options installed on the device
- Job flow sheets
- Folders used to store files on the device

Note:

- The backup process backs up the folders, but does not back up files in the folders. To keep the files, before you restore the settings, transfer the files from the device.
- If you create folders after you create a backup, the new folders are deleted from the device during a restore action.
- Backup and restore work on a single device. You cannot use the backup file on one device to transfer settings to another device. To transfer settings to another device, use Cloning. You can save specific settings to a clone file, then transfer the settings to another device in your fleet.

BACKING UP DEVICE SETTINGS

To back up device settings:

1. In the Embedded Web Server, click **Home > Backup and Restore**.
2. For Backup, click **Back Up Now**.

The device creates or overwrites the backup file. The Status area on the Backup and Restore page shows the date and time of the backup.

RESTORING DEVICE SETTINGS

To restore device settings:

1. In the Embedded Web Server, click **Home > Backup and Restore**.
2. For Restore, click **Restore Backup**.
3. If required, to restart the device, follow the onscreen instructions.

The device settings are restored from the backup file.

Printer Management

You can use the printer management functions to do the following tasks:

- Export the job history to a comma-separated value file
- Delete held jobs automatically
- Specify periods when the printer is locked out

EXPORTING JOB HISTORY

To export the job history to a comma-separated values file:

1. In the Embedded Web Server, click **Jobs**, then in the Job Management area, click **Export Job History**.
2. In the Specify Time Period area, specify the time period when you want to export data. For the Start Date & Time and the End Date & Time fields, enter the information.
3. Click **Start**.
4. To save the job history file, follow the onscreen instructions.

AUTOMATICALLY DELETING HELD JOBS

To delete held jobs automatically:

1. In the Embedded Web Server, click **Jobs**, then in Job Management area, click **Job Settings > Auto Job Promotion**, then click **Enable**.
2. For Automatically Delete Held Jobs, select **On**.
3. For Held Job Retention Period, type the days, hours and minutes for the deletion time.
4. Click **Save**.

LOCKING THE PRINTER

To lock the printer and make it unavailable for use:

1. In the Embedded Web Server, click **Jobs**, then in Job Management area, click **Job Settings > Printer Lockout**.
2. For Printer Lockout, select **Edit**, then click **Enable** toggle button.
3. Specify the lockout period:
   - To specify a daily lockout time, for Lockout Duration, select **Enabled**. For the lockout period, type the start and end time.
   - To lock the printer for whole days, for Lockout Day of Week, select **Enabled** and choose the days for the lockout.
   - To specify a lockout period, for Lockout Period, select **Enabled**. For the lockout period, type the year, month, and day for the start and end time.
4. Click **Save**.

Image Quality and Registration

This chapter contains:

Image Quality and Calibration 216
Simple Image Quality Adjustment (SIQA) Tools 221

Image Quality and Calibration

SETTING IMAGE QUALITY FOR THE SCANNER

When copying, you can select the image quality processing method and parameters the scanner will use and apply to the copy job. For example, you can enhance color reproduction when copying photos.

Note: For details on how to associate a media type and weight with a specific image quality setting, refer to Paper Tray Settings.

To set copy image quality:

1. At the device control panel, log in as Administrator, then access the Paper Tray Settings screen. For details, refer to Accessing Paper Tray Settings.
2. Select **Setting > Device > System Settings > Image Quality**.
3. To set image quality for a feature, select a feature:

FEATURE	DEFAULT SETTING
Photo and text Recognition: This feature allows you to change the sensitivity level with which the device determines a document as text or photos. This setting is used when you select **Photo and Text for Original Type** on the Image Quality screen. Select a sensitivity option: • **More Text**: This option allows the device to recognize very fine print as text. • **Text**: This option allows the device to bias the scanning towards text reproduction. • **Normal**: This option allows the device to balance the text and photo recognition. • **Photo**: This option allows the device to bias the scanning towards photo recognition and reproduction. • **More Photo**: This option allows the device to recognize halftone images from newspapers and advertisements as photos.	Normal
Output Color Recognition: This feature allows you to change a sensitivity level from the five levels with which the device determines a document as monochrome or color. This setting is used when you select **Auto Detect** for Output Color on the Copy screen. • **More Black and White**: This option is the most sensitive to black and white documents. • **Black and White**: This option allows the device to recognize monochrome documents easily. • **Normal**: This option allows the device to balance the color of the documents. • **Color**: This option allows the device to recognize color documents easily • **More Color**: This option is the most sensitive to color documents.	Normal
Photo Reproduction Level: On the Image Quality screen, when copying with Original Type set to Photo and Text, this feature allows you to adjust the color reproduction level in the areas determined by the device as photos. • **More Text**: This option yields a bold copy effect, which emphasizes the dense parts of an image.	Normal

