

VERSION 2.1  
FEBRUARY 2023  
702P08986

# Xerox® PrimeLink™ C9065/C9070 Printer

System Administrator Guide

©2023 Xerox Corporation. All rights reserved. Xerox® and PrimeLink™ are trademarks of Xerox Corporation in the United States and/or other countries.

MeterAssistant®, SuppliesAssistant®, Scan to PC Desktop®, and Xerox Extensible Interface Platform®, are trademarks of Xerox Corporation in the United States and/or other countries. Product status, build status, and/or specifications are subject to change without notice.

Microsoft®, Windows®, Windows XP®, Windows Vista®, and Word are registered trademarks of Microsoft Corporation in the United States and/or other countries.

Apple®, Macintosh®, and Mac OS® are trademarks or registered trademarks of Apple Computer, Inc., registered in the U.S. and other countries. Elements of Apple's Technical User Documentation used by permission from Apple Computer, Inc.

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.

Linux® is a registered trademark of Linus Torvalds.

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

TWAIN is a trademark of TWAIN Working Group.

Universal Serial Bus is a trademark of USB Implementors Forum, Inc. (USB-IF)

UNIX® is a registered trademark of the Open Group.

Oracle® Solaris is a registered trademark of Oracle and/or its affiliates in the United States and other countries.

# Contents

Introduction.....	15
Configuration Steps .....	16
More Information.....	17
Initial Setup .....	19
Physical Connection.....	20
Initial Setup at the Control Panel.....	21
The Installation Wizard.....	21
Configuration Report.....	21
Printing the Configuration Report .....	21
Administrator Access at the Control Panel.....	22
Locking or Unlocking the Device .....	22
Manually Setting the Ethernet Interface Speed.....	23
Assigning a Network Address .....	23
Viewing Services and Options .....	24
Embedded Web Server .....	25
Accessing the Embedded Web Server .....	25
Enabling Services and Options .....	26
Enabling Services and Options at the Control Panel.....	26
Enabling Features in the Embedded Web Server .....	26
Enabling Features at the Control Panel .....	26
Changing the System Administrator Password .....	27
Using the Configuration Overview Page.....	28
Assigning a Name and Location to the Device .....	28
Network Connectivity.....	29
TCP/IP.....	30
Enabling TCP/IP .....	30
Configuring TCP/IP Settings at the Control Panel.....	30
Configuring TCP/IP Settings in the Embedded Web Server .....	32
SNMP.....	36
Enabling SNMP .....	36
Configuring SNMP .....	36
LPD.....	39
Enabling LPD .....	39
Configuring LPD .....	39
Raw TCP/IP Printing.....	40
Enabling Port 9100 .....	40
Configuring Port 9100 .....	40
SMTP .....	41
Configuring SMTP Server Settings .....	41
Configuring Optional SMTP Settings.....	41

Performing an SMTP Server Connection Test .....	42
LDAP .....	43
Configuring LDAP Server Settings .....	43
Defining User Mappings .....	43
Configuring LDAP Custom Filters .....	44
Performing an LDAP Connection Test .....	44
POP3 .....	45
HTTP .....	46
Enabling HTTP .....	46
Configuring HTTP Settings .....	46
Proxy Server .....	47
Microsoft Networking .....	48
Configuring WINS .....	48
IPP .....	49
Enabling IPP .....	49
Configuring IPP .....	49
Universal Plug and Play Discovery .....	50
Enabling UPnP .....	50
Configuring UPnP .....	50
SSDP .....	51
WebDAV .....	52
Enabling WebDAV .....	52
Configuring WebDAV .....	52
WSD .....	53
Enabling WSD .....	53
Configuring WSD .....	53
FTP .....	54
Enabling FTP .....	54
Setting Up the FTP Transfer Mode .....	54
Enabling and Disabling a Secure FTP in the Embedded Web Server .....	54
Google Cloud Print .....	55
Enabling Google Cloud Print .....	55
Registering the Device with the Google Cloud Print Service .....	55
Bonjour Multicast DNS .....	56
Enabling Bonjour .....	56
Configuring Bonjour .....	56
AirPrint .....	57
Configuring AirPrint .....	57
Mopria .....	59
Configuring Mopria .....	59
SOAP .....	60
Security .....	61
Setting Up Access Rights .....	62
Overview .....	62

Authentication .....	62
Authorization .....	62
Personalization .....	62
Local Authentication .....	63
Setting Up Local Authentication .....	63
Defining User Information .....	63
Editing the User Information Database .....	63
Specifying Login Requirements.....	64
Network Authentication.....	65
Setting up Network Authentication .....	65
Configuring Authentication Server Settings for Kerberos.....	65
Configuring Authentication Server Settings for SMB .....	66
Configuring Authentication Server Settings for LDAP .....	66
Authentication Using a Card Reader System .....	67
Setting Up Authentication for Xerox® Secure Access.....	67
Configuring Xerox® Secure Access Login Settings.....	67
Setting Up Authentication for a USB Smart Card Reader System .....	68
Authentication Common Access Card (CAC).....	71
Authentication Common Access Card (CAC) Overview.....	71
Supported Card Types .....	71
Supported Card Readers .....	71
Controlling Access to Tools and Features.....	73
Controlling Access for All Users.....	73
Controlling Access for a Group of Users.....	74
Resetting Feature Access for All Local Users .....	76
Digital Certificates .....	77
Installing a Digital Certificate.....	77
Creating a Self-Signed Certificate .....	77
Creating a Request .....	78
Uploading a Certificate.....	78
Managing Certificates .....	78
Certificate Revocation Retrieval Settings .....	79
Secure HTTP and SSL/TLS .....	80
Configuring Secure HTTP (SSL/TLS).....	80
S/MIME.....	82
IPsec.....	83
Configuring IPsec.....	83
802.1X .....	85
Configuring 802.1X.....	85
FIPS140 Data Encryption.....	86
Overwriting Image Data.....	87
Overwriting Image Data in the Embedded Web Server .....	87
Overwriting Image Data at the Control Panel.....	87
IP Filtering .....	89
Creating an IP Filter Rule .....	89
Unbounded Ports .....	90

Adding an Unbounded Port .....	90
Editing an Unbounded Port .....	90
Deleting an Unbounded Port .....	90
Audit Log .....	91
Enabling Audit Log .....	91
Saving an Audit Log .....	91
Interpreting the Audit Log .....	91
PDF and XPS Signatures .....	93
Address Book Security .....	94
Controlling Address Book Access in the Embedded Web Server .....	94
Controlling Control Panel Address Book Access .....	94
Restricting Access to Job Information .....	95
Hiding or Password Protecting Completed Job Information .....	95
Hiding Active Job Information .....	95
Allowing or Restricting Job Operations .....	95
Hiding or Displaying Network Settings .....	97
Restricting Service Representative Operations .....	98
Setting up Service Representative Restrictions .....	98
Limiting Access to Folder Operations .....	99
Printing .....	101
Selecting Print Mode Options .....	102
Language Emulation Settings .....	103
Configuring PostScript 3 Language Emulations .....	103
Configuring PCL® 6/5e Language Emulations .....	103
Configuring TIFF and JPEG Language Emulations .....	103
Configuring HP-GL/2 Language Emulations .....	103
Managing Banner Page Printing Options .....	105
Enabling Banner Page Printing in the Embedded Web Server .....	105
Enabling Banner Page Printing from the Control Panel .....	105
Enabling Banner Page Printing in the Xerox Version 3 Print Driver .....	105
Enabling Banner Page Printing in the Xerox Version 4 Print Driver .....	106
Print Service Settings .....	107
Allocating Memory for Print Settings .....	107
Configuring Other Types of Print Settings .....	107
Media Print Service Settings .....	109
UNIX®, Linux®, and AS/400 Printing .....	110
Xerox® Printer Manager .....	110
Printing from a Linux® Workstation .....	111
AS/400 for IBM Power Systems .....	112
Copying .....	113
Creating Copy Feature Presets .....	114
Specifying Default Copy Settings .....	115
Copy Control .....	116

Original Size Defaults .....	117
Reduce and Enlarge Presets.....	118
Defining Custom Colors.....	119
Scanning.....	121
Configuring General Scan Service Settings .....	122
Setting Scan Defaults .....	122
Configuring Other Scan Settings.....	122
Setting Scan to PC Defaults .....	122
Scanning to a Folder on the Device.....	124
Managing Folders and Scanned Files .....	125
Creating and Editing a Folder.....	125
Scheduling Deletion of Files Stored in Folders.....	125
Configuring Scan Folder Service Settings.....	126
Scanning to an Email Address.....	127
Configuring Email Settings .....	127
Editing Email Settings.....	128
Network Scanning .....	130
Enabling Network Scanning.....	130
Configuring Network Scanning.....	130
Configuring File Repository Settings .....	131
Configuring the Default Template.....	134
Configuring Template Pool Repository Settings.....	136
Updating the List of Templates at the Control Panel.....	136
Configuring a Validation Server .....	136
Scanning to a Home Folder for a User .....	137
Configuring Scan to Home .....	137
Scanning to a USB Drive.....	138
Enabling Scan to USB Functionality.....	138
Job Flow Sheets .....	139
Setting Up a Job Flow Sheet.....	139
Job Flow Sheet Restrictions.....	141
Linking the Job Flow Sheet to a Folder .....	141
Enabling Network Scan Utility 3 .....	143
Faxing.....	145
Embedded Fax.....	146
Enabling Embedded Fax.....	146
Configuring Embedded Fax Settings.....	146
Configuring Fax General Settings.....	147
Enabling the Output Destination .....	147
Configuring Fax Control Settings.....	147
Setting Fax Defaults .....	149
Setting Incoming Fax Options.....	149
Storing and Forwarding Received Faxes.....	150
Storing and Forwarding Faxes Using Fax Identifiers.....	152

Server Fax .....	154
Enabling Server Fax .....	154
Configuring a Fax Repository using FTP .....	154
Configuring a Fax Repository using SMB .....	155
Configuring a Fax Repository using SMTP .....	155
Server Fax Confirmation Report and Job Log .....	155
Internet Fax .....	157
Configuring Internet Fax Settings .....	157
Configuring Internet Fax General Options .....	157
Internet Fax Addresses .....	159
LAN Fax .....	160
Session Initiation Protocol Fax .....	161
Enabling SIP Fax .....	161
Configuring VoIP Gateway Registration .....	162
Configuring T.38 Settings .....	162
Configuring SIP Settings at the Device Control Panel .....	162
Accounting .....	163
Xerox® Standard Accounting .....	164
Configuring Xerox® Standard Accounting .....	164
Creating a Group Account .....	164
Creating a User Account and Setting Usage Limits .....	165
Managing Group Accounts .....	165
Maximum Usage Limits .....	165
Managing Limits for Individual Users .....	166
Managing Limits for Groups .....	166
Resetting Usage Data Values .....	166
Automatically Resetting the Accounting Counters .....	166
Resetting Standard Accounting to Factory-Default Settings .....	167
Printing a Standard Accounting Report .....	167
Local Accounting .....	168
Configuring Local Accounting .....	168
Creating a User Account and Setting Usage Limits .....	168
Resetting Local Accounting Usage Counters .....	169
Automatically Resetting Local Accounting Usage Counters .....	169
Network Accounting .....	170
Enabling and Configuring Network Accounting .....	170
Configuring Accounting Login Screen Settings .....	171
Accounting and Billing Device Settings .....	172
Enabling Accounting in Print Drivers .....	173
Enabling Accounting in a Xerox Version 3 Windows Print Driver .....	173
Enabling Accounting in a Xerox Version 4 Windows Print Driver .....	174
Enabling Accounting in an Apple Macintosh Print Driver .....	175
Administrator Tools .....	177
Monitoring Alerts and Status .....	178

Setting Up Job Completion Alerts .....	178
Setting Up Device Status Alerts .....	178
Activating a Supplies Plan .....	179
Paper Tray Settings .....	180
Accessing Paper Tray Settings .....	180
Setting Custom Paper Name and Color .....	180
Establishing Start-Up Attributes .....	180
Paper Type Priority .....	180
Setting Paper Tray Attributes .....	181
Setting Up a Dedicated Paper Tray .....	182
Changing Paper Settings During Tray Loading .....	182
Establishing Bypass Tray Defaults .....	183
Customizing the Paper Supply Screen .....	183
Paper Tray Priority .....	183
Managing Automatic Tray Switching .....	184
Image Quality .....	185
NVM adjustments required for GBC AdvancedPunch Pro (APP) Software Version .....	185
Paper Catalog .....	185
SMart eSolutions .....	187
SMart eSolutions Overview .....	187
Configuration Planning .....	187
Configuring SMart eSolutions .....	188
Viewing SMart eSolutions Information .....	189
Troubleshooting .....	190
Configuring Stored File Settings .....	193
Retrieving Stored Files .....	194
Setting Default Touch Screen Settings .....	195
Taking the Printer Offline .....	196
Restarting the Device in the Embedded Web Server .....	197
Changing the Power Saver Settings .....	198
View Usage and Billing Information .....	199
Billing Information .....	199
Usage Counters .....	199
Enabling the Billing Impression Mode .....	199
Cloning .....	200
Saving Device Settings .....	200
Installing a Clone File .....	200
Public Address Book .....	201
Address Book Options .....	201
Editing the Public Address Book as a CSV File .....	201
Importing an Address Book File .....	202
Adding, Editing, and Deleting Address Book Entries .....	202
Font Management Utility .....	204
Customizing Device Contact Information .....	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
Two-Sided Color Scanning Calibration.....	218
Image Registration Adjustments .....	220
Adjusting Image Alignment.....	220
Adjusting Fold Position.....	221
Simple Image Quality Adjustment (SIQA) Tools .....	225
Simple Image Quality Adjustment (SIQA) Tools Overview .....	225
Accessing the SIQA Tools.....	225
Image Transfer Adjustment.....	226
Auto Alignment Adjustment .....	229
Density Uniformity Adjustment .....	231
Customization and Expansion .....	233
Xerox® Extensible Interface Platform® .....	234
Enabling Extensible Services .....	234
Enabling Extensible Service Registration.....	234
Customizing Apps on the Printer .....	236
Xerox® App Gallery .....	236
Customizing Apps Available at the Control Panel.....	236
Setting Up Stored Programming .....	237
Enabling Stored Programming.....	237
Setting the Audio Tones for Stored Programming Registration.....	237
Plug-ins and Kits.....	238
Enabling Plug-ins .....	238
Managing Plug-Ins.....	238
Enabling Digital Signature Verification for Secure Plug-Ins.....	238

Auxiliary Interface Kit .....	239
Setting Up the Inserter Module.....	240



# About this Guide

This guide is designed for a System Administrator with network administrator rights who has knowledge of networking concepts as well as experience creating and managing network user accounts.

This guide will help you install, configure, and manage the device on a network.



Note:

- Network features are not available if you are connected over USB.
- Embedded fax features are not available for all device models.



# Introduction

This chapter contains:

Configuration Steps..... 16

More Information ..... 17

## Configuration Steps

When you configure the device for the first time, it is recommended that you follow these steps in this order:



Note: Most configuration settings are on the Properties tab 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 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 <a href="http://www.xerox.com/office/PLC9065_PLC9070support">www.xerox.com/office/PLC9065_PLC9070support</a> , 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	
Recommended Media List	United States: <a href="http://www.xerox.com/rmlna">www.xerox.com/rmlna</a> Europe: <a href="http://www.xerox.com/rlmeu">www.xerox.com/rlmeu</a>
Information about menus or error messages	View the Status area of the control panel touch screen.
Information Pages	To print from the control panel, touch <b>Device &gt; Information Pages</b> or <b>Device &gt; Support &gt; Support Pages</b> . To print from the Embedded Web Server, click <b>Home &gt; Information Pages</b> .
Order supplies for your device	Go to <a href="http://www.xerox.com/office/PLC9065_PLC9070supplies">www.xerox.com/office/PLC9065_PLC9070supplies</a> , then select your specific device model.
Local sales and Technical Customer Support	<a href="http://www.xerox.com/office/worldcontacts">www.xerox.com/office/worldcontacts</a>
Local sales and customer support	
Device registration	<a href="http://www.xerox.com/office/register">www.xerox.com/office/register</a>



# Initial Setup

This chapter contains:

- Physical Connection ..... 20
- Initial Setup at the Control Panel ..... 21
- Administrator Access at the Control Panel..... 22
- Manually Setting the Ethernet Interface Speed ..... 23
- Viewing Services and Options..... 24
- Embedded Web Server..... 25
- Enabling Services and Options..... 26
- Changing the System Administrator Password..... 27
- Using the Configuration Overview Page ..... 28

## 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

### 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, press the **Machine Status** button, then touch the **Device Information** tab. For details, refer to [Administrator Access at the Control Panel](#).
2. Touch **Print Reports**.
3. Touch **Printer Reports**.
4. Touch **Configuration Report**, then press the **Start** button.

## Administrator Access at the Control Panel

To configure the device from the control panel, press the **Machine Status** button, then touch the **Tools** tab. If the device is locked, log in as Administrator.

To log in as Administrator:

1. At the device control panel, press the **Log In/Out** button.
2. Type **admin**, then touch **Next**.
3. Type the administrator password, then touch **Enter**.



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 **Admin**, then touch **Logout**. On the new screen, touch **Logout**.

## LOCKING OR UNLOCKING THE DEVICE

To lock or unlock the device:

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 **Authentication / Security Settings > System Administrator Settings > System Administrator's Login ID**.
3. To lock the device, touch **On**. To unlock the device, touch **Off**. If you touched On, touch **Keyboard**, then type the System Administrator Login ID. Touch **Save**. Touch **Keyboard**, type the Login ID again, then touch **Save**.

To confirm the change, touch **Yes**.

4. Touch **Save**.

## 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, press the **Machine Status** button, then touch the **Tools** tab. For details, refer to [Administrator Access at the Control Panel](#)
2. Touch **System Settings > Connectivity & Network Setup > Protocol Settings**.
3. Touch **Ethernet Settings**, then touch **Change Settings**.
4. Touch **Ethernet - Rated Speed**, then touch **Change Settings**.
5. To match the speed set on your hub or switch, select the speed.
6. Touch **Save**, then touch **Close**.