FEATURE	DEFAULT SETTING
• **Normal**: This option allows the device to balance between text recognition and reproduction. • **More Photo**: This option softens the image gradation of an image, which enhances the reproducibility of subtle colors.	
Background Suppression (color copy): This feature allows you to set the method of background suppression used for color copies. Background suppression is the function that detects the color density for documents with background colors on colored paper. It also suppresses the scan of background colors for those documents. • **High Quality**: This option allows the device to detect the background color on a pre-scanned image of the entire document. • **High Speed**: This option allows the device to detect the background color on a pre-scanned sample section of the document.	High Quality
Background Suppression (B&W Copy): This feature detects the color density for documents with background colors on colored paper. It also suppresses the scan of background colors for those documents. • **High Quality**: This option allows the device to detect the background color on a pre-scanned image of the entire document. Important: For Image Shift, when you select High Quality and Corner Shift with a Reduce/Enlarge ratio of 60 or less, it is possible that a part of the image does not print or that the output paper is blank. • **High Speed**: This option allows the device to detect the background color on a pre-scanned sample section of the document.	High Quality
Background Suppression (scan jobs): This feature sets the method of background High Quality suppression for scan operations. Select an option for density detection and background color deletion.	High Quality
Image Enhancement: When enabled, this feature gives the printed image a smoother appearance.	On
Auto Start Image Quality Setup: When enabled, the image quality setup is periodically performed, time until the start of printing can be reduced.	Off

CALIBRATING IMAGE COLOR

Note: Performing this calibration process affects only jobs that are printed at the internal controller. It does not apply to jobs coming from the DFEs.

If color gradation of a printed image shifts, use the calibration feature at the control panel. Calibration feature calibrates the color of the image and maintains the quality of the output at a certain level.

To calibrate image color:

1. At the device control panel, log in as Administrator, press the **Home** button. For details, refer to Administrator Access at the Control Panel.

2. Select **Settings > Device > Maintenance > Image Quality > Calibration**. Read the directions on the control panel and follow the steps.
3. From the Calibration screen, select the Screen Type to be calibrated.

Note: For optimal color, calibrate all four screen types.

4. Select **Target**, then select a job type to be impacted by the calibration such as **Copy and Print Jobs**, **Copy Jobs Only**, **Print Jobs Only**, or **None**.

Note: Reset the copy feature list before performing calibration:

- **Copy Job 1**: Calibrates screen gradations used for **Text** or **Map** for Original Type.
- **Copy Job 1**: Calibrates screen gradations used for **Photo & Text** or **Photo** for Original Type.
- **Print Job 1**:
  - For PCL Printer Driver:

    Calibrates screen gradations used for all features set with the **Color Options** such as Image Quality, Image Adjustment Mode, Image Types.

    Calibrates screen gradations used when **Image Options > Screen** tab is set to Auto, Fineness, or Standard.
  - For PostScript Printer Driver:

    Calibrates screen gradations used when **Image Options > Screen** tab is set to Fineness or Standard.

    Calibrates screen gradations used when **Image Options > Image Quality** tab is set to High Quality or High Resolution and when **Auto** is selected at screen.
- **Print Job 2**:
  - For PCL Printer Driver:

    Calibrates screen gradations used when **Image Options > Screen** tab is set to Graduation. The case when **High Resolution** is selected for Image Quality is an exception.

    Calibrates screen gradations used when **Advance > Print Page** tab is set to On.
  - For PostScript Printer Driver:

    Calibrates screen gradations used when **Image Options > Screen** tab is set to Graduation.

    Calibrates screen gradations used when **Image Options > Image Quality** tab is set to High Speed and when **Auto** is selected at screen.

5. Load A3, A4, 11 x 17 in. or 8.5 x 11 in. paper, then for Paper Supply, select an option.
6. To print the calibration chart for the color correction, on the screen, select **Start**.
7. Continue following the steps on the control panel.
8. To perform calibration, place the calibration chart face down with both magenta patches against the left edge of the document glass.
9. To prevent light from bleeding through the sheet, place 5 or more sheets of blank white paper over the chart.
10. Lower the document glass, then on the screen, select **Start**.

11. Select **Confirm**.

COMBINED CALIBRATION

Combined Calibration feature adjusts the image quality automatically when the image quality of copy or print becomes poor.

1. At the device control panel, log in as Administrator, press the **Home** button. For details, refer to Administrator Access at the Control Panel.
2. Select **Settings > Device > Maintenance > Image Quality > Combined Calibration**.
3. Enable **Print Calibration Charts** toggle button.
4. Select **Paper Supply**, then touch **Ok**.
5. Touch **Start**.

   The Calibration Chart prints.
6. Follow the on-screen directions.

TWO-SIDED COLOR SCANNING CALIBRATION

Calibrating Two-Sided Color Scanning

Calibrating Two-Sided Color Scanning feature adjusts the difference of the color between the both side of paper when you load the document with the auto two-sided document feeder.

1. At the device control panel, log in as Administrator, press the **Home** button. For details, refer to Administrator Access at the Control Panel.
2. Select **Settings > Device > Maintenance > Image Quality > 2 Sided Color Scanning Calibration**.
3. In Calibration Type, select **Print Chart**.
4. Select **Paper Supply**, then touch **Ok**.
5. Touch **Start**.

   The Calibration Chart prints.
6. Follow the on-screen directions.

Restoring Previous Color Values for the Duplex Automatic Document Feeder (DADF)

1. At the device control panel, log in as Administrator, press the **Home** button. For details, refer to Administrator Access at the Control Panel.
2. Select **Settings > Device > Maintenance > Image Quality > 2 Sided Color Scanning Calibration**.
3. In Calibration Type, select **Restore Factory Default Values**, then touch **Start**.

Restoring Factory Default Color Values for the Duplex Automatic Document Feeder (DADF)

1. At the device control panel, log in as Administrator, press the **Machine Status** button, then touch the **Tools** tab. For details, refer to Administrator Access at the Control Panel.
2. Touch **Common Service Settings > Image Quality Adjustment > 2 Sided Color Scanning Calibration**.
3. Touch **Restore Factory Default Values**, then touch **Start**.
4. Touch **Close**.

SPOTS/STREAKS DIAGNOSTICS

Spots/Streaks Diagnostics feature diagnoses the cause when problems such as spots or streaks appears in the output.

1. At the device control panel, log in as Administrator, press the **Home** button. For details, refer to Administrator Access at the Control Panel.
2. Select **Settings > Device > Maintenance > Image Quality > Spots/Streaks Diagnostics**.
3. Enable **Print Diagnostic Charts** toggle button.
4. Select **Paper Supply**, then touch **Ok**.
5. Touch **Start**.

   The Chart prints.
6. Follow the on-screen directions.

Simple Image Quality Adjustment (SIQA) Tools

SIMPLE IMAGE QUALITY ADJUSTMENT (SIQA) TOOLS OVERVIEW

Simple Image Quality Adjustment, or SIQA, is a set of maintenance tools that adjust the quality of the printed images generated by the device. SIQA performs three types of adjustments, which must be performed in the following order:

- **Adjust Image Transfer**: This tool corrects for uneven toner and color shift by creating an Image Transfer Adjustment to the Bias Transfer Roll in the device. The adjustment is created and saved for specific stocks and can be selected for any tray when printing on those stocks. Perform the Image Transfer Adjustment before performing any other image adjustment. The Adjust Image Transfer feature can be accessed by creating the custom paper type. To create custom paper type, refer to Custom Paper Settings.
- **Adjust Alignment**: This procedure generates an individual alignment profile for each stock and tray combination you select when performing the procedure. These profiles ensure correct placement of images on the media. You can create a maximum of 50 profiles. Each created profile is then used automatically each time the associated stock is used, ensuring optimal print quality. Perform Alignment Adjustment after you have completed the Image Transfer Adjustment. To perform Alignment Adjustment, refer to Image Registration Adjustments.
- **Density Uniformity**: This procedure adjusts print engine tables, which ensures that ink is deposited uniformly and consistently across the entire surface of a page for each print. Perform the Density Uniformity Adjustment after you have completed the Image Transfer and Alignment Adjustments. To perform Density Uniformity, refer to Density Uniformity Adjustment.

IMAGE REGISTRATION ADJUSTMENTS

Adjusting Image Alignment

Adjustments can be made to the image based on the alignment output of a document. Various adjustments can be modified such as magnification and skew. This can be achieved through the use of the twenty default adjustment types. In addition, a specific paper tray can be assigned to a specific adjustment type.

Adjustments can be made when the position of the output image is misaligned or skewed. This may be a result of paper expansion or contraction, cutting inaccuracy, or paper storage conditions. Use Alignment Adjustment Setting features to compensate for misalignment and skew.

The following alignment adjustments can be made to the position of the output image. These are described in more detail in the following pages.

- **Perpendicularity Adjustment**: Adjust an image to be straight up or down.
- **Skew Adjustment**: Adjust a skewed image.
- **Magnification Adjustment**: Adjust this when the size (scale) of the printed image is offset.
- **Print Position Adjustment**: Use this option when making adjustments to the lead edge of the image (X direction) and side edge of the image (Y direction). For example, use this when the images on sides 1 and 2 are misaligned.

Note: When making adjustments to multiple items, adjust the image in the following order: Perpendicular, Skew, Magnification, Print Position Adjustment.

Alignment Adjustment Procedure

Note: Adjust Side 1 first, then match Side 2 to Side 1. When accounting for paper size tolerances, the most accurate image alignment results are from folding the sheets in half instead of using the 10 mm from edge.

1. At the device control panel, log in as Administrator, press the **Home** button. For details, refer to Administrator Access at the Control Panel.
2. Touch **Settings > Device > Maintenance > Image Quality**.
3. To scroll down and select **Adjust Alignment**.
4. Select **Auto Alignment** or **Manual Alignment**.