### 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 **Machine Status** button, then touch the **Device Information** tab.
2. Touch **Device Configuration**.

The Device Configuration screen appears.

3. To close the Device Configuration screen, touch **Close**.

## 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 the **Machine Status** 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. Click the **Properties** tab.
4. 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, press the **Machine Status** button, then touch the **Tools** tab. For details, refer to [Administrator Access at the Control Panel](#).
2. Touch **System Settings > Common Service Settings > Maintenance**.
3. Touch **Software Options**.
4. Touch **Keyboard**.
5. Type the code, then touch **Save**.
6. Touch **Close**.

### ENABLING FEATURES IN THE EMBEDDED WEB SERVER

To enable services and options in the Embedded Web Server:

1. In the Embedded Web Server, click **Properties > Security > Feature Enablement**.
2. For Unique Function Code, type the required information.
3. Click **Apply**.
4. Click **Reboot**.

### ENABLING FEATURES AT THE CONTROL PANEL

1. At the control panel, press the **Log In/Out** button.
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 **Apply**.

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 **Properties > Security > System Administrator Settings**.
2. If required, change the login credentials for Administrator's Login ID.
3. For Administrator's Passcode, type the new password.
4. Retype the password.
5. Click **Apply**.

## Using the Configuration Overview Page

In the Embedded Web Server, the Configuration Overview page provides shortcuts to commonly accessed pages on the Properties tab. To access the Configuration Overview page, click **Properties > Configuration Overview**.

### 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, click **Properties > Description**.
2. For Device Name, type a name for the device.
3. For Location, type the location of the device.
4. In the fields provided, type the Administrator contact information and the device email address, as needed.
5. Click **Apply**.

# Network Connectivity

This chapter contains:

TCP/IP .....	30
SNMP .....	36
LPD .....	39
Raw TCP/IP Printing.....	40
SMTP .....	41
LDAP .....	43
POP3 .....	45
HTTP .....	46
Proxy Server .....	47
Microsoft Networking .....	48
IPP .....	49
Universal Plug and Play Discovery .....	50
SSDP .....	51
WebDAV .....	52
WSD.....	53
FTP .....	54
Google Cloud Print .....	55
Bonjour Multicast DNS.....	56
AirPrint.....	57
Mopria.....	59
SOAP .....	60

## 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, press the **Machine Status** button, then touch the **Tools** tab. For details, refer to [Administrator Access at the Control Panel](#).
2. Touch **System Settings > Connectivity & Network Setup > Protocol Settings**.
3. Touch **TCP/IP - Common Settings**, then touch **Change Settings**.
4. Select the item you want to change, then touch **Change Settings**.
5. Touch **IPv4 Mode** or **IPv6 Mode**. To enable both IPv4 and IPv6, touch **Dual Stack**.
6. Touch **Save**.
7. Touch **Close**.

### 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, press the **Machine Status** button, then touch the **Tools** tab. For details, refer to [Administrator Access at the Control Panel](#).
2. Touch **System Settings > Connectivity & Network Setup > Protocol Settings**.
3. Select **TCP-IP - Network Settings**, then touch **Change Settings**.
4. Select **IPv4 - IP Address Resolution**, then touch **Change Settings**.
5. Touch **Static**, then touch **Save**.
6. Touch **IPv4 - IP Address**, then touch **Change Settings**.
7. Using the touch-screen keypad, type the static IP address, then touch **Save**.
8. Touch **IPv4 - Subnet Mask**, then touch **Change Settings**.
9. Using the touch-screen keypad, type the subnet mask, then touch **Save**.
10. Touch **IPv4 - Gateway Address**, then touch **Change Settings**.
11. Using the touch-screen keypad, type the gateway address, then touch **Save**.
12. Touch **Close**.

## Manually Configuring an IPv6 Network Address

To configure an IPv6 network address:

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 **Connectivity & Network Setup > Protocol Settings**.
3. Touch **TCP/IP - Network Settings**, then touch **Change Settings**.
4. Touch **IPv6 Address Manual Configuration**, then touch **Change Settings**.
5. Touch **Enabled**, then touch **Save**.
6. Touch **Manually Configured IPv6 Address**, then touch **Change Settings**.
7. Using the touch-screen keypad, type the static IP address, then touch **Save**.
8. Touch **Manually Configured IPv6 Address Prefix**, then touch **Change Settings**.
9. Using the touch-screen keypad, type the prefix, then touch **Save**.
10. Touch **Manually Configured IPv6 Address Gateway**, then touch **Change Settings**.
11. Using the touch-screen keypad, type the gateway address, then touch **Save**.
12. Touch **Close**.

## Configuring IPv4 Dynamic Address Settings

To configure IPv4 dynamic address 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 > Connectivity & Network Setup > Protocol Settings**.
3. Touch **TCP/IP - Network Settings**, then touch **Change Settings**.
4. Touch **IPv4 - IP Address Resolution**, then touch **Change Settings**.
5. Touch **DHCP, BOOTP, DHCP/AutoIP, or STATIC**, then touch **Save**.
6. Touch **Close**.

## 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 **Machine Status** button, then touch the **Tools** tab. For details, refer to [Administrator Access at the Control Panel](#).
2. Touch **System Settings > Connectivity & Network Setup > Protocol Settings**.
3. Touch **TCP/IP-Network Settings**, then touch **Change Settings**.
4. Touch **IPv6 Address Manual Configuration**, then touch **Change Settings**.
5. Touch **Disabled**, then touch **Save**.

6. To view the acquired IPv6 address information, touch **Automatically Configured IPv6 Address**, then touch **Change Settings**.
7. Touch **Close**.

### 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, press the **Machine Status** button, then touch the **Tools** tab. For details, refer to [Administrator Access at the Control Panel](#).
2. Touch **System Settings > Connectivity & Network Setup > Protocol Settings**.
3. Touch **TCP/IP - Network Settings**, then touch **Change Settings**.
4. Touch **IPv4 DNS Server Setup**, or **IPv6 DNS Server Setup**, then touch **Change Settings**.
5. Do one of the following:
  - To allow your DHCP server to provide the DNS server address, touch **Get IP Address from DHCP**, then touch **Change Settings**. Touch **Enabled**, then touch **Save**.
  - To provide the DNS server address manually, touch **Preferred DNS Server IP Address**, then touch **Change Settings**. Type the DNS server address, then touch **Save**.
6. Touch **Close**.

### 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 **Properties > Connectivity > Protocols > TCP/IP**.



Note: IPv4 is enabled by default.

2. Type a unique host name for your device.
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. In the Domain Name field, type a valid domain name.
6. Click **Apply**.

### DNS Configuration for IPv4

To configure settings for IPv4:

1. In the Embedded Web Server, click **Properties > Connectivity > Protocols > TCP/IP**.
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. To instruct the device to release its IP address when the device restarts, for Release Current IP Address When the Host is Powered Off, select **Enabled**.
7. Click **Apply**.

## 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 **Properties > Connectivity > Protocols > TCP/IP**.
2. For IP Mode, select **IPv6**, or to use both IPv4 and IPv6, select **Dual Stack**. 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, for Get IP Address from DHCP, select **Enabled**.
6. Type the required Domain Name.
7. Click **Apply**.



Note: If you enable or disable IPv6, when you click Apply, the device restarts.

## DNS Configuration for IPv6

To configure settings for IPv6:

1. In the Embedded WebServer, click **Properties > Connectivity > Protocols > TCP/IP**.
2. Select a method for obtaining the DNS server address:
  - To allow the DHCP server to provide the DNS server address automatically, for DHCPv6–Lite, select **Enabled**.
  - To specify the DNS server addresses manually, for DHCPv6–Lite, clear the check box for **Enabled**. Type the IP addresses of the Preferred DNS Server, the Alternate DNS Server 1, and the Alternate DNS Server 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. To use IPv6 before using IPv4 to resolve DNS, for DNS Resolution via IPv6 First, select **Enabled**.
8. To instruct the device to release the IP address when the device restarts, for Release Current IP Address When the Host is Powered Off, select **Enabled**.
9. Click **Apply**.

### **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 **Properties > Connectivity > Port Settings**.
2. For SNMP, select **Enabled**.
3. To enable the UDP transport protocol if necessary, for UDP, select **Enabled**.
4. Click **Apply**.

### CONFIGURING SNMP

To configure SNMP settings:

1. In the Embedded Web Server, click **Properties > Connectivity > Protocols > SNMP Configuration**.
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 **Apply**.


 Note: If you do not click Apply, the protocol remains disabled.

### 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's Login ID field, type the administrator login credentials.
  7. Click **Apply**.

### 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 **Properties > Connectivity > Protocols > SNMP Configuration**.
2. For SNMP Properties, click **Edit SNMP v3 Properties**.
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 Privacy 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 / Remote Clients Account, click **Account Enabled**.
7. To reset the password, for Reset to default Password, click **Reset**.
8. Click **Apply**.

### Adding IP Trap Destination Addresses

To configure IP trap destinations:

1. In the Embedded Web Server, click **Properties > Connectivity > Protocols > SNMP Configuration**.
2. At the bottom of the page, click **Advanced**.

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 **Apply**.

## 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 **Properties > Connectivity > Port Settings**.
2. For LPD, select **Enabled**.



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

3. Click **Apply**.

### CONFIGURING LPD

To configure the Line Printer Daemon protocol:

1. In the Embedded Web Server, click **Properties > Connectivity > Protocols > 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. Click **Apply**.

## 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 **Connectivity > Port Settings**.
2. For Port 9100, select **Enabled**.
3. Click **Apply**.

### CONFIGURING PORT 9100

To configure port 9100:

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

## 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 **Properties > Connectivity > Protocols > SMTP Server > General**.
2. For SMTP Server Setup, select the needed method to locate an SMTP server.
  - To map to a specific SMTP server, select **STATIC**.
  - To allow DNS to automatically find an SMTP server on the network, select **From DNS**.



Note: If you select From DNS, before you can define the SMTP server, ensure that DNS is configured for either IPv4 or IPv6.

3. Type the SMTP server IP address or host name.
4. Type the port numbers for sending email, sending Internet Fax, and for receiving email. The default port number is 25.
5. For SMTP - SSL / TLS Communication, select an option.
6. Type the Device's Email Address.
7. Click **Apply**.

### 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 **Properties > Connectivity > Protocols > SMTP Server > Connection Test**.
2. In the Connection Test Email area, type your email address.
3. Click **Send Email**.

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.

## 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 **Properties > Connectivity > Protocols > LDAP > LDAP Server**.
2. For Server Information, type the appropriately formatted main and backup LDAP server addresses, host names, and port numbers. The default port number is 389.
3. For LDAP Server, select the type of LDAP server.
4. In the Optional Information 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 5-100.
  - e. For Search Timeout, select **Use LDAP Server Timeout** or **Wait**. If you select **Wait**, type a duration between 5-120 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 1-5.
5. In the Perform Query on 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 **Apply**.

### 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 **Properties > Connectivity > 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. If necessary, to remap fields, for Imported Heading, use the menus.



Note: Headings are defined by your LDAP server schema.

4. Click **Apply**.

## 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**. Then type the LDAP search string or filter that you want to apply.
6. For Internet Fax Address Book Filter, select **Enable Filter**. Then type the LDAP search string or filter that you want to apply.
7. Click **Apply**.

## PERFORMING AN LDAP CONNECTION TEST

To perform the LDAP connection test:

1. In the Embedded Web Server, click **Properties > Connectivity > 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 **Properties > Connectivity > Protocols > POP3 Setup**.
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 Login 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 1–120 minutes. The default value is 10 minutes.
8. Click **Apply**.

## 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. 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 > Connectivity & Network Setup > Port Settings**.
3. Touch **Internet Services (HTTP)**, then touch **Change Settings**.
4. Touch **Port Status**, then touch **Change Settings**.
5. Touch **Enabled**, then touch **Save**.
6. Touch **Close**.

### CONFIGURING HTTP SETTINGS

To configure HTTP settings:

1. In the Embedded Web Server, click **Properties > Connectivity > Protocols > HTTP**.
2. For Maximum Number of Sessions, change the number as needed. The default is 5.
3. To use cross-site request forgery protection, for CSRF Protection, select **Enabled**.
4. Type the port number. The default is 80.
5. You can encrypt HTTP communication between the device and client computers using the Embedded Web Server, including data sent using IPSec, SNMP, and Audit Log. To encrypt HTTP communication, for Secure HTTP (SSL), select **Enabled**. Ensure that a digital certificate is installed on the device.
6. 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.
7. For Connection Timeout, type the number of seconds until the connection times out.
8. Click **Apply**.

## 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 **Properties > Connectivity > Protocols > 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 **Apply**.

## Microsoft Networking

### CONFIGURING WINS

When running Windows Internet Naming Service (WINS), the device registers the IP address and NetBIOS host name with a WINS server. WINS allows users to communicate with the device using the host name only.

To configure primary and secondary WINS servers:

1. In the Embedded Web Server, click **Properties > Connectivity > Protocols > Microsoft Networking**. The SMB client page opens.
2. To allow your DHCP server to provide your WINS server address to the device, for Obtain WINS Server Address Automatically, select **DHCP**.
3. If you want to provide the WINS server address manually, for the Primary Server IP Address field, type the address.
4. If needed, for the Secondary Server IP Address field, type the secondary WINS server address.
5. Click **Apply**.

## 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 **Properties > Connectivity > Port Settings**.
2. For IPP, select **Enabled**.
3. Click **Apply**.

### CONFIGURING IPP

To configure IPP printing:

1. In the Embedded Web Server, click **Properties > Connectivity > 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 Administrator Mode, select **Enabled**.
6. Type the Connection Timeout period. The default is 60 seconds.
7. Click **Apply**.

## 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 **Properties > Connectivity > Port Settings**.
2. For UDP, UPnP Discovery, and SOAP, select **Enabled**.
3. Click **Apply**.

### CONFIGURING UPNP

To configure UPnP:

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

## 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 **Properties > Connectivity > Protocols > SSDP**.
2. For SSDP Port Status, click **Enabled**.
3. For Valid Advertising Period, type an interval value from 60–4320 minutes.



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

4. For Maximum TTL, type a value from 1–10.



Note: Maximum 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 **Apply**.

## 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 **Properties > Connectivity > Port Settings**.
2. For WebDAV, select **Enabled**.
3. Click **Apply**.

### CONFIGURING WEBDAV

To configure WebDAV settings:

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

## 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 **Properties > Connectivity > Port Settings**.
2. To enable the WSD print service, for WSD Print, select **Enabled**.
3. To enable the WSD scan service, for WSD Scan, select **Enabled**.
4. Click **Apply**.

### CONFIGURING WSD

To configure the WSD protocol:

1. In the Embedded Web Server, click **Properties > Connectivity > 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** in seconds. The default is 30.
  - **Notification Delivery Timeout** in seconds. The default is 8.
  - **Maximum TTL**. The default maximum time to live is 1.
  - **Maximum Number of Subscribers**. The default is 50.
3. Click **Apply**.

## 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 **Properties > Connectivity > Port Settings**.
2. For FTP Client, select **Enabled**.
3. Click **Apply**.

### SETTING UP THE FTP TRANSFER MODE

To set up the FTP transfer mode:

1. In the Embedded Web Server, click **Properties > Connectivity > Protocols > FTP**.
2. For Transfer Mode, select **Passive Mode**, or **Active Mode**.
3. Click **Apply**.

### 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 **Apply**.

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.

## Google Cloud Print

The Google Cloud Print service allows users to access the cloud print queue from any Internet-connected device in any geographic location. To allow access to the service, provide users with registration details. Users register for the service with the information that you provide.

### ENABLING GOOGLE CLOUD PRINT

To enable Google Cloud Print:

1. In the Embedded Web Server, click **Properties > Connectivity > Port Settings**.
2. For Google Cloud Print, select **Enabled**.
3. Click **Apply**.

### REGISTERING THE DEVICE WITH THE GOOGLE CLOUD PRINT SERVICE

To allow users to use Google Cloud Print, supply users with the registration details. To print the registration details:

1. In the Embedded Web Server, click **Properties > Connectivity > Protocols > Google Cloud Print**.
2. Click **Register This Device to Google Cloud Print**. The device prints the registration details and instructions.
3. Tell users to complete the registration using the printed information.

The user follows the printed instructions, which registers the device to the Google Cloud Print Service. Information about the registration appears in the Status area of the Google Cloud Print page.

## 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 **Properties > Connectivity > Port Settings**.
2. For Bonjour, select **Enabled**.
3. Click **Apply**.

### CONFIGURING BONJOUR

To configure Bonjour:

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

## 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:

- 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.
- 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 **Properties > Connectivity > Protocols > 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, type the device name and location. Optionally, type the geographical coordinates.
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 Device Digital Certificate area, for Device Digital Certificate Management, click **Settings**.
  - 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 Device Software 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 Check for Update 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 Software Update page, type up to three email addresses, then click **Apply**.

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, click **Back**.
9. To specify what happens when a data error occurs, for Print Job Handling when Data Error Occurs, select **Cancel Print Job** or **Force Print Job**.
10. Click **Apply**.

## 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

To configure Mopria:

1. In the Embedded Web Server, click **Properties > Connectivity > Protocols > Mopria**.
2. Select **Enabled**.
3. Click **Apply**.



Note: Before you disable Mopria, disable IPP and Bonjour. If AirPrint is configured on the printer, disabling IPP and Bonjour also disables AirPrint. To continue to use AirPrint, enable AirPrint again. For details, refer to [Configuring AirPrint](#).

## 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 **Properties > Connectivity > Port Settings**.
2. For SOAP, select **Enabled**.
3. Click **Apply**.

# Security

This chapter contains:

Setting Up Access Rights .....	62
Local Authentication.....	63
Network Authentication .....	65
Authentication Using a Card Reader System .....	67
Authentication Common Access Card (CAC) .....	71
Controlling Access to Tools and Features .....	73
Digital Certificates.....	77
Secure HTTP and SSL/TLS .....	80
S/MIME.....	82
IPsec .....	83
802.1X.....	85
FIPS140 Data Encryption .....	86
Overwriting Image Data.....	87
IP Filtering.....	89
Unbounded Ports.....	90
Audit Log.....	91
PDF and XPS Signatures .....	93
Address Book Security.....	94
Restricting Access to Job Information .....	95
Hiding or Displaying Network Settings .....	97
Restricting Service Representative Operations.....	98
Limiting Access to Folder Operations.....	99

## 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
- **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.

## Local Authentication

### SETTING UP LOCAL AUTHENTICATION

To configure local authentication:

1. In the Embedded Web Server, click **Properties > Security > Authentication Configuration**.
2. On the Authentication Configuration page, for Login Type, select **Log In to Local Accounts**.
3. To enable these services, for Print Stored File from Folder or for Folder to PC/Server, select **Enabled**.
4. To allow users without accounts to access the device, for Non-account Print, select **Enabled**.
5. To use the domain name for print client authentication, select **Enabled**.
6. Click **Apply**, then click **Reboot Device**.

### 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

You can add users to the User Information Database on the device or you can edit existing user information. The database can contain a maximum of 1000 users.

To edit the User Information Database:

1. In the Embedded Web Server, click **Properties > Security > Authentication Configuration**.
2. Click **Next**.
3. In the Authentication Configuration area, for Account Number, type a number from 1–1000, then click **Edit**. Each user in the database has a unique number.
4. In the User Identification area, type the user information:
  - a. For the User Name and UserID fields, type the required information.
  - b. If necessary, type a password, then retype the password.
  - c. Type an email address.
5. In the Feature Access area, specify feature access to the following services for the user:
  - Copy Service
  - Fax Service
  - Scan Service
  - Print Service
  - Device Access

6. In the Impression / Limits area, specify the copy and scan usage limits for the user.




Note: Users can scan up to 5000 impressions per job.

7. In the User Role area, for User Role, select **System Administrator**, **Account Administrator**, or **User**.
8. If needed, add the user to an authorization group.
9. Click **Apply**.

The user is added to the User Information Database. When you add other users, for Account Number, ensure that you type a unique account number for each user.

## SPECIFYING LOGIN REQUIREMENTS

To specify password requirements:

1. In the Embedded Web Server, click **Properties > Security > User Details Setup**.
  2. To display text other than User ID, on the device control panel, in the Alternative Name for User ID field, type the text.
  3. For Mask User ID, select an option:
    - **Hide**: This option shows user ID characters as asterisks on the control panel touch screen.
    - **Show**: This option shows user ID characters as text on the control panel touch screen.
  4. For Failed Access Log, 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.
5. To allow users to log in without case sensitivity, for User ID for Login, select **Non-Case Sensitive**.
  6. In the Login Attempts Limit 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**.
  7. Click **Apply**.

## 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 **Properties > Security > Authentication Configuration**.
2. On the Authentication Configuration page, for Login Type, select **Log In to Remote Accounts**.
3. To enable these services, for Print Stored File from Folder or for Folder to PC/Server, select **Enabled**.
4. To allow users without accounts to access the device, for Non-account Print, select **Enabled**.
5. To allow a guest user to access the device, for Guest User, select **On**. For Guest Passcode, type the guest user password, then for Retype Guest Passcode, type the password again.
6. To use the domain name for authentication, for Use Domain Name for Print Client Authentication, select **Enabled**.
7. Click **Apply**, then click **Reboot Device**.
8. After the device restarts, refresh your browser, navigate back to the **Authentication Configuration > Step 1 of 2** page, and at the bottom of the page, click **Next**.
9. For Authentication System, click **Configure**.
10. On the Authentication System page, select your Authentication System.
11. Type the Server Response Timeout and the Search Timeout.
12. If necessary, to assign the UPN, for Assign UPN (User Principal Name), select **Enabled**.
13. Click **Apply**.
14. Click **Reboot Device**.

### 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 **Apply**.

## CONFIGURING AUTHENTICATION SERVER SETTINGS FOR SMB

To configure settings for the SMB server:

1. In the Embedded Web Server, click **Properties > Security > Remote Authentication Servers > SMB Server**.
2. For SMB Server Setup, select an option:
  - **By Domain Name**
  - **By Domain Name & Server Name / IP Address**
3. For each of your servers, type the Domain Name and Server Name / IP Address.
4. Click **Apply**.



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, click **Properties > Connectivity > Protocols > LDAP > LDAP Authentication**.
2. 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.
3. If you selected Authentication of User Attributes:
  - a. Type the Attribute of Typed 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 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 32 characters.
4. 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.
5. Click **Apply**.

## Authentication Using a Card Reader System

### SETTING UP AUTHENTICATION FOR XEROX® SECURE ACCESS

Before you begin:

- Enable Secure HTTP (SSL).
- Install the Xerox® Secure Access Unified ID System® (authentication server) and configure with user accounts. For details, refer to the authentication server documentation.
- Connect and configure your card reader.
- Install the appropriate plugin for your card reader and device model. Download the latest plugin files and plugin installation instructions from [www.xerox.com/support](http://www.xerox.com/support).



Note: Accounts created on the Xerox® Secure Access authentication server must match accounts stored in the device local database or in another network authentication server.

To configure authentication services for Xerox® Secure Access:

1. In the Embedded Web Server, click **Properties > Security > Authentication Configuration**.
2. On the Authentication Configuration page, for Login Type, select **Xerox Secure Access**.
3. To enable these services, for Print Stored File from Folder or for Folder to PC/Server, select **Enabled**.
4. To allow users without accounts to access the device, for Non-account Print, select **Enabled**.
5. To use the domain name for authentication, for Use Domain Name for Print Client Authentication, select **Enabled**.
6. Click **Apply**, then click **Reboot Device**.
7. After the device restarts, refresh your browser, navigate back to the **Authentication Configuration > Step 1 of 2** page, and at the bottom of the page, click **Next**.
8. For Authentication System, click **Configure**.
9. On the Authentication System page, from the drop-down list, select **Authentication Agent**.
10. Type the Server Response Timeout and the Search Timeout.
11. If necessary, for Assign UPN (User Principal Name), select **Enabled**.
12. Click **Apply**.
13. Click **Reboot Device**.

### CONFIGURING XEROX® SECURE ACCESS LOGIN SETTINGS

To configure Xerox® secure access login settings:

1. In the Embedded Web Server, click **Properties > Security > Remote Authentication Servers > Xerox Secure Access Settings**.
2. Type the **Default Prompt** text and **Default Title** text.
3. To allow users to type their credentials at the control panel, for Local Login, select **Enabled**.

4. To allow the device to obtain the user accounting code from a network accounting server automatically when the user logs in at the control panel, for Get Accounting Code, select **Enabled**.  
Ensure that network authentication and network accounting are configured. If Get Accounting Code is not enabled, the user is required to type an accounting code when logging in at the control panel.
5. For Connection Timeout, type a connection timeout from 1-300 seconds.
6. Click **Apply**.

## 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

#### Enabling USB for Smart Cards

To enable the USB interface for a smart card reader:

1. In the Embedded Web Server, click **Properties > Services > USB > General**.
2. To enable USB for smart cards, for Smart Card, select **Enabled**. To use the public key infrastructure for Smart Card certificates, select **Enabled (PKI Only)**.
3. Click **Apply**.

#### Enabling Smart Cards

To enable smart cards:

1. In the Embedded Web Server, click **Properties > Security > Smart Card Settings > General**.
2. For Smart Card, click **Enabled**.
3. To enable login and logout tones for a non-contact card reader, for Smart Card Log In / Out Tone, select **Enabled**.
4. Click **Apply**.

#### Setting Smart Card Certificate Information

To set certificate information for smart cards:

1. In the Embedded Web Server, click **Properties > Security > Smart Card Settings > Certificate Settings**.
2. To verify certificates, for Certificate Verification, select **Enabled**.
3. Type the hexadecimal values for the object identifiers for the authentication, signing, and encryption certificates.
4. Click **Apply**.

## 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 **Machine Status** button, then touch the **Tools** tab. For details, refer to [Administrator Access at the Control Panel](#).
2. Touch **Authentication / Security Settings > Authentication > User Details Setup > Use of Smart Card**.
3. Touch **Change Settings**.
4. To enable the use of a smart card, touch **Enabled**. To use the public key infrastructure for the certificates, touch **Enabled (PKI Only)**.
5. For Jobs Validated by Card, select **Copy, Print, or Fax / Scan**, as needed



Note: You can select any or all of the available options.

6. Touch **Save**.

### 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 **Machine Status** button, then touch the **Tools** tab. For details, refer to [Administrator Access at the Control Panel](#).
2. Touch **Authentication / Security Settings > Authentication > User Details Setup > Smart Card Certificate Verification**.
3. Touch **Change Settings**.
4. Touch **Enabled**.
5. Touch **Save**.



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 **Machine Status** button, then touch the **Tools** tab. For details, refer to [Administrator Access at the Control Panel](#).
2. Touch **Authentication / Security Settings > Authentication > User Details Setup > Smart Card Logout Timing**.
3. Touch **Change Settings**.
4. Select **Log Out when Card is Removed** or **Log Out from Control Panel**.
5. Touch **Save**.

## 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

## Security

- 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

#### Locking or Unlocking Tools and Features for All Users

You can configure the device to require users to authenticate themselves to access tools and features at the control panel and in the Embedded Web Server.

To lock or unlock tools and features:

1. In the Embedded Web Server, click **Properties > Security > Authentication Configuration**.
2. Click **Next**.
3. In the Access Control area, for Device Access, click **Configure**.
4. For Services Pathway, to require authentication for all services at the control panel, select **Locked**. To allow unauthenticated access, select **Unlocked**.
5. For Job Status Pathway, to require authentication for all services accessed from the Job Status button, select **Locked**. To allow unauthenticated access, select **Unlocked**.
6. For Machine Status Pathway, to require authentication for all services accessed from the Machine Status button, select **Locked**. To allow unauthenticated access, select **Unlocked**.
7. For Local UI Tools & CWIS Properties Tab, to require authentication for all services in the Tools tab at the control panel, and for the Properties tab in the Embedded Web Server, select **Locked**. To allow unauthenticated access, select **Unlocked**.
8. Click **Apply**.

#### Locking, Unlocking, or Hiding Individual Services for All Users

1. In the Embedded Web Server, click **Properties > Security > Authentication Configuration**.
2. Click **Next**.
3. In the Access Control area, for Service Access, click **Configure**.
4. To require authentication for all services, click **Lock All**. To allow unauthenticated access to all services, click **Unlock All**.
5. To set the access for each individual service, select the required access:
  - **Locked (Show Icon)**: Use this setting to require authentication for the service at the control panel. The service icon is visible to all users.
  - **Locked (Hide Icon)**: Use this setting to require authentication for the service at the control panel. The service icon is hidden until an authorized user logs in.
  - **Locked**: Use this option to hide the service so that it is not available at the control panel.
  - **Unlocked**: Use this option to allow access to the service without authentication.
6. Click **Apply**.

## CONTROLLING ACCESS FOR A GROUP OF USERS

If your network is connected to an LDAP server, you can configure network authentication and control individual access to services and features for users or groups.

You can use LDAP server user groups to control access to device services and features. For example, if the LDAP server contains a group of users called Admin, you can configure the Admin group on the device so that only members of this group have administrator access to the device. When a user belonging to the group Admin logs onto the device, the device performs an LDAP directory lookup to verify the user. Once authenticated, the user is allowed administrative rights to the device.

You can set up and control access to your device:

- User Roles Access Setup
- Device Access Setup
- Service Access Setup
- Feature Access Setup

Before you begin:

- Configure [Network Authentication](#).
- Configure [LDAP Server Settings](#).

### User Role Access Setup

To assign users to specific access groups according to role:

1. In the Embedded Web Server, click **Properties > Connectivity > Protocols > LDAP > LDAP Authorization Access**.
2. In the User Role area, for System Administrator Access, click **Edit**.
3. For System Administrator Access, type the name of the group, defined in the LDAP server database, that you want to use to grant system administrator access to the device. Click **Apply**.
4. For Accounting Administrator Access, click **Edit**.
5. Type the name of the group, defined in the LDAP server database, that you want to use to grant accounting administrator access to the device. Click **Apply**.
6. Continue with other access settings, as needed.
  - [Device Access Setup](#)
  - [Service Access Setup](#)
  - [Feature Access Setup](#)
7. Click **Apply**.

## Device Access Setup



Note: Device Access setup requires that authentication is enabled and that Tools and Feature Access are configured to require users to log in before they can access pathways.

To set up device access:

1. In the Embedded Web Server, click **Properties > Connectivity > Protocols > LDAP > LDAP Authorization Access**.
2. In the Device Access area, for Services Pathway, click **Edit**. Type the name of a group, defined at the LDAP server, that you want to use to provide access to the services features on the device.
3. Click **Apply**.
4. Repeat the same process for the Job Status Pathway and Machine Status Pathway.
5. Continue with other access settings, as needed.
  - [User Role Access Setup](#)
  - [Service Access Setup](#)
  - [Feature Access Setup](#)
6. Click **Apply**.

## Service Access Setup



Note: Service Access Setup requires that authentication is enabled and that Tools and Feature Access are configured to require users to log in before they can access services.

You can specify access to the services of the device in the Service Access area. Type the names of the LDAP groups for any of the services listed.

To set up service access:

1. In the Embedded Web Server, click **Properties > Connectivity > Protocols > LDAP > LDAP Authorization Process**.
2. In the Service Access area, for the service, click **Edit**.
3. Type the name of the LDAP group allowed to access the service, then click **Apply**.
4. Repeat the process for each of the individual services in the Service Access area, as needed.
5. Continue with other access settings, as needed.
  - [User Role Access Setup](#)
  - [Device Access Setup](#)
  - [Feature Access Setup](#)
6. Click **Apply**.

## Feature Access Setup



Note: Feature Access Setup requires that authentication is enabled and Tools and Feature Access are configured to require users to log in before they can access features.

You can set specific access to the color copying feature of the device listed on the Feature Access page.

To set up feature access:

1. In the Embedded Web Server, click **Properties > Connectivity > Protocols > LDAP > LDAP Authorization Access**.
2. In the Feature Access area, for Color Copying, click **Edit**.
3. Type the names of the LDAP groups allowed to access the color copying feature, then click **Apply**.
4. Continue with other access settings, as needed.
  - [User Role Access Setup](#)
  - [Device Access Setup](#)
  - [Service Access Setup](#)
5. Click **Apply**.

## RESETTING FEATURE ACCESS FOR ALL LOCAL USERS

Before you begin, configure the device for local authentication. Add user information and feature access information to the User Information Database. For details, refer to [Local Authentication](#).

To reset feature access for all local users:

1. In the Embedded Web Server, click **Properties > Security > Authentication Configuration**.
2. Click **Next**.
3. In the Authentication Configuration area, for All User Accounts, click **Edit**.
4. For Reset All Feature Access, select **Reset**.
5. Click **Apply**.

## 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 **Properties > Security > Device Digital Certificate Management**.
3. Click **Create New Certificate**.
4. Select **Self Signed Certificate**.
5. Click **Continue**.
6. Select a Digital Signature Algorithm.
7. Select a Public Key Size and type the name of the Issuer.
8. For Days of Validity, type the number of days, 1-9999, until the certificate expires.
9. Click **Apply**.

## CREATING A REQUEST

To create a request:

1. In the Embedded Web Server, click **Properties > Security > Device Digital Certificate Management**.
2. Click **Create New Certificate**.
3. Select **Certificate Signing Request (CSR)**, then click **Continue**.
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, and Organization Unit.
5. Click **Apply**.
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 **Properties > Security > Device Digital Certificate Management**.
2. Click **Upload Signed Certificate**.
3. If the certificate is password-protected, type the password, then retype the password.
4. Click **Browse** or **Choose File**, navigate to the signed certificate in .crt format, then click **Open** or **Choose**.
5. Click **Import**.



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 **Properties > Security > Certificate Management**.
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, then click **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, click **Delete**.
7. To save the certificate to your computer, click **Export this certificate**.

## CERTIFICATE REVOCATION RETRIEVAL SETTINGS

To configure certificate revocation retrieval settings:

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

## 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 SECURE HTTP (SSL/TLS)



Note:

- Before you can enable Secure HTTP, ensure that you install a digital certificate on the device.
- If Secure HTTP is enabled, all pages in the Embedded Web Server contain **https://** in the web page URL.

To configure HTTP SSL / TLS settings:

1. In the Embedded Web Server, click **Properties > Security > SSL / TLS Settings**.
2. For HTTP - SSL/TLS Communication, select **Enabled**.
3. Type the port number you want to use for HTTP SSL / TLS.
4. To use secure LDAP, for LDAP - SSL/TLS Communication, select **Enabled**.
5. To use secure email, for SMTP - SSL / TLS Communication, select a method that your server supports:
  - **STARTTLS (If Available)**
  - **STARTTLS**
  - **SSL / TLS**



Note: If you are unsure what method your server supports, select **STARTTLS (If Available)**. If you select STARTTLS, the device attempts to use STARTTLS. If your server does not support STARTTLS, SMTP communication is not encrypted.

6. To use POP3, for POP3 - SSL / TLS Communication, select **Enabled**.
7. To use S/MIME, for S/MIME Communication, select **Enabled**.
8. To verify a remote server certificate, for Verify Remote Server Certificate, select **Enabled**.
9. For Protocol Version, select the TLS version to be used.

10. Click **Apply**.

## 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 **Properties > Security > 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. Type 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 **Apply**.

## 802.1X

802.1X is an Institute for Electrical and Electronics Engineers (IEEE) standard that defines a method for port-based network access control or authentication. In an 802.1X-secured network, the 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, click **Properties > Security > IEEE 802.1X**.
2. For Enable IEEE 802.1x, select **Enabled**.
3. For Authentication Method, select the method used on your network:
  - **EAP-TTLS / PAP**
  - **EAP-TTLS / CHAP**
  - **EAP-TTLS / MS-CHAPv2**
  - **PEAP / MS-CHAPv2**



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

4. For Login Name: (Device Name), type the login name required by your authentication switch and server.
5. Type the password, then retype the password.
6. If necessary, for Certificate Validation, select **Enabled**.
7. Click **Apply**.