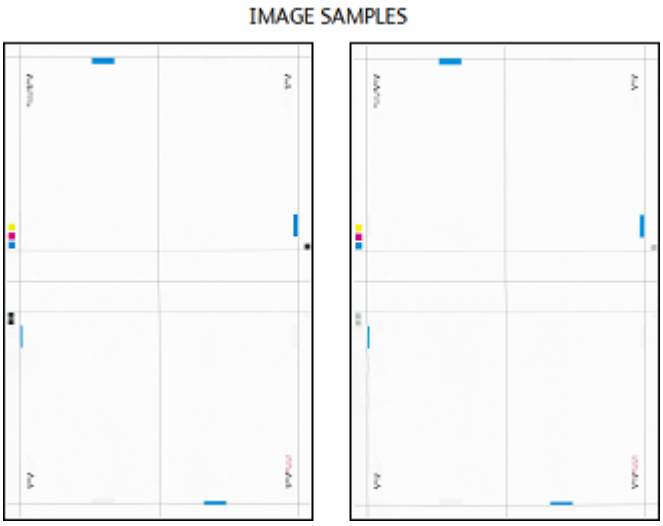
Auto Alignment Adjustment

To perform Auto Alignment Adjustment:

1. Print a duplex copy of the Black Paper PDF file that corresponds to the paper size used in your region. The PDF files are located on www.xerox.com/office/PLC92XXdocs in the documentation for the Xerox® PrimeLink® C9265/C9275/C9281 Series Multifunction Printers.
   - 11 x 17 in.: SIQA Black Paper for Adjustment-Tabloid.pdf
   - A3: SIQA Black Paper for Adjustment-A3.pdf
2. Touch **Alignment Adjustment**.
3. Touch **Auto Alignment**.
4. Select a paper tray with 11 x 17 in. or A3 size paper.
5. Touch **OK**.
6. For Coverage 1 and Coverage 2, select a coverage value. Use the table below as a guide.

COVERAGE VALUE	AREA COVERAGE
1–3	Low area coverage - text only
4–8	Medium area coverage - equal mixture of text and graphic images
9–10	High area coverage - primarily graphic images

7. To print the calibration chart, touch **Start**.



8. Touch **Document Feeder Scan Precision Adjustment**.
9. To complete the scan using the Document Feeder and Document Glass, follow the instructions on the control panel touch screen.
   a. Load the chart into the DADF and touch **Scan**.
   b. Place the chart on the Document Glass as shown in the diagram with the black paper over it. The side with the white squares and arrows must be facing up. Align the squares on the chart with the white square on the Black Paper.
   c. Reposition the Calibration Chart as indicated on the control panel touch screen and on the Black Paper, then for each scan, touch **Scan**.
   d. After you have completed all scans, **Start Adjustment**.

Manual Alignment Adjustment

To perform Manual Alignment Adjustment:

1. Select **Manual Alignment**.
2. Touch **Type Setup**, then select **Type**.
3. Touch **Sample Printout**.
4. Select the paper tray from which you are printing, then select 1-Sided. Using the Number of Sheets option, run at least 3 sheets.
5. Press the **Start** button.

   Note: If the position of the sample output is correct, a line prints at a position 10 mm from the edge of the paper. If the position of the line on the sample output is misaligned, make adjustments accordingly. To indicate the paper feed direction, two lines print on the image of side 1 and one line prints on the image of side 2 of the sample.

   The current sample output prints.
6. Make adjustments to the image in the following order: Perpendicular, Skew, Magnification, Print Position.
7. Select **OK**.

Adjusting Fold Position

This section describes the procedure for adjusting the fold position. You can adjust the fold position for various paper types, as well as set adjustment values to any of 10 default types. You can assign a set type to each tray.

Fold Position Adjustment

To adjust fold position:

1. Load the paper tray.
2. At the device control panel, log in as Administrator. For details, refer to Administrator Access at the Control Panel.
3. Touch **Settings > Device > Maintenance**.
4. Touch **Adjust Finisher**.
5. For Fold Position Adjustment, do the followings:.
   a. Touch **Fold Position Type Setup**.
   b. Select the paper fold position type you want to set or adjust.
   c. Touch **Name**.
   d. Type a type name, then touch **OK**.

Note: Use a name that identifies the fold type, such as Single Fold Plain.

   e. Select the desired settings, then touch **OK**.
   f. Select the tray, then press the **Start** button.
   g. Measure the fold position via the output sample and adjust the fold position accordingly.
   h. Make adjustments to the items as needed.
   i. After you finish making adjustments, print another output sample with **Sample Printout** and check the adjustment results.
6. For Punch Unit Type, select the punch unit from the list, then touch **OK**.
7. For Fold Assist Crease, select the number of crease from the list, the touch **OK**.