## FIPS140 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 FIPS140. You can warn users with a control panel message when data is about to be transmitted that is not encrypted to FIPS140 standard. For details, refer to the device Security White Paper on the Xerox website.

To enable the data encryption warning message:

1. In the Embedded Web Server, click **Properties > Security > FIPS140 Validation Mode**.
2. For FIPS140 Validation Mode, select **Enabled**.
3. Click **Apply**.



Note: FIPS140 encryption does not apply to the SMB protocol or to the PDF Direct Print Service.



Note: Support for FIPS140 is compliant with the SFTP protocol.

## Overwriting Image Data

To ensure that image data on the device hard drive is not accessible, you can delete and overwrite image data. Image data is any and all in-process or temporary user data on the hard drive, such as current jobs, queued jobs, and temporary scan files, but not saved jobs or folders. To use this feature, you must purchase and install the Data Security Kit.

### OVERWRITING IMAGE DATA IN THE EMBEDDED WEB SERVER

#### Deleting Image Data Immediately

To delete image data from the device hard drive:

1. In the Embedded Web Server, click **Properties > Security > On Demand Overwrite > Immediate**.
2. Select the number of overwrites to perform.
3. Click **Apply**.

While the data is deleted, the device is offline. When the process has completed, the device restarts.

#### Scheduling Routine Deletion of Image Data

To schedule a regular time to delete the image data from the device hard drive:

1. In the Embedded Web Server, click **Properties > Security > On Demand Overwrite > Scheduled**.
2. For Scheduled Image Overwrite, select **Enabled**.
3. Select the Frequency of the overwrite operation.
4. To specify when you want the image data deleted, set the date, day, and time, as needed.
5. Click **Apply**.

#### Manually Deleting Image Data

To remove image data manually:

1. In the Embedded Web Server, click **Properties > Security > On Demand Overwrite > Scheduled**.
2. Click **Start**.

While the data is deleted, the device is offline. When the process has completed, the device restarts.

### OVERWRITING IMAGE DATA AT THE CONTROL PANEL

#### Manually Deleting Image Data

To delete image data from the device hard drive manually:

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 **Authentication / Security Settings > Overwrite Hard Disk**.
3. Touch **Number of Overwrites**, then touch **1 Overwrite** or **3 Overwrites**.
4. Touch **Save**.
5. Touch **Run Image Overwrite**.
6. Touch **Start**.
7. Touch **Yes**. The following data is deleted:
  - Secure, Sample, and Delay print jobs
  - Images stored in folders
  - PDL spool files
  - Fax documents
  - All temporary files



Note:

- All image data is deleted.
- While data is deleted, the device is offline. When the process has completed, the device restarts.

### Scheduling Routine Deletion of Image Data

To schedule a regular time for image data to be deleted from the device hard drive:

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 **Authentication / Security Settings > Overwrite Hard Disk**.
3. Touch **Number of Overwrites**, then touch **1 Overwrite** or **3 Overwrites**.
4. Touch **Save**.
5. Touch **Scheduled Image Overwrite**.
6. Touch **Daily**, **Weekly**, or **Monthly**. To specify when you want image data deleted, use the arrow icons.



Note: All image data is deleted.

## 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 **Properties > Security > IP Filtering**.
2. For IPv4 Filtering or IPv6 Filtering, select **Enabled**.
3. For the option that you enabled, click **Add**.
4. In the Define IP Filter Rule area, type the Source IP Address. 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 **Apply**, 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 **Apply**.

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 **Properties > Security > Unbounded Port**.
2. Click **Add**.
3. Type the port number.
4. For Port Destination, select **Source** or **Destination**.
5. For Protocol, select **TCP** or **UDP**.
6. Click **Apply**.

### EDITING AN UNBOUNDED PORT

To edit an unbounded port:

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

### DELETING AN UNBOUNDED PORT

To delete an unbounded port:

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

## 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 **Properties > Security > Audit Log**.
2. For Audit Log, select **Enabled**.
3. Click **Apply**.

### SAVING AN AUDIT LOG

1. In the Embedded Web Server, click **Properties > Security > Audit Log**.
2. For Export Audit Log, right-click the **Export as text file** link and save the compressed **auditfile.txt** file to your computer.
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 Server Fax jobs, an audit log entry is recorded for each Server Fax 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.

## PDF and XPS Signatures

You can add a digital signature to PDF or XPS 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 **Properties > Security > PDF / XPS Signature Settings**.
2. For PDF Signature, select when you want the signature added.
3. Select the required PDF Signature Hash Algorithm.
4. For XPS Signature, select when you want the signature added.
5. For Signing Certificate, select the type of certificate to which these changes apply.
6. Click **Apply**.

## Address Book Security

### CONTROLLING ADDRESS BOOK ACCESS IN THE EMBEDDED WEB SERVER

You can allow all users to edit the public address book in the Embedded Web Server or you can restrict access to system administrators only.

To control address book access:

1. In the Embedded Web Server, click the **Address Book** tab.
2. In the Security area, click **Access Rights**.
3. Select **System Administrators Only** or **Open to All Users**.
4. Click **Apply**.

### CONTROLLING CONTROL PANEL ADDRESS BOOK ACCESS

Before you begin, configure local authentication. For details, refer to [Setting Up Local Authentication](#). To restrict users from using or editing the address book at the control panel you can create an Authorization Group.

To restrict access to the control panel address book:

1. In the Embedded Web Server, click **Properties > Security > Create Authorization Groups**.
2. For one of the group numbers, click **Edit**.
3. Type the Group Name.
4. To allow access for the group, for Restrict Recipient Selection Method, select **No Restriction**, or to require authentication for the group, **Always Apply Restriction**.
5. For Restrict User to Edit Address Book, select **No Restriction**, or **Always Apply Restriction**.
6. For Allow User to Disable Active Settings, select **Allow** or **Do Not Allow**.
7. Click **Apply**.

## Restricting Access to Job Information

You can control how job information displays at the control panel when the user presses the Job Status button.

### HIDING OR PASSWORD PROTECTING COMPLETED JOB INFORMATION

To control access to completed job information:

1. In the Embedded Web Server, click **Properties > Security > Job Status Default > Completed Jobs View**.
2. For Completed Jobs View, select an option:
  - **Require Login to View Jobs:** This option allows users to view completed jobs only when they are logged in.
  - **No Job Viewing:** This option prevents users from seeing completed job information.
3. If you selected 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 **Apply**.

### HIDING ACTIVE JOB INFORMATION

To hide or show active job information:

1. In the Embedded Web Server, click **Properties > Security > Job Status Default > Active Jobs View**.
2. For Hide Job Details, select an option:
  - To hide job details, select **Yes**.
  - To show job details, select **No**.
3. Click **Apply**.

### ALLOWING OR RESTRICTING JOB OPERATIONS

To control the job operations that a user can perform:

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

## Hiding or Displaying Network Settings

To show or hide the IPv4 address or host name of the device on the control panel touch screen:

1. In the Embedded Web Server, click **Properties > Security > Display Network Settings**.
2. Select **Show IP Address (IPv4 only)** or **Show Host Name**. To hide network information, select **Hide Network Information**.
3. Click **Apply**.

## 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 **Properties > Security > Service Representative Restricted Operation**.
2. For Restricted Operation, select **Enabled**.
3. To set a password, type and retype the password.
4. Click **Apply**.

## Limiting Access to Folder Operations

You can limit access to folder operations on the device. Limiting access forces users to provide a password to perform a folder operation. The restriction does not apply to any folders that are already registered.

1. In the Embedded Web Server, click **Properties > Security > Limit Access to Folder**.
2. For Limit Access, select **Enabled**.
3. Click **Apply**.



# Printing

This chapter contains:

- Selecting Print Mode Options ..... 102
- Language Emulation Settings..... 103
- Managing Banner Page Printing Options ..... 105
- Print Service Settings ..... 107
- UNIX®, Linux®, and AS/400 Printing ..... 110

## Selecting Print Mode Options

To specify the print mode that you want the device to use for individual protocol types:

1. In the Embedded Web Server, click **Properties > Services > Printing > Print Mode**.
2. For each print mode listed, select **Auto**, **PostScript 3**, **HP-GL/2**, **PCL 6 / 5e**, or **TIFF / JPEG**.
3. For each print mode, select **PJL** as needed.

## 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 3 LANGUAGE EMULATIONS

To configure PostScript 3 language emulations:

1. In the Embedded Web Server, click **Properties > Services > Printing > Language Emulations > PostScript 3**.
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. Click **Apply**.
5. For Memory Settings, select **Factory Settings** or select **Logical Printer Number**.
6. Set the user details, then enable the native mode of the print driver, as needed.
7. Click **Apply**.
8. To view the color profiles, in the Profiles area, click **List of Profiles**.
9. To return to the Language Emulations page, click **Back**.

### CONFIGURING PCL® 6/5E LANGUAGE EMULATIONS

To configure PCL® 6/5e language emulations:

1. In the Embedded Web Server, click **Properties > Services > Printing > Language Emulations > PCL 6 / 5e**.
2. In the Language Emulations area, set the printer settings as needed.
3. Click **Apply**.

### CONFIGURING TIFF AND JPEG LANGUAGE EMULATIONS

To configure TIFF and JPEG language emulations:

1. In the Embedded Web Server, click **Properties > Services > Printing > 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. Click **Apply**.
5. For Memory Settings, select **Factory Settings** or select **Logical Printer Number**.
6. Click **Apply**.

### CONFIGURING HP-GL/2 LANGUAGE EMULATIONS

To configure HP-GL/2 language emulations:

1. In the Embedded Web Server, click **Properties > Services > Printing > 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. Click **Apply**.
5. For Memory Settings, select **Factory Settings** or **Logical Printer Number**.
6. Click **Apply**.

## 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 **Properties > Services > Printing > Print Mode**.
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 **Apply**.

### 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 **Machine Status** button, then touch the **Tools** tab. For details, refer to [Administrator Access at the Control Panel](#).
2. Touch **System Settings > Print Service Settings > Other Settings**.
3. Touch **Banner Pages**.
4. Touch **Change Settings**.
5. Touch **Start Page**, **End Page**, or **Start Page & End Page**.
6. To allow banner page printing to be enabled or disabled from the print driver, touch **Allow Print Driver to Override**.
7. Touch **Save**.

### 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 **Machine Status** button, then touch the **Tools** tab. For details, refer to [Administrator Access at the Control Panel](#).
2. Touch **System Settings > Print Service Settings > Allocate Memory**.
3. Touch a selection, then touch **Change Settings**. 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 **Save**.

### CONFIGURING OTHER TYPES OF PRINT 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 > Print Service Settings > Other Settings**.

3. Touch an item, then touch **Change Settings**.

- **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**, or **Select Tray 5**.
- **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**.

- **XPS Print Ticket Processing:** You can specify how the device processes print tickets in XPS documents. To use the Microsoft-compliant mode, touch **Compatible Mode**. Otherwise, touch **Standard Mode**. To disable this feature, touch **Off**.
  - **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**.
4. Touch **Save**.
  5. Touch **Close**.

## MEDIA PRINT SERVICE SETTINGS

The media print service allows you to associate paper trays with different paper supplies.

### Enabling the Media Print Service

To enable the media print service:

1. In the Embedded Web Server, click **Properties > Services > Media Print > General**.
2. For Media Print, select **Enabled**.
3. Click **Apply**.

### Enabling the Media Print Service for USB

To enable the media print service for USB:

1. In the Embedded Web Server, click **Properties > Services > USB > General**.
2. For Media Print, select **Enabled**.
3. Click **Apply**.

### Configuring Media Print Service Settings

To configure media print 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 > Media Print Service Settings**.
3. To associate a paper tray to a paper supply selection, from the list, select a paper supply preset, then touch **Change Settings**.
4. Select the tray to be associated to the selected paper supply, then touch **Save**.



Note: The Media Print - Text feature allows users to print PDF, JPG, TIFF, and XPS files directly from a USB Flash Drive.

## 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](http://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-Linuxia64-x.xx.xxx.xxxx.rpm to support RPM-based 32-bit Linux environments
    - Xeroxv5Pkg-Linuxia64-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`
  - HP-UX: `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 `xeroxpmtmgr`, 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](http://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](http://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](http://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:

Creating Copy Feature Presets .....	114
Specifying Default Copy Settings .....	115
Copy Control .....	116
Original Size Defaults .....	117
Reduce and Enlarge Presets .....	118
Defining Custom Colors .....	119

## Creating Copy Feature Presets

To define a preset for commonly used copy 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 > Copy Service Settings**.
3. Touch **Preset Buttons**.
4. Touch a preset in the list, then touch **Change Settings**.
5. Make the required changes to the preset, then touch **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 **Machine Status** button, then touch the **Tools** tab. For details, refer to [Administrator Access at the Control Panel](#).
2. Touch **System Settings > Copy Service Settings**.
3. Touch **Copy Defaults**.
4. Touch the desired setting. For details on copy settings, refer to the *Xerox® PrimeLink™ C9065/C9070 Printer User Guide*.
5. Touch **Change Settings**.
6. Make the required changes to the setting, then touch **Save**.

## Copy Control

To control copy 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 > Copy Service Settings**.
3. Touch **Copy Control**.
4. Touch a setting in the list.
5. Touch **Change Settings**.
6. Make the required changes, then touch **Save**.

## Original Size Defaults

To change the default size specifications for originals:

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 > Copy Service Settings**.
3. Touch **Original Size Defaults**.
4. Touch an original size in the list.
5. Touch **Change Settings**.
6. Make the required changes to the preset, then touch **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 **Machine Status** button, then touch the **Tools** tab. For details, refer to [Administrator Access at the Control Panel](#).
2. Touch **System Settings > Copy Service Settings**.
3. Touch **Reduce / Enlarge Presets**.
4. Touch a preset in the list, then touch **Change Settings**.
5. Make the required changes to the preset, then touch **Save**.

## Defining Custom Colors

To define custom colors:

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 > Copy Service Settings**.
3. Touch **Custom Colors**.
4. Touch a custom color in the list, then touch **Change Settings**.
5. To increase or decrease the values for Yellow, Magenta, or Cyan, touch the arrows.
6. Touch **Save**.



# Scanning

This chapter contains:

Configuring General Scan Service Settings .....	122
Scanning to a Folder on the Device .....	124
Managing Folders and Scanned Files .....	125
Scanning to an Email Address .....	127
Network Scanning.....	130
Scanning to a Home Folder for a User.....	137
Scanning to a USB Drive .....	138
Job Flow Sheets.....	139
Enabling Network Scan Utility 3.....	143

## 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 **Machine Status** button, then touch the **Tools** tab. For details, refer to [Administrator Access at the Control Panel](#).
2. Touch **System Settings > Scan Service Settings > Scan Defaults**.
3. To change a default setting:
  - a. Touch a default setting, then touch **Change Settings**.
  - b. Change the default setting, then touch **Save**.
4. Touch **Close**.

### CONFIGURING OTHER SCAN SETTINGS

To define other scanning settings for all users:

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 > Scan Service Settings > Other Settings**.
3. To change a setting:
  - a. Touch a setting, then touch **Change Settings**.
  - b. Make the appropriate change, then touch **Save**.
4. Touch **Close**.

### 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 **Machine Status** button, then touch the **Tools** tab. For details, refer to [Administrator Access at the Control Panel](#).
2. Touch **System Settings > Scan Service Settings > Scan to PC Defaults**.
3. In the list, touch a default setting, then touch **Change Settings**.

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 selected 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**.

## 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. In the Embedded Web Server, click the **Scan** tab, then click **Folder**.
2. For an available folder, click **Create**.
3. Type a name for the folder.
4. If required, type a Folder Passcode, then retype the passcode.
5. For Check Folder Passcode, select an option:
  - To check the passcode for every job operation, select **Always**.
  - To check the passcode when saving or modifying jobs, select **Save (Write)**.
  - To check the passcode when printing or deleting jobs, select **Print / Delete**.
  - To ignore the passcode for all operations, select **Off**.
6. To delete files after they are printed or retrieved, for Delete Files after Print or Retrieve, select **Enabled**.
7. To delete files after the stored file folder date expires, for Delete Expired Files, select **Enabled**.
8. Click **Apply**.

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 **Edit**.
  - Click **Delete**, then to confirm the deletion, click **OK**.
- To view the list of files in a folder, for the folder, click **File List**.

### 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 **Machine Status** button, then touch the **Tools** tab. For details, refer to [Administrator Access at the Control Panel](#).
2. Touch **System Settings > Stored File Settings**.
3. Touch **Expiration Date for Files Stored in Folder**, then touch **Change Settings**.
4. Touch **On**. Select the number of days that files are kept before deletion. Select the time that the files are deleted on the last day.  
If necessary, to move between fields, touch **Next**.
5. Touch **Save**.

## 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](http://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, press the **Machine Status** button, then touch the **Tools** tab. For details, refer to [Administrator Access at the Control Panel](#).
2. Touch **System Settings > Email/ Internet Fax Service Settings > Email Control**.
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:

- **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.
- **Incoming 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**.
- **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**.
- **Split Send Method:** To split a large email into multiple email messages, touch **Split into Pages**, or **Split by Data Size**.
- **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.
- **Allow Casual Users to Edit From Field:** To allow any user to edit the From field of an email, touch **Yes**.
- **Allow Guest Users to Edit From Field:** To allow users authenticated as a guest to edit the From field of an email, touch **Yes**.
- **Allow to Edit From if Search Found:** To allow users to edit the From field of an email if a search for an email address in the address book is successful, touch **Yes**.

- **Allow to Edit From if Search Failed:** To allow users to edit the From field of an email if a search for an email address in the address book fails, touch **Yes**.
  - **Email Sending When Search Failed:** To disable the Email service if a search for an email address in the address book fails, touch **Enabled**.
  - **Add Me to [To] Field:** To automatically add the authenticated user email address to the To field of an email, touch **Yes**.
  - **Add Me to [Cc] Field:** To automatically add the authenticated user email address to the Cc field of an email, touch **Yes**.
  - **Edit Email Recipients:** To allow users to edit the To, Cc, and Bcc fields of an email, touch **Yes**.
4. Touch **Close**.

## EDITING EMAIL SETTINGS

To edit general email settings in the Embedded Web Server:

1. In the Embedded Web Server, click **Properties > Services > Email > General**.
2. Click **Edit**.
3. Change the email settings as needed:
  - For Receiving Protocol, select **POP3** or **SMTP**.
  - For From Address, type the text that you want to appear in the From field of email messages.
  - For From Name, type the text that you want to appear in the Name field of email messages.
  - For Allow Authenticated Users to Edit [From:] Field when, select: **Address Book (LDAP) Search Successful** or **Address Book (LDAP) Search Failure**.
  - To allow users authenticated as a guest to edit the From field of an email, for Allow Guest Users to Edit [From:] Field, select **Yes**.
  - To allow authenticated users to send an email if the user search in the address book fails, for Allow Authenticated Users to send Email despite LDAP Search Failure, select **Yes**.
  - To allow users to edit the From field of an email if the user search for an email address in the address book is successful, for Edit [From:] Field when Authorization is not Required, select **Yes**.
  - For Subject, type the text that you want to appear in the Subject field of email messages.
  - For Message, type the text that you want to appear in the body of email messages.
  - In the User, Attachment, and Device Information areas, select additional information that you want to add to the body of email messages.
  - For Signature, type the text that you want to be added to the end of the body of email messages.
  - To use email encryption, for Encryption, select **Enabled**.
  - From the Confirmation Sheet drop-down menu, select an option:
    - To print a confirmation sheet only when an error occurs, select **Errors Only**.
    - To print a confirmation sheet after every email transmission, select **On**.

- To prevent confirmation sheets from printing, select **Off**.
  - To add the email address for the authenticated user to the To field of an email automatically, for Add Me to [To] Field, select **Enabled**.
  - To add the email address for the authenticated user to the Cc field of an email automatically, for Add Me to [Cc] Field, select **Enabled**.
  - To allow users to edit the To, Cc, and Bcc fields of an email, for Edit Email Recipients, select **Enabled**.
  - For Incoming Email Print Options, select the parts of the email that you want to print.
  - For Print Delivery Confirmation Email, select an option:
    - To prevent an email delivery confirmation message from printing, select **Off**.
    - To print an email delivery confirmation message after every email transmission, select **On**.
    - To print an email delivery confirmation message only when transmission fails, select **Print when delivery fails**.
  - To print an error report when an email transmission error occurs, for Print Error Notification Email, select **Enabled**.
  - To allow the device to respond to a request for a read receipt (MDN) after an email is received, for Response to Read Receipts, select **Enabled**.
  - For Domain Filtering, select an option:
    - To block email transmissions to or from specific domains, select **Block Domains**, then click **Edit**. On the Domain Filter Settings page, type the domain names that you want to block, then click **Apply**.
    - To allow email transmissions to or from specific domains, select **Allow Domains**, then click **Edit**. On the Domain Filter Settings page, type the domain names that you want to allow, then click **Apply**.
4. Click **Apply**.

## Network Scanning

Network Scanning allows you to scan an original document and distribute and archive the scanned image file. The Network Scanning feature is designed to simplify the task of scanning many multi-page documents and saving the scanned image files in one or more file locations.

To specify how and where scanned images are stored, you must create a template. You can create, manage, and store multiple templates in a template pool repository on a network server. Xerox® software, such as SMARTsend and ScanFlowStore, is designed to help you create and manage Network Scanning templates.

For instructions for this feature, refer to [www.xerox.com/support](http://www.xerox.com/support). In the Search or Choose field, type **Xerox PrimeLink C9065 Printer** or **Xerox PrimeLink C9070 Printer**, then select the desired documentation.

### ENABLING NETWORK SCANNING

To enable network scanning:

1. In the Embedded Web Server, click **Properties > Services > Network Scanning > Scan Template Management**.
2. For Status, select **Enabled**.

### CONFIGURING NETWORK SCANNING

To configure network scanning:

1. In the Embedded Web Server, click **Properties > Services > Network Scanning > General**.
2. For Confirmation Sheet, set the use of confirmation sheets:
  - To disable printing of confirmation sheets, select **Off**.
  - To print a confirmation sheet for every scan, select **On**.
  - To print a confirmation sheet only if an error occurs, select **Errors Only**.
3. For Filename Extension, select an option:
  - **Lower Case**: File name extensions are reflected in lower case letters.
  - **Upper Case**: File name extensions are reflected in upper case letters.
4. If you are using a remote template pool server, for Refresh Start Time, select the time of day from 0:00–23:59, when the template list is refreshed. To refresh the template list, click **Refresh Template List Now**.
5. In the Template Distribution Repositories area, select a Login Source.
6. To add optional information to the job log, if needed, select **User Name**, and **Domain**.
7. Click **Apply**.

## CONFIGURING FILE REPOSITORY SETTINGS

A file repository is a network location where scanned images are stored. Before you can create a template, you must configure the file repository settings.

The device supports the following transfer protocols:

- FTP
- SMB
- HTTP/HTTPS

### FTP

Before you begin:

- Ensure that FTP services are running on the server or computer to be used to store scanned image files. Note the IP address or host name.
- Create a user account and password with read and write access for the device to use to access the repository folder. Note the user name and password.
- Create a folder within the FTP root. Note the directory path, user name, and password. This is your file repository.
- Test the connection. Log into the file repository from a computer with the user name and password. Create a new folder in the directory, then delete it. If you cannot do this, check the user account access rights.

To configure FTP repository settings:

1. In the Embedded Web Server, click **Properties > Services > Network Scanning > File Repository Setup**.
2. To add a file destination, click **Add**. To edit the default file destination, click **Edit**.
3. For Friendly Name, type a name for the repository.
4. For Protocol, select **FTP**.
5. For Host Name / IP Address & Port, type the appropriately formatted address and port number of your FTP server.
6. For File Path, type the directory path of the folder beginning at the root of FTP services. Example:  
/directoryname/foldername.
7. For Login Credentials to Access the Destination, select an option:
  - **Authenticated User and Domain:** The authentication server validates the user credentials, prepended by the domain name, against the LDAP server.
  - **Authenticated User:** The authentication server validates the user credentials against the LDAP server.
  - **Prompt at User Interface:** Users type their credentials at the control panel.
  - **System:** Login name and password credentials are specified in this field and stored in the device. The device uses the system credentials to log into the file server.
8. To configure the system to access the file server directly, type the Login Name and Password.
9. Retype the password.
10. Click **Apply**.

## SMB

Before you begin:

- Ensure that SMB services are running on the server or computer on which you want to store scanned image files. Note the IP address or host name.
- Create a user account and password with read and write access for the device to use for access to the repository folder. Note the user name and password.
- On the SMB server, create a shared folder. This is your file repository. Note the directory path, share name of the folder, and the computer name or server name.
- Test the connection. Log into the file repository from a computer with the user name and password. Create a new folder in the directory, then delete it. If you cannot create a new folder, check the user account access rights.

To configure SMB file repository settings:

1. In the Embedded Web Server, click **Properties > Services > Network Scanning > File Repository Setup**.
2. To add a file destination, click **Add**. To edit the default file destination, click **Edit**.
3. For Friendly Name, type a name for the repository.
4. For Protocol, select **SMB**.
5. For Host Name / IP Address & Port, type the appropriately formatted address and port number for the server on which the file repository is located. The default port number is 139.
6. For Shared Name, type the share name.
7. For File Path, type the directory path of the folder starting at the root of the shared folder. Example: If you have a folder named scans in the shared folder, type `\scans`.
8. For Login Credentials to Access the Destination, select an option:
  - **Authenticated User and Domain:** The authentication server validates the user credentials, prepended by the domain name, against the LDAP server.
  - **Authenticated User:** The authentication server validates the user credentials against the LDAP server.
  - **Prompt at User Interface:** Users type their credentials at the control panel.
  - **System:** Login name and password credentials are specified in this field and stored in the device. The device uses the system credentials to log into the file server.
9. To configure the system to access the file server directly, type the Login Name and Password.
10. Retype the password.
11. Click **Apply**.

## HTTP/HTTPS

Before you begin:

- Enable HTTP or Secure HTTP (SSL). If you are using SSL, ensure that a certificate is installed on the device.
- Configure your web server, and ensure that HTTP/HTTPS services are running. POST requests and scanned data are sent to the server to be processed by a CGI script. Note the IP address or host name of the web server.

- Create a user account and password for the device on the Web server. Note the user name and password.
- Create a home directory for the device.
- Create a bin directory in the home directory
- Copy an executable CGI script in the bin directory. You can create your own script, or download a sample script. Note the path to the script. The script can be defined with `script_name.extension` or by `path/script_name.extension`.
- Create a folder with read and write permissions on the Web server or alternate server. Note the directory path, user name, and password. This is your file repository.
- To test the connection, log in to the device home directory on the Web server. Send a POST request and file to the Web server. Verify that the file is in the repository.

### CGI Scripts

A CGI (Common Gateway Interface) script is a program on a Web server that is executed when the server receives a request from a browser. A CGI script is required to allow files to be transferred to your HTTP server from your device.

When a document is scanned, the device logs into the Web server, sends a POST request along with the scanned file, then logs out. The CGI script handles the remaining details of file transfer.

### Configuring HTTP and HTTPS

To configure HTTP/HTTPS file repository settings:

1. In the Embedded Web Server, click **Properties > Services > Network Scanning > File Repository Setup**.
2. To add a file destination, click **Add**. To edit the default file destination, click **Edit**.
3. For Friendly Name, type a name for the repository.
4. For Protocol, select **HTTP** or **HTTPS**. Secure HTTP (SSL) is used to encrypt HTTP communication between the device and client computers using the Embedded Web Server. This encryption includes data sent using IPSec, SNMP, and Audit Log A.
5. For Host Name / IP Address & Port, type the appropriately formatted address and port number of your HTTP or HTTPS server.
6. If you selected HTTPS, to verify that a digital certificate is installed on the device, click **View Trusted SSL Certificates**.
7. If you selected HTTPS, to have the server SSL certificate validated for the correct host name and checked for a signature of a trusted certificate authority, select **Validate Repository SSL Certificate**.
8. To verify that your proxy settings allow the device to access your Web server, click **View HTTP Proxy Server Settings**.
9. For Script Path and filename (from HTTP root), type the path to the CGI script starting at the root. Example: `/directoryname/foldername`.
10. For File Path, type the directory path of the folder starting at the root. For Web server directories, type in the path starting at the root. Example: `\\directoryname\\foldername`.

11. For Login Credentials to Access the Destination, select an option:
  - **Authenticated User and Domain:** The authentication server validates the user credentials prepended by the domain name against the LDAP server.
  - **Authenticated User:** The authentication server validates the user credentials against the LDAP server.
  - **Prompt at User Interface:** Users type their credentials at the control panel.
  - **System:** Login name and password credentials are specified in this field and stored in the device. The device uses the system credentials to log into the file server.
  - **None:** No credentials are required.
12. If the system accesses the file server directly, for Login Name and Password, type the required information, as needed.
13. Retype the password.
14. Click **Apply**.

## CONFIGURING THE DEFAULT TEMPLATE

Before you can use the Network Scanning feature, create and edit a template. A template contains scan settings and at least one destination for the scanned image files.

All templates are based on the default template. To configure the default template, set up one or more file repositories, then create the default template. After you create the default template, users can create and edit templates from the Scan tab in the Embedded Web Server. A template inherits settings from the default template.



Note: Users and system administrators cannot delete the default template. System administrators can change the template properties.

To configure the default template:

- Add or edit the file destination.
- Add metadata, then configure other options.



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

## Editing File Destination Settings

To edit scan file destinations in the scan template:

1. In the Embedded Web Server, click **Properties > Services > Network Scanning > Default Template**.
2. Select the Filing Policy.
3. Select the File Destination.
4. If required, for Add (Optional), add to the file path.
5. Click **Apply**.

## Adding MetaData Fields

You can add fields to the template to help you manage scanned image files. The fields appear when a user selects the template at the device control panel. The user types information about the document they are scanning. The information is filed with each scanned image file in the Job Log. Third-party software can access the Job Log to retrieve information and associate it with the scanned files.

To add metadata fields:

1. In the Embedded Web Server, click **Properties > Services > Network Scanning > Default Template**.
2. In the MetaData (Optional) area, click **Add**.
3. In the Attributes area, for Name (Required), in the field, type a name. This text is not shown at the control panel. This text is used by third-party software to access the MetaData information. This field cannot be empty.
4. For User Editable, select an option:
  - **Editable:** This option allows users to modify the field. For Label, type a label that identifies the purpose of the field to the user.
  - **Not Editable:** This option prevents users from modifying the field. The field will not display on the control panel and the text typed in the Default Value field is used.
5. If you selected Not Editable, type a Default Value. If you have allowed the user to edit the field, the Default Value is optional.
6. If you selected Editable, to prompt the user to type data for this field before scanning, select **Require User Input**.
7. If you selected Editable, to show the typed characters as asterisks at the control panel, select **Mask User Input (\*\*\*\*)**. To write any masked data to the Job Log file, select **Record User Input to Job Log**. Consider data security issues before selecting this option.
8. If there are validation servers configured for the device, set Validate Data Before Scanning options, as needed.
9. Click **Apply**.

## Configuring Other Default Template Scanning Options

1. In the Embedded Web Server, click **Properties > Services > Network Scanning > Default Template**.
2. To edit the following settings, for a setting, click **Edit**. For descriptions of many of these settings, refer to the *Xerox® PrimeLink™ C9065/C9070 Printer User Guide*.
  - Network Scanning
  - Advanced Settings
  - Layout Adjustment
  - Filing Options
  - Report Options
  - Network Scanning Image Settings
  - Compression Capability
3. To delete any custom settings applied to the Default Template and restore the Default Template to its original settings, click **Apply Factory Default Settings**.

## CONFIGURING TEMPLATE POOL REPOSITORY SETTINGS

If you want to store Network Scanning templates on your network, or if you are using a scanning management application such as SMARTsend®, or ScanFlowStore®, you must provide information about the server that hosts the templates.

1. In the Embedded Web Server, click **Properties > Service > Network Scanning > Advanced > Template Pool Setup**.
2. You can configure your template pool repository to transfer files using FTP, SMB, HTTP, or HTTPS. To configure the settings, follow the instructions for setting up the file repository. For details, refer to [Configuring File Repository Settings](#).



Note: The format for an FTP directory path is /directory/directory; for SMB, the format is \directory\directory.

## UPDATING THE LIST OF TEMPLATES AT THE CONTROL PANEL

If you store templates in a template pool repository on your network, when you make changes to the repository, update the template list that appears at the control panel.

To update the list of templates displayed on the control panel:

1. On the control panel, press the **Services Home** button, then touch the **Network Scanning** icon.
2. Touch **Update Templates**.

## CONFIGURING A VALIDATION SERVER

Scan metadata entered at the device control panel can be verified against a list of valid values by a validation server.

To configure a validation server:

1. In the Embedded Web Server, click **Properties > Services > Network Scanning > Validation Servers**.
2. Click **Add**.
3. Select the appropriate protocol from the drop-down list.
4. For Host Name / IP Address & Port, type the appropriately formatted address and port number of the server. The default port number is 443 for HTTPS.
5. For Path, type the path on the server.



Note: The format for a directory path for FTP is /directory/directory. The format for a directory path for SMB is \directory\directory.

6. Type a **Response Timeout** from 5-100 seconds.
7. Click **Apply**.

## Scanning to a Home Folder for a User

The Scan to Home feature allows users to scan to their home folder, as defined in your LDAP directory, or to a shared folder on the network.

Before you begin:

- Enable and configure Network Scanning.
- Configure Network Authentication. The authentication server and the server to which you are scanning must have the same domain.

To scan to the home folder defined in an LDAP directory:

- Ensure that LDAP server settings are configured.
- Ensure that the home folder location for each user is defined in the LDAP directory.

To scan to a shared folder on the network, create a shared folder on your network with read and write access privileges.

### CONFIGURING SCAN TO HOME

To configure scanning to a user home directory:

1. In the Embedded Web Server, click **Properties > Services > Scan to Home > General**.
2. For Status, click **Enabled**.
3. Type a Friendly Name up to 127 characters in length. The Friendly Name is the default description of the template that appears for users when they perform scans at the control panel.
4. Type a Template Name up to 127 characters. The Template Name is the default name that appears for users when they perform scans at the control panel. If you leave this field blank, the template is named **@S2HOME**.
5. Specify the home directory:
  - To scan to a user home directory as defined in the LDAP directory, for Determine Home Directory, select **LDAP Query**.
  - To scan to a user home directory as defined on a specific computer, for Determine Home Directory, select **NO LDAP Query**. For Network Home Path, type the IP address of the computer.
6. To create a subfolder for the scanned files, select **Automatically Create Subfolder**, then type the Subfolder name.
7. To create a folder for each user in the directory, select **Append "User Name" to Path**.
8. To create a folder for each user in the directory if it does not already exist, select **Automatically Create User Name Folder**.
9. Select a directory structure.
10. Choose the level of login access and control required to access the destination.
11. If required, type the Login Name.
12. Type the Password, then retype the password.
13. Click **Apply**.

## 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 **Properties > Services > Store to USB > General**.
2. For Store to USB, select **Enabled**.
3. Click **Apply**.

## 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, follow the instructions in this order:

- Create a Job Flow Sheet.
- 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 **Scan > Job Flow Sheets**.
2. For Sheet Type, select an option.
3. For Sheet Order, select the order in which you want the sheets to appear.
4. Click **Display Job Flow Sheets List**.
5. Click **Create Job Flow Sheet**.
6. For Job Flow Sheet Name, type a name for the sheet.
7. For Description, type a description for the sheet.
8. For Keyword, type keywords that can help users find the sheet at the control panel.
9. Click **Apply**.

#### Defining Actions for a Job Flow Sheet

To define the actions performed by a Job Flow Sheet:

1. Refresh your browser, then navigate back to the Job Flow Sheets page.
2. Click **Display Job Flow Sheets List**.
3. Select the sheet that you created, then click **Edit Job Flow Sheet**.