Single Fold Position Adjustment

To adjust single fold settings:

1. Select **Single Fold**.
2. Touch **Paper Supply**, then select the tray.
3. Specify **Sheets per Booklet** and touch **Next**.
4. Touch **Sample Printout**, then click **Print** and check the output sample printout and measure the offset amount.
5. Select **Long at Left** or **Long at Right**.
6. In the Values A Before Adjustment field, using the Up and Down arrow buttons, enter the measurement offset value that you obtained from the sample printout.

7. Touch **OK**, then touch **Sample Printout**.
8. Check the output sample printout and measure the offset amount.
9. Make adjustments again, as needed.
10. Touch **OK**.

Booklet Position Adjustment

To adjust booklet fold positioning:

1. Select **Booklet Creation**.
2. Touch **Paper Supply**, then select the tray.
3. Touch **Adjustment Method**.
4. Select **Standard** or **Variable**.

   Note: If you choose **Standard**, it enables you to enter the adjustment values for 2-sheet booklets and 16-sheet booklets each so that you can specify the optimal adjustment values for booklets consisting of any number of sheets.
5. Select **Variable** and set the value for Sheet per Booklet, then touch **Next**.
6. Touch **Sample Printout**, then click **Print** and check the output sample printout and measure the offset amount.
7. On the **Booklet Fold State** pop-up, select the fold setting for booklet and enter the measured values of the printed samples.
8. Click **OK**.
9. To print an output sample and check the adjustment results, touch **Sample Printout**.
10. Make adjustments again, as needed.
11. Touch **OK**.

C Fold Position Adjustment

To adjust the C fold position:

1. Select **C Fold-A4** or **C Fold-8.5x11**.
2. Touch **Sample Printout**.
3. Touch **Paper Supply**, select the tray, then touch **Print**.
4. Check the output sample, then measure the A and B fold position movement amounts.
5. For Values A, type the measurement value you obtained in the previous step.

   Note: Set value A and value B so that an edge of the paper does not extend past a fold position of the paper. An edge of paper extending past a fold position of the paper can cause a paper jam.
6. To print an output sample and check the adjustment results, touch **Sample Printout**.
7. Make adjustments again, as needed.
8. Touch **OK**.

Z Fold Position Adjustment

To adjust the Z fold position:

1. Select **Z Fold-A4** or **Z Fold-8.5x11**.
2. Press **Sample Printout**.
3. Touch **Paper Supply**, select the tray, then touch **Print**.
4. Check the output sample, and measure the A and B fold position movement amounts.
5. For Values A, type the measurement value you obtained in the previous step.

Note: Set value A and value B so that an edge of the paper does not extend past a fold position of the paper. An edge of paper extending past a fold position of the paper can cause a paper jam.

6. To print an output sample and check the adjustment results, touch **Sample Printout**.
7. Make adjustments again, as needed.
8. Touch **OK**.

Z Fold Half Sheet Position Adjustment

To adjust the Z fold position:

1. Select **Z Fold Half Sheet-A3**, **Z Fold Half Sheet-B4**, **Z Fold-11x17**, or **Z Fold-8K**.
2. Press **Sample Printout**.
3. Touch **Paper Supply**, select the tray, then touch **Print**.
4. Check the output sample, and measure the A and B fold position movement amounts.
5. For Values A, type the measurement value you obtained in the previous step.

Note: Set value A and value B so that an edge of the paper does not extend past a fold position of the paper. An edge of paper extending past a fold position of the paper can cause a paper jam.

6. To print an output sample and check the adjustment results, touch **Sample Printout**.
7. Make adjustments again, as needed.
8. Touch **OK**.

DENSITY UNIFORMITY ADJUSTMENT

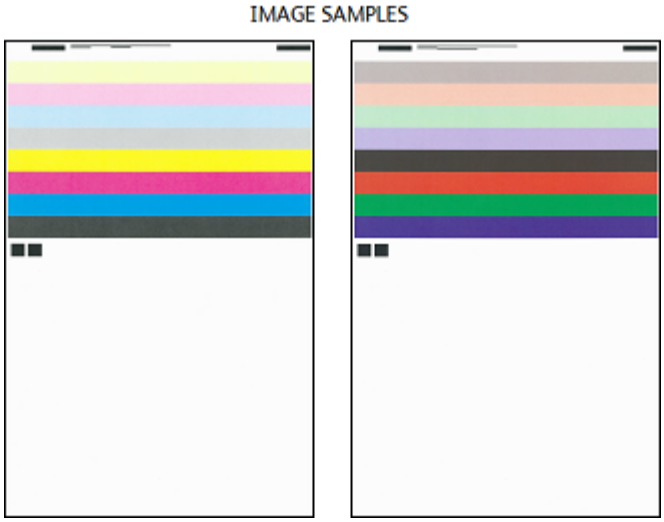
Density Uniformity Adjustments ensure uniform toner coverage across the page. These routines involve both perpendicular and paper feed direction. Both of these routines adjust the imaging system of the printer, regardless of paper type.