4. In the Edit Job Flow Sheet area, for Edit Destination, select an action that you want to take on the documents in your folder. Choose from **Print**, **Send as Fax**, **Send as IP Fax (SIP)**, **Send as Internet Fax**, **Send as Email**, **FTP Transfer**, **SFTP Transfer**, **SMB Transfer**, or **Email Notification**.

5. Click **Edit Job Flow Sheet**.

6. Specify the options for the action that you selected:

- **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.

- **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 IP Fax (SIP):** Type the name and fax number of the recipient.

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.

If you purchased and installed the Thumbnail Preview Kit, you can use thumbnail previews. To use thumbnail previews, for Add Thumbnail, select **Enabled**.

If you purchased and installed the Searchable PDF Kit, you can use compression and searchable text. To use compression and searchable text, for MRC High Compression and Searchable Text, select **Enabled**. Select the settings for each option.

- **FTP Transfer**, **SFTP Transfer**, or **SMB Transfer:** For Name and Server Name, type the required information.

For SMB, type the shared name.

To save the scanned documents to a folder, for Save in, type the directory path of the folder.

Type the login name and password of the folder.

Select the file format.

If you purchased and installed the Thumbnail Preview Kit, you can use thumbnail previews. To use thumbnail previews, for Add Thumbnail, select **Enabled**.

If you purchased and installed the Searchable PDF Kit, you can use compression and searchable text. To use compression and searchable text, for MRC High Compression and Searchable Text, select **Enabled**. Select the settings for each option.

- **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.

7. Click **Apply**.

The Job Flow Sheet contains the action that you specified. To add more actions, repeat this process. Each action that you specify is added to the actions performed on the folder. You can see the actions on the Job Flow Sheet Common Attributes page.

## 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 **Scan > Folder**.
2. For the folder to which you want to create a link, click **Edit**.
3. If available, in the Link Job Flow Sheet to Folder area, for Sheet Type, select the type of Job Flow Sheet to which you want to create a link.

4. Click **Display Job Flow Sheets List**.
5. Select your Job Flow Sheet from the list, then click **Link Job Flow Sheet to Folder**.

## 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 **Properties > Connectivity > Port Settings**.
2. For SNMP, WebDAV, and SOAP, select **Enabled**.
3. Click **Apply**.

You can now install and use the scan utility.



# Faxing

This chapter contains:

- Embedded Fax ..... 146
- Server Fax..... 154
- Internet Fax..... 157
- LAN Fax ..... 160
- Session Initiation Protocol Fax..... 161

## 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](#).
- To send faxes to a network repository, configure the network repositories, then set up a default network location. For information, refer to [Network Scanning](#).
- 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



Note: The Embedded Fax and Server Fax Services cannot be enabled at the same time.

To enable the embedded fax server:

1. In the Embedded Web Server, click **Properties > Services > Fax > Fax Settings**.
2. For Fax Service, select **Scan to Fax**.
3. Click **Apply**.

### CONFIGURING EMBEDDED FAX SETTINGS

To configure embedded fax settings at the device:

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 > Fax Service Settings > Local Terminal Information Settings**.
3. To change a setting:
  - a. Touch a setting, then touch **Change Settings**.
  - b. Touch an option, then touch **Save**.

Use this method to change the following settings, as needed:

- **Local Name:** If needed, type the name of the printer.
- **Fax Name:** If needed, type the name associated with the fax line.

- **Device Password:** If needed, type a password. The password prevents your printer from receiving faxes or from being polled by other devices that are not F-Code compatible.
- **Line 1 - Fax Name:** If needed, type a name for the fax line.
- **G3 Line 1 - Fax ID:** Type the fax number. The fax number is the telephone number of the fax line.
- **G3 Line 1 - Dial Type:** Select the dial type.
- **G3 Line 1 Transmission:** Select **Detect Tone**, or **Do Not Detect Tone**.

## CONFIGURING FAX GENERAL SETTINGS

To configure fax general settings:

1. In the Embedded Web Server, click **Properties > Services > Fax > General**.
2. Click **Edit**.
3. For Transmission Report - Job Undelivered, select **Off** or **Errors Only**.
4. For Filename Format, select a format.
5. For Polling / Storage for Remote Devices, select **Disabled** or **Enabled**.
6. Click **Apply**.

## 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, click **Properties > Services > Fax > Output Destination**.
2. Select **Enabled**.
3. Click **Apply**.

At the control panel, select the output tray for faxes.

## CONFIGURING FAX CONTROL 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 > Fax Service Settings > Fax Control**.

3. Change the following fax settings as needed:

- **Re-enter Recipients:** To require users to type the recipient address twice, ensuring that the fax is sent to the correct address, touch **Enter Twice**.
- **Re-enter Broadcast Recipients:** To allow the broadcast send, touch **Enter Once Only**. To require users to enter the recipient twice before allowing the broadcast send, touch **Enter Twice**.
- **Re-enter Speed Dial Recipients:** To require users to type the speed dial recipient twice, touch **Enter Twice**. To require users to type the fax number or email address after typing the speed dial recipient, touch **Re-enter Fax Number of Email**.
- **Re-enter Group Recipients:** To require users to type the group recipient twice, touch **Enter Twice**.
- **Transmission Header / Cover Page:** Select the information that appears in the transmission header or cover page.
- **Transmission Header Text - Polling:** To attach a transmission header to a polling file, touch **Display Header**.
- **Polled Files - Auto Delete:** To delete polled faxes automatically, touch **Yes**.
- **Polling / Storage for Remote Devices:** To allow remote devices to poll for faxes stored on the printer, touch **Enabled**.
- **Rotate 90 Degrees:** To rotate scanned faxes 90 degrees, touch **Yes**.
- **G3 Sender ID - Fax:** To notify G3-ID to recipients, touch **On**.
- **Save Undelivered Faxes:** To save undelivered faxes, touch **Yes**. You can access saved undelivered faxes on the Job Status screen.
- **Save Deleted Faxes:** To save deleted faxes, touch **Yes**. You can access saved deleted faxes on the Job Status screen.
- **Saved Faxes - Auto Delete:** To delete saved faxes after 24 hours automatically, touch **Delete after 24 Hours**.
- **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, touch **Yes**. This option reduces transmission costs.
- **Manual Send / Receive Default:** To specify the default on-hook manual setting when a fax line is shared with a telephone, touch **Manual Receive** or **Manual Send**.
- **Fax Receiving Mode:** To set the default fax receiving mode that appears when you press the Machine Status button, touch **Auto Receive** or **Manual Receive**.
- **Border Limit:** If a received fax document is longer than a page, specify the border size around the document to force a page break (0-177mm).
- **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, touch **Yes**.
- **Tray for Printing Incoming Faxes:** Select the tray that you want to use for received faxes.
- **2 Pages Up On Receipt:** To print two pages on a single sheet of paper, touch **Yes**.

- **2 Sided Printing:** To print on both sides of a single sheet of paper, touch **Yes**.
- **Edge Erase - Top & Bottom Edges:** Set the top and bottom edge erase margins. Specify a border of 0–20 mm (0–0.8 in.).
- **Edge Erase - Left & Right Edges:** Set the left and right edge erase margins. Specify a border of 0–20 mm (0–0.8 in.).
- **Reduce 8.5 x 11 Original to A4:** To resize letter size documents to A4 when the Reduce/Enlarge setting is set to Auto on the Layout Adjustment screen, touch **Yes**.
- **Pseudo-Photo Gradation Mode:** Touch **Error Diffusion** or **Dither**.
- **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, touch **Enabled**. Locate these folders on a classify received faxes by line type and store them in folders as specified in the Embedded Web Server at **Properties > Services > Fax > Fax Received Options**.
- **Filename Format for Store and Folder:** Select a file format.
- **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. Touch **Delete Job** or **Run Job**.
- **Maximum Stored Pages:** Set the maximum number of pages that can be stored for a fax document.
- **Skip Blank Pages:** To enable the printer to skip blank pages, touch **Enabled**.
- **Fax Data in Folder Priority 1, Fax Data in Folder Priority 2, and Fax Data in Folder Priority 3:** To classify received faxes and store them in folders, select **F Code**, **Remote Terminal ID**, or **Remote Terminal Name**.
- **Direct Fax:** To allow the device to receive a LAN fax sent from a print driver, select **Enabled**. For details about LAN fax, refer to the print driver help.
- **Block Inbound Faxes:** Type up to 50 fax numbers that you want to block.
- **Block Unknown Fax Numbers:** To block unknown fax numbers, touch **Yes**.

## SETTING FAX DEFAULTS

To define defaults for incoming faxes for all users:

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 > Fax Service Settings > Fax Defaults**.
3. Touch a default setting in the list, then touch **Change Settings**.
4. Make the desired changes to the default setting, then touch **Save**.

## 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 **Machine Status** button, then touch the **Tools** tab. For details, refer to [Administrator Access at the Control Panel](#).
2. Touch **System Settings > Fax Service Settings > Reduce/Enlarge Presets**.
3. Choose one of the pre-configured presets or select an item in the list, then touch **Change Settings**.
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.
5. Touch **Save**.

### Original Document Size Defaults

To specify default size settings for received faxes:

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 > Fax Service Settings > Original Size Defaults**.
3. To modify an original document size default setting:
  - a. From the list, touch an original document size item, then touch **Change Settings**.
  - 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 **Save**.

### 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

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, click **Properties > Services > Fax > Fax Received Options**.
2. For Folder Selector Setup, click **Enabled**.
3. Click **Apply**. After the settings are confirmed, navigate back to the Fax Received Options page.
4. In the Folder Selector Setup area, select a fax line, then click **Change Settings**.
5. For Save Incoming Fax in Designated Folder, select **Enabled**.
6. Type the three-digit number for the folder that you have created to receive faxes, then click **Apply**.

After setting up a fax folder, if needed, specify the forwarding destinations for the received faxes stored in the folder.

### Setting Up Fax Forwarding Destinations

To specify fax forwarding destinations for the faxes in a folder:

1. Navigate back to the Fax Received Options page.
2. Select the fax line, click **Change Settings**, then click **File Transfer Settings**.
3. For each destination that you want to configure, select **Enabled**.
4. Click **Next**.

5. Configure the fax forwarding destination:

- **Print:** Select the options as necessary for Paper Supply tray, Output Destination tray, Quantity, and 2 Sided Printing. If other options are available, select them if needed, for example to use staples.

- **Send as Fax:** Type the name and fax phone number of the recipient, then select the starting rate.

For the Folder Number and Folder Passcode fields, type the required information.

If needed, select **Send Relay Broadcast**, or **Print at Relay Station**.

If needed, type the information for Relay Station ID / Broadcast Recipients, F Code, and Password (F Code Communication).

- **Send as Internet Fax:** Type the names and email addresses for each recipient, then select the Internet fax profile. If needed, for Header, select **On**.

- **Send as Email:** Type the names and email addresses for each recipient. For File Format, select the format.

To use thumbnail previews, for Add Thumbnail, select **Enabled**. To use this option, purchase and install the Thumbnail Preview Kit.

If needed, select **MRC High Compression options**. For Searchable Text, enable the options. To use this option, purchase and install the Searchable PDF Kit.

- **FTP Transfer, SFTP Transfer, or SMB Transfer:** For the Name and Server Name fields, type the required information.

For SMB, type the shared name.

To save the faxes to a folder, for Save in, type the directory path of the folder.

For the Login Name and Password of the folder, type the required information.

Select the file format.

If you purchased and installed the Thumbnail Preview Kit, you can use thumbnail previews. To use previews, for Add Thumbnail, select **Enabled**.

If you purchased and installed the Searchable PDF Kit, you can use compression and searchable text. To use compression and searchable text, for MRC High Compression options, and Searchable Text, select **Enabled**. Select the settings for each option.

- **Email Notification:** Type the email addresses of the recipients, then select the options for When to Notify. Type the message to include in the body of the email.

6. If you are sending faxes to more than one destination, to configure the next destination, click **Next**. If you want to edit a setting, click **Previous**. When you have configured the final destination, click **Apply**.

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 [Configuring Embedded Fax Settings](#). 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 **Machine Status** button, then touch the **Tools** tab. For details, refer to [Administrator Access at the Control Panel](#).
2. Touch **System Settings > Fax Service Settings > Fax Received Options**.
3. For Folder Selector by G3 ID, click **Enabled**.
4. Click **Apply**. After the settings are confirmed, navigate back to the Fax Received Options page.
5. In the Folder Selector by G3 ID area, click **Create/Delete**.
6. Type the G3 ID telephone number, and the three-digit folder number of the folder that you created to store the faxes.
  - You can specify the telephone number of a device that sends faxes to your printer.
  - You can use the asterisk wildcard (\*) to receive faxes from a range of telephone numbers.
7. Click **Apply**.

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](#).

## Server Fax

The Server Fax kit allows you to send a fax over a network to a fax server, which then sends the fax to a fax machine over a phone line.

Before you can send a server fax, you must configure a fax filing repository, or filing location. Once configured, the device transfers faxed images to the repository. The fax server retrieves the documents from the repository and transmits them over the telephone network. You can also print a transmission report.

You can set up a repository that uses one of the following protocols:

- FTP
- SMB
- SMTP

### ENABLING SERVER FAX

Before you begin, purchase and install the optional Server Fax Kit.

To enable the Server Fax functionality:

1. In the Embedded Web Server, click **Properties > Services > Fax > Fax Settings**.
2. For Fax Service, select **Scan to Fax Server**.
3. Click **Apply**.

### CONFIGURING A FAX REPOSITORY USING FTP

Before you begin:

- Ensure that FTP services are running on the server or computer where the fax repository resides. Note the IP address or host name.
- Create a user account and password for the device. When the Server Fax feature is used, the device logs in using this account, transfers the file to the server or computer, and logs out. Note the user account and password details.
- Create a directory within the FTP root to be used as a fax repository. Note the directory path.

To configure a fax repository using FTP:

1. In the Embedded Web Server, click **Properties > Services > Fax > Fax Repository Setup**.
2. From the Protocol drop-down menu, select **FTP**.
3. Type the appropriately formatted IP address or host name and port number of the FTP server.
4. For File Path, type the full path to the root location of the fax repository. For example: /(directory name)/(directory name).
5. For Login Credentials to Access the Destination, select an authentication option.
6. For Login Name and Password, type the user account ID and password.
7. Retype the password.

8. Click **Apply**.

## CONFIGURING A FAX REPOSITORY USING SMB

Before you begin:

- Create a shared folder to be used as a fax repository. Note the Share Name of the folder and of the Computer Name or Server Name.
- Create a user account and password for the device with full access rights to the fax repository. Note the user account and password.
- In the Embedded Web Server, click **Properties > Services > Fax > Fax Repository Setup**.

To configure a fax repository using SMB:

1. From the **Protocol** drop-down menu, select **SMB**.
2. Type the appropriately formatted address or host name and, if required, type the port number of the SMB server or workstation on which the fax filing repository is located.
3. For Shared Name, type the share name.
4. Type the File Path, relative to the share, to the fax repository location. For example: if the path is sharename \wc\fax, in the File Path field, type \wc\fax.
5. Type the Login Name and Password.
6. Retype the password.
7. Click **Apply**.

## CONFIGURING A FAX REPOSITORY USING SMTP

To configure a fax repository using SMTP:

1. In the Embedded Web Server, click **Properties > Services > Fax > Fax Repository Setup**.
2. For Protocol, from the drop-down menu, select **SMTP**.
3. In the Domain Name field, type the domain name of your SMTP server.
4. If necessary, for Email Address Display Format, select **add "FAX="**.
5. Click **Apply**.

## SERVER FAX CONFIRMATION REPORT AND JOB LOG

You can configure a confirmation sheet to notify users about the status of a fax transmission.

To configure the server fax confirmation report and job log settings:

1. In the Embedded Web Server, click **Properties > Services > Fax > General**.
2. For Job Log, click **Edit**.

3. For Confirmation Sheet, select an option:
  - To print a confirmation sheet for every transmission, select **On**
  - To print a confirmation sheet only when a fax transmission fails, select **Errors Only**.
4. To display the user name or domain information on the Job Log, for Job Log, select **User Name** or **Domain**.  
The Job Log is filed in the fax repository with the fax job.
5. Click **Apply**.

## 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 **Properties > Services > Internet Fax > General**.
2. Click **Edit**.

3. Change the following settings, as needed:

- To send the Internet fax to an email address using an SMTP server, for Send, select **Via Email Server**. To send to an email address using a fully qualified host name or IP address, select **Via P2P**. Selecting Via 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, for Transmission Header Text - Fax Transfer, select **Enabled**.
- 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, for Auto Printing of Error Notification Mail, select **Enabled**.
- 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 request a read receipt, 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 **Errors Only**. If you do not want a report, select **Off**.

4. Click **Apply**.

## 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 the 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 **Machine Status** button, then touch the **Tools** tab. For details, refer to [Administrator Access at the Control Panel](#).
2. Touch **System Settings > Common Service Settings > Maintenance**.
3. Touch **Software Options**, then touch **Keyboard** on the Software Options dialog.
4. To enable SIP Fax, type the software PIN.
5. Touch **Save**.
6. Follow any prompts that appear on the screen.
7. Touch **Close**.

### ENABLING SIP FAX



Note: Before you begin, purchase and install the SIP Fax Kit.

To enable SIP Fax using the Embedded Web Server:

1. In the Embedded Web Server, click **Properties > Connectivity > Port Settings**.
2. For SIP, select **Enabled**.
3. In the Embedded Web Server, enable TCP/IP (no special settings are required).
4. In the Embedded Web Server, click **Properties > Protocols > SIP**.
5. Type the SIP User ID, which consists of a SIP user name and IP address, such as 1234@192.168.1.1. This ID corresponds to the Fax Number of the device for the G3 FAX. The IP address is that of the SIP server. If there is no SIP server in the environment, use the device IP address.
6. Select the appropriate SIP Transfer Protocol.
7. For Enable SIP Server, select **Yes**.
8. For SIP Server IP Address Resolution, select **DHCP** or **Static**.
9. In the Primary SIP Proxy Server Setup fields, type the required data.
10. In the Primary SIP Registrar Server Setup fields, type the required data.
11. For Domain Filtering, select **Off**, **Allow Domains**, or **Block Domains**.
12. To edit domain filter settings, for Domain Filtering, click **Edit**. Edit the domains as needed, then click **Apply**.
13. Click **Apply**.