Note: Xerox recommends using a good quality and centerline paper type, such as 304.8 mm (12 in.) or SRA3 (320 x 450 mm) (12.6 x 17.7 in.), 90 g/m^2 Uncoated for Density Uniformity Adjustment routines. Do not use heavyweight or lightweight papers.

Density Uniformity Adjustment (Perpendicular)

To perform the Density Uniformity Adjustment (Perpendicular):

1. At the device control panel, log in as Administrator, press the **Home** button. For details, refer to Administrator Access at the Control Panel.
2. Touch **Settings > Device > Maintenance > Image Quality**.
3. Touch **Density Uniformity Adjustment (Perpendicular)**.
4. Touch **Manual Process** or **Semi Auto Process Using Scanner**.
5. To perform Manual Process, do the followings:
   a. Touch **Output Color** and select any color from the list.
   b. Touch **Level** and set the value from 1 to 6.
   c. Touch **Inboard/Outboard** and set the value.
   d. Click **OK**.
   e. After adjustments, touch **Print Sample**.
6. To perform Semi Auto Process using Scanner, do the followings:
   a. Touch **Paper Supply** and select the tray.
   b. Enable **Print Calibration Chart** toggle button.
   c. Touch **Start** and follow the instructions on the control panel touch screen to print the two charts.



7. Touch **Scan**.
8. Using the instructions on the control panel touch screen, scan the two calibration charts.
9. To begin the density uniformity adjustment, touch **Start**.
10. When the adjustment completes, touch **OK**.

Density Uniformity Adjustment (Paper Feed Direction)

To perform the Density Uniformity Adjustment (Paper Feed Direction):

1. Touch **Paper Supply** and select the paper.
2. Touch **Start**.

3. To print the samples, touch **Sample Printout**.

CREATING A CUSTOM CURL PROFILE AS ADMINISTRATOR

To create a Custom Curl Profile as administrator, follow the below steps:

1. At the device control panel, log in as Administrator, then press the Home button. For details, refer to Administrator Access at the Control Panel.
2. Select **Device > Maintenance > Image Quality > Adjust paper curl**.
3. Select an existing or empty Custom Type entry from the list.
4. Enter a name for the type setting as desired.
5. Set the appropriate paper type.
6. Select **Adjust Paper Curl**.
7. Select one of the listed Type number.
8. Select **Type Setup**.
9. Enter a name for the Type number.
10. Adjust curl levels as necessary following the below steps.
11. Each Type number has three print modes and each can be set to Auto or fixed curl adjustment level (0–5).
    - 1 Sided – Face Up
    - 1 Sided – Face Down
    - 2 Sided
12. Adjust curl setting value (0–5) for one or more of the print modes as necessary.
    - 0 provides the best performance to minimize up curl exiting the fuser.
    - 5 provides the best performance to minimize down curl exiting the fuser.

    Note: 0 setting is new and can help with excessive up curl and is only available on January 2026 release software or later versions.
13. You can print samples after adjusting the values and evaluate curl performance.
14. Save the type setting and exit.
15. Select the type setting and apply it to the custom paper setting for the media being run.

Customization and Expansion

This chapter contains:

Xerox Extensible Interface Platform® 230
Customizing Apps on the Printer 232
Pins (Formally Known as Stored Programming) 233
Plug-ins and Kits 234
Setting Up the Inserter Module 236

Xerox Extensible Interface Platform®

Xerox Extensible Interface Platform® allows independent software vendors and partners to develop personalized and customized document management solutions. These solutions can be integrated and accessed directly from the control panel of the printer. These solutions can use existing printer infrastructure and databases. Examples of applications include the following:

- ScanFlow Store®
- Xerox® Scan to PC Desktop®
- Equitrac Office®

For more information on Xerox Extensible Interface Platform® applications for your printer, contact your Xerox Service Representative or see www.office.xerox.com/eip/enus.html on the Xerox website.

ENABLING EXTENSIBLE SERVICES

Before you begin:

- Ensure that a digital certificate is installed on the printer. For information, refer to Digital Certificates.
- Enable HTTP (SSL). For information, refer to Secure HTTP and SSL/TLS.

ENABLING EXTENSIBLE SERVICE REGISTRATION

To enable the extensible service registration:

1. In the Embedded Web Server, click **Apps > EIP Settings**.
2. Select the remote system management, apps, hardware, authentication and accounting, and security that you want to enable. Click **Save**.
3. In the EIP Settings area, click **General Settings** select the services that you want to enable.
   To allow users to use Xerox® ConnectKey® Apps on the printer, enable **Allow ConnectKey App Install**. To allow the installation of unencrypted apps, enable **Allow Unencrypted ConnectKey App Install**.
4. If necessary, in the Browser Settings area, select **General**.
5. If necessary, select **Verify server certificates**.
6. To configure proxy settings, in the Proxy Server area, select **Proxy Server**, then click **Enable** toggle button.
   a. In Embedded Web Server select **Apps > EIP Settings > General Settings > Proxy Server Settings** in the Proxy Server area, select an option:
      - **Automatically Detect Settings**: Select this option to detect settings automatically.
      - **Same Proxy for All Protocols**: Select this option to use the same settings for the HTTP and HTTPS server. In the HTTP Server area, type the server name, port number and, if needed, the authentication information.
      - **Different Proxy for Each Protocol**: Select this option to enter separate server addresses for HTTP and HTTPS. In the HTTP Server area, type the server name, port number and, if needed, the authentication information for HTTP. In the HTTPS Server area, type the information for the HTTPS server.
      - For **Addresses to Bypass Proxy Server**, type any Web addresses or domains that you want to bypass the proxy server.

- **Use Automatic Proxy Configuration Script**: Select this option to use a proxy configuration script. In the Automatic Proxy Configuration Script area, type the URL for the script.

b. Click **Save**.

7. For Cross-Origin Resource Sharing (CORS), go to **Cross-Origin Resource Sharing (CORS)** select an option:
   - **Allow Any Domain**: To allow any domain, select this option.
   - **Allow Only Trusted Domains**: To specify trusted domains, select this option. For Trusted Domains. To specify the trusted domains, use a comma-separated list. Click **Save**.
8. Click **Save**.

SETTING UP A FILE REPOSITORY

A template contains scan settings and at least one destination for the scanned image files. You can associate a scan template with your service or use the default template.

To configure File Repositories:

1. In the Embedded Web Server, log in as administrator, then click **Apps**.
2. Click **EIP Settings**.
3. In the Scan Template Settings area, click **File Repositories**.
4. In the File Repository area, click an item in the list.

If there are no repositories in the list:

1. Click the **Plus** icon (**+**), then select a protocol.
2. Enter the configuration information.
3. Click **Save**.

CONFIGURING TEMPLATE POOL REPOSITORY SETTINGS

If you use a scanning management application, such as SMARTsend or ScanFlowStore, provide information about the server that hosts the templates on this page.

1. In the Embedded Web Server, click **Apps**.
2. Click **EIP Settings**.
3. In the Scan Template Settings area, click **Template Pool > Edit**.
4. Click **Server Type**, then select the protocol for the server where the Template Pool is located.
5. Enter the configuration information, then click **Save**.

Customizing Apps on the Printer

The apps on the printer control panel allow users to perform operations, for example, to send email or to use network scanning. Standard apps are preinstalled on the printer. To provide more functions, you can install Xerox® ConnectKey® Apps from the Xerox App Gallery. You manage the Standard Apps and Xerox® ConnectKey® Apps that are available on the printer.

XEROX APP GALLERY

Xerox® ConnectKey® Apps are small programs that add functionality to Xerox printers. The Xerox App Gallery Web Portal allows you to install, purchase, and manage Xerox® ConnectKey® Apps.

You can use your Xerox App Gallery account to find apps that provide new features or new capabilities for your printer. For example, select apps to increase productivity, or improve workflows. The Gallery offers Xerox® Apps that Xerox® and Xerox® third-party partners design. Use your Xerox App Gallery account to do the following tasks:

- View and acquire apps
- Install apps onto your printer
- Manage your apps

The Xerox App Gallery App is pre-installed on the printer. The App Gallery App allows you to access your account from the control panel to manage your apps.

You can access your account through the Xerox App Gallery home page at www.xerox.com/AppGalleryHome. When you set up your account, associate the printers that you administer with your account. Install apps onto the selected printers. For documentation and support, refer to www.support.xerox.com/support/xerox-app-gallery/support/enus.html.

Before you install Xerox® ConnectKey® Apps from the Xerox App Gallery, ensure that you have enabled the Xerox® Extensible Interface Platform®.

CUSTOMIZING APPS AVAILABLE AT THE CONTROL PANEL

You can control the apps that are available on the control panel for your users. Show, hide, and delete apps as needed.

1. In the Embedded Web Server, click **Apps**, then click **Edit Apps Screen of Device**.
2. To show or hide an app on the control panel:
   a. Click **+** to show apps.
   b. Click **Save**

   Repeat this procedure for each app that you want to show or hide.
3. To delete an app:
   a. For the app that you want to delete, click **Close** icon.
   b. Click **Save**.

   You cannot delete standard apps. You can delete apps that you have installed on the printer.

Pins (Formally Known as Stored Programming)

The Xerox® PrimeLink® C9200 series printers support a job memory feature called Pins. The Pins feature allows users to store the settings of a commonly used jobs and is available to be selected on the main screen of the control panel. For example, a calendar has specific settings for paper, folding, and binding. A user can save the calendar production settings and reuse the settings to produce other calendars.

ENABLING PINS FOR COPY APP

To add a job to Pins on the home screen of the control panel:

1. Touch **Copy**.
2. Program the settings for the job you want to save as a pin.
3. Scroll to the bottom of the menu, select **Save Settings as Pin**.
4. Edit the name.