## 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 **Properties > 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

You should only change T.38 settings if your network policy does not allow the default settings.

To configure T.38 settings:

1. In the Embedded Web Server, click **Properties > Connectivity > Protocols > T.38**.
2. Select a **T.38 Transport Protocol**.
3. Type the appropriate Port Numbers in the fields provided.
4. Click **Apply**.

## 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 Settings:** Set the appropriate tray for received faxes.
- **Local Terminal Information:** Set the Local Name, Company Logo, G3 SIP Line ID, and other information.

# Accounting

This chapter contains:

Xerox® Standard Accounting .....	164
Local Accounting .....	168
Network Accounting .....	170
Configuring Accounting Login Screen Settings.....	171
Accounting and Billing Device Settings.....	172
Enabling Accounting in Print Drivers .....	173

## Xerox® Standard Accounting

Xerox® Standard Accounting (XSA) 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 XSA 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 XSA is enabled, you cannot enable other accounting modes.

You can create a maximum of:

- 2499 unique XSA user IDs
- 500 General Accounts
- 499 Group Accounts

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



Note: XSA settings and account data are stored in the device. It is recommended that you back up settings using the Cloning feature. If XSA 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](#).

### CONFIGURING XEROX® STANDARD ACCOUNTING

To configure Xerox® Standard Accounting:

1. In the Embedded Web Server, click **Properties > Accounting > Accounting Configuration**.
2. For Accounting Type, select **Xerox Standard Accounting**.
3. For each feature that you want to track, select **Enabled**.
4. Click **Apply**.
5. Click **Reboot Device**. To restart the printer, follow the onscreen instructions.

If you want to use authentication, configure [Local Authentication](#) or [Network Authentication](#).

### CREATING A GROUP ACCOUNT

Before creating new user accounts, create at least one group.

To create a group account:

1. In the Embedded Web Server, click **Properties > Accounting > Xerox Standard Accounting > Group Accounts**.
2. If there are group accounts on the device, click **Add Account**.
3. Type an Account ID using up to 12 digits.

4. Type an Account Name using up to 32 alphanumeric characters.



Note: Ensure that the Account ID and Account Name are unique.

5. Click **Apply**.

## CREATING A USER ACCOUNT AND SETTING USAGE LIMITS

To create a new user account:

1. In the Embedded Web Server, click **Properties > Accounting > Xerox Standard Accounting > Manage Accounting**.
2. Click **Add New User**.
3. Type a User ID and a User Name using up to 32 alphanumeric characters for the new user.



Note: Ensure that each User ID and User Name is unique.

4. For Usage Limits, type the maximum number of impressions or sent images that the user can produce. The maximum number of impressions or images sent is 9,999,999.



Note:

- Cover sheets and banner pages are counted as impressions.
- If the device is set to print a Confirmation Report or an acknowledgement report, the reports are counted toward the limit for the user.

5. In the User Role area, assign the user to a User Role and Authorization Group.
6. Click **Apply**.

## MANAGING GROUP ACCOUNTS

To manage the group accounts on the device:

1. In the Embedded Web Server, click **Properties > Accounting > Xerox Standard Accounting > Group Accounts**.
2. Select a group account, then click **Manage**.
3. In the Account ID area, edit the account details. You can change the account name, and set the group as the default for new users.
4. In the User Access area, select the users for the group.
5. Click **Apply**.

## MAXIMUM USAGE LIMITS

Once a user reaches the maximum usage limit set for the user, the user is no longer able to use that feature until you reset the limit. When the user logs in to the device, the user receives a notification message that the limit for that feature is reached.

If a user exceeds the limit while a job is in process, the device tracks the number of impressions generated over the limit and subtracts the overage from the limit after the limit is reset.

If a user reaches the set limit before a print job completes, an error report prints. The printed error report notifies the user that the limit is reached. The job is deleted from the print queue, and any sheets remaining in the paper path finish printing.

### MANAGING LIMITS FOR INDIVIDUAL USERS

To manage limits for individual users:

1. In the Embedded Web Server, click **Properties > Accounting > Xerox Standard Accounting > Manage Accounts**.
2. Select a user, then click **Limits & Access**.
3. In the Usage Limits area, change user limits if necessary.
4. To reset an impression or image limit, select **Reset**. To reset all limits, click **Reset All**.
5. Change the User Role settings if necessary.
6. To change the group access rights, for Group Account Access, click **Edit**.
7. Click **Apply**.

### MANAGING LIMITS FOR GROUPS

To manage limits for groups:

1. In the Embedded Web Server, click **Properties > Accounting > Xerox Standard Accounting > Group Accounts**.
2. Select a group, then click **View Usage**.
3. To reset an impression or image limit, select **Reset**. To reset all limits, click **Reset All**.
4. Click **Apply**.

### RESETTING USAGE DATA VALUES

To reset usage data values:

1. In the Embedded Web Server, click **Properties > Accounting > Xerox Standard Accounting > Report and Reset**.
2. To reset all usage data to 0, click **Reset Usage Data**.
3. To acknowledge the confirmation message, click **OK**.

### AUTOMATICALLY RESETTING THE ACCOUNTING COUNTERS

You can reset the Xerox Standard Accounting counters automatically, for example, to implement a policy of resetting counters every year.

1. In the Embedded Web Server, click **Properties > Accounting > Xerox Standard Accounting > Report and Reset**.
2. Click **Auto Reset**.

3. To reset the accounting counters automatically, for Auto Reset of Accounting Counter, select **Reset Every Month, Reset Every Quarter, or Reset Every Year**.
4. For Auto Reset Timing of Accounting Counter, from the lists, select the day, month, and time of day for the reset to occur.
5. Click **Apply**.

## RESETTING STANDARD ACCOUNTING TO FACTORY-DEFAULT SETTINGS

To reset Xerox® Standard Accounting settings to factory defaults:



Note: The following steps delete all of the Xerox® Standard Accounting (XSA) accounts on the device.

1. In the Embedded Web Server, click **Properties > Accounting > Xerox Standard Accounting > Report and Reset**.
2. To delete all user, group, and general accounts, click **Reset to Default**.
3. To acknowledge the warning message, click **OK**.

## PRINTING A STANDARD ACCOUNTING REPORT

You can print a report that lists the number of impressions recorded for each user and each account.

To print a report:

1. In the Embedded Web Server, click **Properties > Accounting > Xerox Standard Accounting > Report and Reset**.
2. Click **Generate Report**.
3. Right-click the Download report in .csv format link and save the .csv file to your computer.

## Local Accounting

Local Accounting tracks the number of copy, print, and scan jobs for each user. You can set different user limits for each type of job performed. You can reset limits anytime. When Local Accounting is enabled, before accessing services, users are required to log in to the device. Before printing documents from a computer, users provide their account details in the print driver.

Before you begin:

- Install print drivers on all user computers.
- If you want to use authentication, configure [Local Authentication](#).

### CONFIGURING LOCAL ACCOUNTING

To configure Local Accounting:

1. In the Embedded Web Server, click **Properties > Accounting > Accounting Configuration**.
2. For Accounting Type, select **Local Accounting**.
3. For each feature that you want to track, select **Enabled**.
4. Click **Apply**.
5. Click **Reboot Device**. To restart the device, follow the onscreen instructions.

If you want to use authentication, configure [Local Authentication](#).

### CREATING A USER ACCOUNT AND SETTING USAGE LIMITS

You can add users to the local database on the device, or edit the user information in the database. The database can contain a maximum of 1000 users.

To create a user account:

1. In the Embedded Web Server, click **Properties > Accounting > Accounting Configuration**.
2. Click **Next**.
3. For Account Number, type a number, then click **Edit**.
4. Type the user name and user ID.
5. Set the feature and device access for the user.
6. In the Impressions / Limits area, type the limits for the user.
7. If you have local authentication configured, you can enter authentication information into the User Identification area:
  - In the User Identification area, type, then retype a password for the user. If necessary, type an email address for the user.
  - In the User Role area, select a role for the user. If necessary, assign the user to an authorization group.
8. Click **Apply**.

When you add other users, ensure that you type a unique account number for each user.

## RESETTING LOCAL ACCOUNTING USAGE COUNTERS

To reset local accounting usage counters:

1. In the Embedded Web Server, click **Properties > Accounting > Accounting Configuration**.
2. Click **Next**.
3. For All User Accounts, click **Edit**.
4. To reset the total impression count, select **Reset**.
5. To reset all account limits, select **Reset**.
6. Click **Apply**.

## AUTOMATICALLY RESETTING LOCAL ACCOUNTING USAGE COUNTERS

You can reset the accounting counters automatically, for example, to implement a policy of resetting the counters every year.

To reset the accounting counters:

1. In the Embedded Web Server, click **Properties > Accounting > Accounting Configuration**.
2. Click **Next**.
3. To reset the counters automatically, select **Reset Every Month**, **Reset Every Quarter**, or **Reset Every Year**.
4. Set the date and time for the reset.
5. Click **Apply**.

## Network Accounting

Network Accounting allows you to manage device usage with detailed cost analysis capabilities. Print, Scan, Fax, and Copy jobs are tracked at the device and stored in a job log. All jobs require authentication of User ID and Account ID, which are logged with the job details in the job log. The job log information can be compiled at the accounting server and formatted into reports.

The Network Accounting software can be combined with Xerox® Business Partner Solutions for enhanced functionality and the ability to scale to enterprise accounts.

Before you begin:

- Install and configure Xerox® certified network accounting software on your network. For help, refer to the manufacturer instructions.
- To test communication between the accounting server and the device, open a Web browser, type the IP Address of the device in the address bar, then click **Enter**. The home page of the device Embedded Web Server appears.
- To track print and LAN Fax jobs, install print drivers on all user computers.
- If you require authentication, configure [Local Authentication](#) or [Network Authentication](#).

### ENABLING AND CONFIGURING NETWORK ACCOUNTING

To enable and configure Network Accounting:

1. In the Embedded Web Server, click **Properties > Accounting > Accounting Configuration**.
2. For Accounting Type, select **Network Accounting**.
3. For the features that you want to track, select **Enabled**.
4. To authenticate users at the control panel, for Verify User Details, select **Yes**. To use this setting, configure network authentication.
5. To authenticate users at the control panel for printing, for Verify User Details for Printer Jobs / Direct Fax Jobs, select **Yes**.
6. For Customize User Prompts, select a method for prompting users for their credentials.
7. To track color impressions only, for Color Tracking Only, select **Enabled**.
8. Click **Apply**.
9. Click **Reboot Device**.
10. If necessary, configure Network Authentication.

To use authentication, configure [Local Authentication](#) or [Network Authentication](#).

## Configuring Accounting Login Screen Settings

To configure accounting login settings:

1. In the Embedded Web Server, click **Properties > Accounting > Accounting Login Screen Settings**.
2. For Alternative Name for User ID, type the text that appears on the control panel that prompts the user to provide a user name.
3. For Mask User ID, select an option:
  - To display user ID characters as asterisks on the control panel, select **Hide**.
  - To allow user ID characters to appear on the control panel, select **Show**.
4. If you have configured Network Accounting, for Alternative Name for Account ID, type the text that appears on the control panel that prompts the user to provide a user name.
5. If you have configured Network Accounting, for Mask Account ID, select an option:
  - To allow user ID characters to appear as asterisks on the control panel, select **Hide**.
  - To allow user ID characters to appear on the control panel, select **Show**.
6. Click **Apply**.
7. To restart the device, click **Reboot Device**, then follow the on-screen instructions.

## Accounting and Billing Device Settings

You can connect billing devices to the printer. To configure 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 **Accounting > Accounting / Billing Device 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:

- **Connect with Accounting / Billing Device:** To enable an accounting or billing device that is connected to the device, select **Connected**.
  - **Accounting / Billing Device:** Select the type of device.
  - **Track Copy Jobs:** To track copy pages, select **Track with Accounting / Billing Device**.
  - **Track Print Jobs:** To track print pages, select **Track with Accounting / Billing Device**.
  - **Track Scan Jobs:** To track scanned or faxed pages, select **Track with Accounting / Billing Device**.
  - **Interrupt Mode:** To enable the interrupt mode, select **Enabled**.
  - **Job with Insufficient Credit:** For jobs with insufficient credit, select **Delete Job Immediately**, or **Hold Job**.
  - **Charge Print Jobs:** To track charges by card number, select **Charge by Card Number**.
  - **Track with Cumulative Device:** Select **Track with Accounting Device** or **High Speed Printing**.
  - **Scan Ahead for Copy Job:** To scan ahead for a copy job, select **Enabled**.
4. Touch **Close**.

## Enabling Accounting in Print Drivers

Jobs sent from a computer can be counted only if the accounting functionality is enabled in the print driver. For details on how to enable accounting in the print driver, refer to the print driver help.

### ENABLING ACCOUNTING IN A XEROX VERSION 3 WINDOWS PRINT DRIVER

To enable accounting in Windows print driver:

1. In the Windows Control Panel, locate the printer.
2. Right-click the printer, then select **Printer properties**.
3. Click the **Configuration** tab.
4. In the Bi-Directional Communication area, for Connection, select **Off**. Click **OK**.
5. Reopen the print driver, then navigate back to the Configuration tab.
6. In the Accounting area, for System, select **Local Accounting**, **Xerox Standard Accounting**, or **Xerox Network Accounting**.
7. For Print-Time Prompt, select an option:
  - **Always Prompt**: This option always prompts users to type their User ID and Account ID when they send a job to the printer.
  - **Do Not Prompt**: This option does not prompt users to log in. If you select this option, in the Accounting Codes (Required) window, type the User ID, Account ID, and Passcode as required. Click **OK**.
  - **Only Prompt for Color, Only Prompt for Fax, or Only Prompt for Color or Fax**: Select one of these options to prompt users to log in to the service. The options are available only if the device is configured to provide the services.
8. To show characters as asterisks when an ID is entered, for Mask User ID, Mask Billing ID, and Mask Account ID, select **Enabled**.
9. To show the code that a user entered when prompted for the Account ID, select **Remember Last Entered Codes**.
10. If you are using an auxiliary accounting device such as a badge reader or coin box, for Auxiliary Accounting Interface, select **Enabled**. The Accounting window appears each time a user submits a job.
11. If you want to specify the default User ID and Account ID:
  - a. Click **Accounting Codes**, then click **Setup**.
  - b. In the Accounting Codes (Optional) window, type the User ID, Account ID, and Passcode as required.
  - c. Click **OK**.
12. Click **OK**.

To re-enable the bi-directional communication with the SNMP server, open the print driver, then navigate to the Configuration tab. In the Bi-Directional Communication area, for Connection, select **Automatic (Recommended)**, then click **OK**.

## ENABLING ACCOUNTING IN A XEROX VERSION 4 WINDOWS PRINT DRIVER

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



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

To enable Accounting in the Windows print driver:

1. In the Windows Control Panel, locate the printer.
2. Right-click the printer, then select **Xerox Printer Properties**.
3. Set the bi-directional communication to manual:
  - a. Click the **Communication** tab.
  - b. Click **Bi-Directional Communication**, then select **Manual**.
4. Set the device configuration to manual:
  - a. Click the **Configuration** tab.
  - b. Click **Device Configuration**, then select **Manual**.
5. Click the **Accounting** tab.
6. Click **Accounting System**, then select **Local Accounting**, **Xerox Standard Accounting**, or **Xerox Network Accounting**.
7. For Print-Time Prompt, select an option:
  - **Always Prompt**: This option always prompts users for a User ID and Account ID when they send a job to the device.
  - **Do Not Prompt**: This option does not prompt users to log in. If you select this option, in the Default Accounting Codes (Required) area, type the user ID, account ID, and passcode, as required. Click **OK**.
  - **Only Prompt for Color, Only Prompt for Fax, or Only Prompt for Color or Fax**: Select one of the options to prompt the user to log in to the service. The options are available only if the device is configured to provide the services.
8. To show characters as asterisks when an ID is entered, select **Mask User ID**, **Mask Billing ID**, and **Mask Account ID**.
9. To show the code that the user entered when prompted for the Account ID, select **Remember Last Entered Codes**.
10. If you are using an auxiliary accounting device such as a badge reader or coin box, for Auxiliary Accounting Interface, select **Enabled**. The Accounting window appears each time a user submits a job.
11. If you want to specify the default User ID and Account ID, in the Default Accounting Code (Optional) area, type the user ID, account ID, and passcode, as required.
12. Click **OK**.

To re-enable the bi-directional communication with the SNMP server, open the print driver, then navigate to the Communication tab. Click **Bi-Directional Communication**, then select **Automatic**. To re-enable automatic device configuration, click the **Configuration** tab. Click **Device Configuration**, then select **Automatic**. Click **OK**.

## ENABLING ACCOUNTING IN AN APPLE MACINTOSH PRINT DRIVER

To enable accounting in Macintosh print drivers:

1. Open a document and select **File**, then select **Print**.
2. Select the Xerox device.
3. From the drop-down menu, select **Accounting**.
4. For Accounting System, select **Auditron** (Local Accounting), **Xerox Standard Accounting**, or **Xerox Network Accounting**.
5. To require users to type their User ID and Account ID every time they print, select **Prompt for Every Job**.
6. To show user ID and account ID characters as asterisks, select **Mask User ID** and **Mask Account ID**.
7. To specify the default User ID and Account ID, select **Use Default Accounting Codes**. In the Default User ID and Default Account ID fields, type the appropriate information, then select the default account type.
8. If you are using Xerox Network Accounting with an external accounting device, select **Auxiliary Accounting Interface**.
9. To save your settings, from the Presets menu, select **Save As**.
10. Type a name for the preset.
11. Click **OK**.



Note: Users select this preset each time they print using the print driver.