   Note: Use a name that identifies the settings of Job you are trying to save.
5. Touch **OK**.

   The saved pin will be available in the pins icon on the home screen of the control panel.

SELECTING A JOB FROM PINS

1. On the main screen of the control panel, touch **Pins**.
2. Select the name of the job you created in Pins.

   The selected job screen opens with the settings you saved for the job.
3. To print a job, touch **Start**.

Note: Jobs in Pins created as administrator is only available in the administrator mode.

EDITING PINS

At the Control Panel, the job history of Copy, Scan, and Fax are saved in Pins. The job history also save email jobs in the control panel. The saved jobs can be viewed in the Embedded Web Server. Click on **Select Action** (vertical ellipse icon) to perform the actions for the saved jobs are as follows:

1. Click **Create Pin** and enter the name in the Edit Name window, then click **Save**.
2. To view the job details, click **Details**.
3. To delete the saved job, click **Delete**.

Plug-ins and Kits

You can expand the capabilities of your printer using plug-ins and kits, for example card readers, and coin-operated accessories. You can order kits from Xerox that contain hardware and installation instructions. Follow the instructions to install, set up, and configure the kit. If the kit requires a Xerox plug-in, download the plug-in file from www.xerox.com, then store the file on your computer.

ENABLING PLUG-INS

To enable plug-ins:

1. In the Embedded Web Server, click **System > Plug-in Settings > Embedded Plug-ins**.
2. For Embedded Plug-ins, select **Enabled**.
3. Click **Close**.

MANAGING PLUG-INS

Your expansion kit contains full instructions for installing and managing your plug-ins. If your kit requires a Xerox plug-in, download it from www.support.xerox.com, then save the file to your computer. You can install updates from the Xerox website.

To manage plug-ins:

1. In the Embedded Web Server, click **System > Plug-in Settings > List of Embedded Plug-ins**.
2. Select an option to manage your plug-ins:
   - **Add**: Select this option to install a plug-in. Click **Browse**, locate the plug-in installation file, then click **Open**. Click **Upload**, and if prompted, restart the printer.
   - **Details**: To view information, select a plug-in.
   - **Stop**: To deactivate a plug-in, select a plug-in, in the action area, click the three dots for option, then click **Deactivate**. If prompted, restart the printer.
   - **Start**: To start a deactivated plug-in, select a plug-in, in the action area, click the three dots for option, then click **Activate**. If prompted, restart the printer.
   - **Update**: Select this option to install a plug-in update. Before you install the update, deactivate the plug-in. Select a plug-in, then click **Update**. Click **Browse**, locate the plug-in update file, then click **Open**. Click **Update**, and if prompted, restart the printer.
   - **Delete**: Select this option to delete a plug-in. Before you delete the plug-in, deactivate it. Select a plug-in, then click **Delete**.

ENABLING DIGITAL SIGNATURE VERIFICATION FOR SECURE PLUG-INS

To enable the verification of digital signatures for secure plug-ins:

1. In the Embedded Web Server, click **System > Plug-in Settings > Signature Verification**.
2. For Signature Verification when Adding / Updating, select **Enabled**.
3. Click **Close**.

AUXILIARY INTERFACE KIT

An Auxiliary Interface Kit, or a Foreign Device Interface kit, is a third-party access and accounting device such as a coin-operated printer accessory or a card reader that can be attached to the printer. Installation instructions are included with the Foreign Device Interface Kit. After the kit is installed, you must enable and configure the device at the Control Panel.

Setting Up the Inserter Module

The Inserter Module inserts cover sheets or separator sheets, such as blank or pre-printed sheets, into print jobs. The paper fed from the Inserter Module is not printed on, but the paper is placed into the printed output at selected locations. The Inserter Module detects the size of the loaded paper automatically, based on values specified in the non-volatile memory.

To set up the Inserter Module to detect the fed paper size:

1. At the control panel, log in as administrator, press the **Home** button, then touch the **Settings** icon.
2. Touch **Device > Maintenance > NVM Read/Write**.
3. To enter the NVM code 769–503, for Chain-Link, in the first box, type `769`. In the second box, type `503`. Touch **Change**.
   The current NVM value appears.
4. For the paper that you are feeding into the Inserter Module, for New Value, type 0–4 as appropriate.
   The values for the fed paper sizes are listed:
   - `0`: Legal, 215.9 x 355.6 mm (8.5 x 14 in.)
   - `1`: A4, 210 x 297 mm (8.27 x 11.69 in.)
   - `2`: 215 x 315 mm (8.47 x 12.4 in.)
   - `3`: Letter, 215.9 x 279.4 mm (8.5 x 11 in.)
   - `4`: 215.9 x 330.2 mm (8.5 x 13 in.)
5. To confirm the new setting, touch **Change**.
6. Log out as administrator. To restart the printer, follow the onscreen prompts.