# Administrator Tools

This chapter contains:

Monitoring Alerts and Status.....	178
Activating a Supplies Plan.....	179
Paper Tray Settings .....	180
SMart eSolutions.....	187
Configuring Stored File Settings.....	193
Retrieving Stored Files.....	194
Setting Default Touch Screen Settings.....	195
Taking the Printer Offline .....	196
Restarting the Device in the Embedded Web Server.....	197
Changing the Power Saver Settings .....	198
View Usage and Billing Information .....	199
Cloning .....	200
Public Address Book.....	201
Font Management Utility .....	204
Customizing Device Contact Information .....	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.

### SETTING UP JOB COMPLETION ALERTS

To set up job completion alerts for email recipients:

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

### SETTING UP DEVICE STATUS ALERTS

To set up device alerts for email recipients:

1. In the Embedded Web Server, click **Properties > General Setup > Alert Notification > Email Notification for Device Status**.
2. For each Recipient's Email Address, from the Send Notice drop-down list, select a notification frequency option.
3. In the Mail Notice Status Settings area, 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 **Apply**.

## 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 **Properties > General Setup > Supplies Plan**.
2. For Supplies Plan, 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 **Machine Status** button, then touch the **Tools** tab. For details, refer to [Administrator Access at the Control Panel](#).
2. Touch **System Settings > Common Service Settings > Paper Tray Settings**.

### SETTING CUSTOM PAPER NAME AND COLOR

From the Paper Tray Settings screen, you can select the Custom Paper Name / 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, 64–105 g/m<sup>2</sup>, 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 the **Custom Paper Name/Color** option.
3. Select the item that you want to rename, then touch **Change Settings**.
4. For Custom Type or Custom Paper Color, type the needed name. To save the name and return to the previous screen, select **Save**.

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.

### 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 the **Paper Tray Attributes on Setup Screen**.
3. Touch **Enabled** or **Disabled**, then touch **Save**.

### 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 **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
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. Touch **Change Setting**.
5. Select a feature.
6. Touch **Save**, then touch **Close**.

## 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**. Refer to [Accessing Paper Tray Settings](#).
2. Touch **Paper Tray Attributes**.
3. Select the tray that you want to change.
4. Touch **Change Settings**.

5. Select the paper type, paper size, and paper color. For Auto Paper, to select the color, use the up or down scroll arrow.
6. Touch **Save**.
7. Touch **Confirm**, then touch **Close**.
8. Touch **Close**.

### 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**. Refer to [Accessing Paper Tray Settings](#).
2. Touch **Paper Tray Attributes**.
3. Select the tray that you want to set up as a dedicated paper tray.
4. Touch **Change Settings**.
5. Select the paper type, paper size, and paper color.
6. Touch **Save**.
7. Select **Dedicated Tray**.
8. Touch **Confirm**, then touch **Close**.
9. Touch **Close**.

### 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**.
4. Touch **Save**.

## 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", 13 x 18", 12.6 x 19.2", 12 x 18", 11 x 17", 11 x 15", 8.5 x 14", 8.5 x 13", 8.5 x 11", 8 x 10", 7.25 x 10.5", 5.5 x 8.5", and 5 x 7"
- Others: SRA3, A4 Oversized, 9 x 11", 215 x 315 mm, 8K, 16K, 100 x 148 mm, 148 x 200 mm, 4 x 6"
- 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**. Refer to [Accessing Paper Tray Settings](#).
2. Touch **Tray 5 - Paper Size Defaults**.
3. Touch a paper size setting, then touch **Change Setting**.
4. Select the paper size that you want. Select from **A/B Series Size**, **Inch Size**, **Others**, or **Custom Size**.
5. Touch **Save > Close**.

## 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 **Customize Paper Supply**.
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.
4. Touch **Save**, then touch **Close**.

## 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**. Refer to [Accessing Paper Tray Settings](#).
2. Touch **Paper Tray Priority**.
3. Touch **Change Settings**.
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. Touch **Save**.
6. After you have set the priority for all trays, touch **Close**.

## 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**. Refer to [Accessing Paper Tray Settings](#).
2. Touch **Auto Tray Switching Control**.
3. To change a setting:
  - a. Touch a setting, then touch **Change Settings**.
  - b. Touch an option, then touch **Save**.

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.

4. Touch **Close**.

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 **Image Quality**.
3. Select the paper type that you want to change.
4. Touch **Change Settings**.

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

5. Select a different setting, then touch **Save > Close**.



Note: For all custom paper types, the options available include **Plain A**, **Plain B**, **Plain C**, and **Plain D** paper.

## 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	<b>0:</b> Software Version lower than 18.13 <b>1:</b> 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: \*3035333451
- Disable: \*3035333450



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](http://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 **Save**.

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 <a href="#">Printing the Configuration Report</a> .		
3	For information on DNS Settings, refer to <a href="#">Configuring TCP/IP Settings in the Embedded Web Server</a> .  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 <a href="#">Proxy Server</a> .		
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 **Properties > General Setup > SMart eSolutions Setup > Communication Status**.
2. Click **Configure**.
3. For SMart eSolutions Enablement, select **Enabled**.
4. In the Communication Setup area, for Daily Transmission Time, enter the time of day for communication transmissions to occur between the device and the communication server.
5. For Payload Type, select an option.
6. Click **Apply**.
7. To test the communication between your device and the Xerox server, click **Test XCDG Connection**.

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

### Setting Up Email Notification

To set up email notifications:

1. In the Embedded Web Server, click **Properties > General Setup > SMart eSolutions Setup > Email Notification**.
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 **Apply**.

## Setting Up Software Updates

To set up software updates:

1. In the Embedded Web Server, click **Properties > General Setup > SMart eSolutions Setup > 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 **Apply**.
5. Click **Apply**.

## Terminating the SMart eSolutions Service

To terminate the service:

1. In the Embedded Web Server, click **Properties > General Setup > SMart eSolutions Setup > Communication Status**.
2. Click **Configure**.
3. For SMart eSolutions Enablement, clear **Enabled**.
4. Type a reason for disabling the service.
5. Select your job type.
6. Click **Apply**.

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

## VIEWING SMART ESOLUTIONS INFORMATION

### Viewing the Communication Status

The SMart eSolutions Communication Status page shows the device serial number, the current device configuration status for SMart eSolutions. The page also shows the date of the last transmission to the Xerox® Communication Server.

To view the page, in the Embedded Web Server, click **Properties > General Setup > SMart eSolutions Setup > Communication Status**.

## Accessing the SMart eSolutions Assistants

The SMart eSolutions assistants show when the device transmitted information to Xerox, and what the device transmitted.

To access the assistants, in the Embedded Web Server, click **Properties > General Setup > SMart eSolutions**, then select an assistant:

- **Meter Assistant:** The Meter Assistant shows the details of dates when the device transmitted billing meter data to Xerox.
- **Supplies Assistant:** The Supplies Assistant shows the details of dates when the device transmitted supplies data to Xerox and which components were requested.
- **Maintenance Assistant:** The Maintenance Assistant shows the details of when data was last transmitted to Xerox. If necessary, you can use a button to transmit data to Xerox immediately. There is a link that you can use to export data to a file.

## 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 **Connections** tab, then click **LAN Settings**.  
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](http://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 **Machine Status** button, then touch the **Tools** tab.
2. Touch **System Settings > Stored File Settings**.
3. To change a setting:
  - a. Touch a setting, then touch **Change Settings**.
  - b. Touch an option or type a value, then touch **Save**.

Use this method to change the following settings:

- **Expiration Date for Files in Folder:** 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 that files are kept before deletion, and the time that they are deleted on the last day.
- **Stored Job Expiration Date:** 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**.
- **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 10–900 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 0–12 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, click **Properties > General Setup > Internet Services Settings**.
2. For Auto Refresh Interval, type an interval. For void, type 0, otherwise specify an interval between 20–600 seconds.
3. If needed, for Retrieve Scanned Files / Files in Folder, select **Retrieve only when proxy is bypassed and HTTP/1.1 is used**.
4. For Name of File(s) When Retrieved From Folder, specify the name for the retrieved file. Select **img File Number**, or **File Name**.
5. Click **Apply**.

## Setting Default Touch Screen Settings

To set the default touch screen settings:

1. At the control panel, press **Machine Status**, then touch the **Tools** tab.
2. To set the control panel default screens and buttons, touch **System Settings > Common Service Settings > Screen / Button Settings**.
3. To change a setting:
  - a. Touch a setting, then touch **Change Settings**.
  - b. Touch an option, then touch **Save**.

Use this method to change the following settings:

- **Screen Default:** Set the screen that appears when the printer is powered on.
  - **Service Screen Default:** Set the screen that appears when the Services button is pressed.
  - **Service 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 **Services 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.
  - **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.
  - **Default Keyboard Layout:** Set the keyboard layout.
  - **Screen Brightness:** Adjust the brightness of the screen.
  - **Reconfirm Email Recipient:** If you do not want users to reconfirm email recipients, touch **Confirmation Not Required**. 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**.
  - **Customize Keyboard Button:** Customize the touch screen keyboard button in the lower-right corner. The default text is . com.
  - **Screen After Inserting USB:** Select the screen that appears when a user inserts a USB drive in the Xerox device.
  - **Display Consumables Screen:** Select when the consumables screen is displayed.
  - **Keyboard Input Restriction:** Set the restriction to **Off**, or **On (ASCII Only)**.
  - **Operation of Up / Down Buttons:** Enable or disable fast scrolling.
4. Touch **Save**.

## 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 **Machine Status** button.
2. Touch **Device Information > Others > Print Mode**.
3. Touch **Off-line**.
4. Touch **Close**.

## Restarting the Device in the Embedded Web Server

To restart the device using the Embedded Web Server:

1. In the Embedded Web Server, click the **Status** tab.
2. At the bottom of the General page, click **Reboot Device**, then click **OK**.



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 **Properties > General Setup > Power Saver Settings**.
2. For Time to Low Power Mode, type a time between 1–120 minutes.
3. For Time to Sleep Mode, type a time between 1–120 minutes.
4. To schedule a power-off time, for Scheduled Power Off, select **Enabled**, then type the time for the power off.
5. For Sleep Mode Settings, select **Prioritize Power Saver**, or **Prioritize Wake Up Time**.
6. Click **Apply**.

## 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 **Status > Billing and Counters > Billing Information**.

The list of pages printed or generated by device appears.

2. To update the page, click **Refresh**.

### 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 **Status > Billing and Counters > Usage Counters**. A detailed list of pages printed or generated by the device appears.
2. To update the information, click **Refresh**.

### 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 × 432 mm (11 × 17 in.). With BIM enabled, oversized prints are counted as two Letter prints that measure 215.9 × 279.4 mm (8.5 × 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 **Properties > General Setup > Billing Impression Mode**.
2. Type the PIN activation code.
3. Click **Apply**.

## Cloning

This feature allows you to save your device settings in a clone file. You can use the clone file to copy your device settings to another device, or use it to back up and restore settings on your own device.



Note: If you are using the clone file to copy your device settings to another device, both devices must be the same model and have the same software.

To determine the software version of your device:

1. In the Embedded Web Server, click **Properties > General Setup > Configuration**.
2. Scroll down to the **Software** section.

### SAVING DEVICE SETTINGS

To save device settings to a clone file:

1. In the Embedded Web Server, click **Properties > General Setup > Cloning**.
2. In the Create Clone File area, select feature settings, as needed. By default, all features are selected.
3. To view the specific parameters that can be cloned for any of the features, click **View Feature Details**.
4. Click **Clone**. The Cloning page displays.
5. On the Cloning page, in the Create Clone File area, right-click **Cloning.dat** and save the file to your computer.



Note: The default name for the file is **Cloning.dat**. If you rename the file, use **.dat** as the file extension.

### INSTALLING A CLONE FILE



Note: This procedure causes the device to restart. During this time, the device is inaccessible via the network for several minutes.

To install a clone file:

1. In the Embedded Web Server, click **Properties > General Setup > Cloning**.
2. In the Install Clone File area, click **Browse**, then navigate to your clone file.
3. Select the file, then click **Open**.
4. Click **Install**, then click **OK**.

## 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 Management area, click **Download Template**.
3. Click **Download in CSV format**.
4. To save the file to your computer, follow the on-screen instructions.

### 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 Management area, click **Export Template with Column Headings only**.
3. Click **Download in CSV format**.
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 Management area, click **Import**.
3. To import a new address book file, in the Import Your 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. For Common Tasks, click **Add New Name**.
3. Edit the fields in the Common Settings area. To provide more detailed information for an option, click **Details**.
4. Click **Save & Close**.

#### 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, click **Edit**.
3. Edit the fields in the Common Settings area. To provide more detailed information for an option, click **Details**.
4. Click **Save & Close**.

### 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 **OK**.

### 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 Management area, click **Delete All Names**.
3. To confirm the deletion, click **OK**.

### 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**.
2. In the Management area, click **Import Data**.
3. To import a new address book file, for Address Book File, click **Browse**.
4. Select the CSV file, then click **Open**.
5. 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 Management area, click **Export Data**.
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](http://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 the **Support** tab.
2. Click **Change Settings**.
3. Update the fields as needed, then click **Apply**.

## 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 **Properties > General Setup > Configuration**.
2. To verify the software version, scroll down to the Software area.

### UPDATING THE SOFTWARE

1. In the Embedded Web Server, click **Properties > Services > Device Software > Upgrades**.
2. For Upgrades, select **Enabled**.
3. Click **Apply**.
4. Refresh your browser and navigate to **Properties > Services > Device Software > Manual Upgrade**.
5. In the Manual Upgrade area, click **Browse** or **Choose File**. Locate and select the software upgrade file with the **.bin** format.
6. Click **Open**.
7. Click **Install Software**. The file is sent to the device. After the software is installed, the device restarts.
8. To verify that the software version has updated, 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 **Machine Status** button, then touch the **Tools** tab.
2. Touch **System Settings > Common Service Settings > Device Clock/Timers**.
3. To change a setting:
  - a. Touch a setting, then touch **Change Settings**.
  - b. Select an option, then touch **Save**.

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.
- **Connection 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**.
- **Auto Print:** 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.

## Fax Speed Dial Setup Settings

To set up and administer the Fax Speed Dial feature:

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 **Setup & Calibration > Setup > Add Address Book Entry**.
3. From the Speed Dial Recipient list, select the first available entry.
4. From the Items list, touch **Address Type**.
5. Touch **Fax**.
6. Touch **Save**.
7. For each of the other items in the Items list, select the item, type the required information, then select **Save**.
8. Touch **Close**.

## 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 **Properties > Security > Watermark > Watermark**.
2. In the Watermark area, specify the date format and watermark appearance.
3. In the Force Watermark area, for the jobs that require a watermark on the output, select **On**.
4. Click **Apply**.

### CREATING A UNIVERSAL UNIQUE ID

To print the Universal Unique ID number in the watermark:

1. In the Embedded Web Server, click **Properties > Security > Watermark > Universal Unique ID**.
2. For Print Universal Unique ID, select **Yes**.
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 **Apply**.

### 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 **Properties > Security > Force Annotation > Create Text String**.
2. Type up to eight annotation text strings with a maximum of 64 characters each.
3. Click **Apply**.

#### Applying Layouts to Text Strings

To apply a template to an annotation text string:

1. In the Embedded Web Server, click **Properties > Security > Force Annotation > Apply Layout Template to Copy/Print Jobs**.
2. To apply the template to the annotation text string for one of the available types of jobs, click **Change Settings**.
3. To apply the layout template, for Apply Layout Template, select **Enabled**.
4. In the Layout Template List area, select one of the preset templates.
5. Click **Apply**.

### **Deleting Layout Templates**

To delete layout templates:

1. In the Embedded Web Server, click **Properties > Security > Force Annotation > Delete Layout Template**.
2. In the Layout Template List area, select the templates that you want to delete.
3. Click **Delete Selected Layout Template(s)**.

## 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 **Properties > General Setup > Memory Settings**.
2. In the Memory Settings area, specify memory allocation and spooling behavior.
3. Click **Apply**.

## 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 **Properties > General Setup > Backup and Restore**.
2. For Backup, click **Start**.

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 **Properties > General Setup > Backup and Restore**.
2. For Restore, click **Start**.
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 **Properties > General Setup > Job Management > 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 **Export file in .csv format**.
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 **Properties > General Setup > Job Management > Auto Job Promotion**.
2. For Automatically Delete Held Jobs, select **Enabled**.
3. For Period before Automatic Deletion, type the hours and minutes for the deletion time.
4. Click **Apply**.

### LOCKING THE PRINTER

To lock the printer and make it unavailable for use:

1. In the Embedded Web Server, click **Properties > General Setup > Job Management > Printer Lockout**.
2. For Printer Lockout, select **Enabled**.
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 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 **Apply**.



# Image Quality and Registration

This chapter contains:

- Image Quality and Calibration ..... 216
- Image Registration Adjustments..... 220
- Simple Image Quality Adjustment (SIQA) Tools..... 225

## 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 **Common Service Setting > Image Quality Adjustment > Image Quality**.
3. To set image quality for a feature, select a feature:

FEATURE	DEFAULT SETTING
<b>Photo and text Recognition:</b> 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 <b>Photo and Text for Original Type</b> on the Image Quality screen. Select a sensitivity option: <ul style="list-style-type: none"> <li>• <b>More Text:</b> This option allows the device to recognize very fine print as text.</li> <li>• <b>More Photo:</b> This option allows the device to recognize halftone images from newspapers and advertisements as photos.</li> </ul>	Normal
<b>Output Color Recognition:</b> 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 <b>Auto Detect</b> for Output Color on the Copy screen. <ul style="list-style-type: none"> <li>• <b>More Black and White:</b> This option allows the device to recognize monochrome documents easily.</li> <li>• <b>More Color:</b> This option allows the device to recognize color documents easily.</li> </ul>	Normal
<b>Photo Reproduction level:</b> 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. <ul style="list-style-type: none"> <li>• <b>More Text:</b> This option yields a bold copy effect, which emphasizes the dense parts of an image.</li> <li>• <b>More Photo:</b> This option softens the image gradation of an image, which enhances the reproducibility of subtle colors.</li> </ul>	Normal
<b>Background Suppression (color copy):</b> 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. <ul style="list-style-type: none"> <li>• <b>High Speed:</b> This option allows the device to detect the background color on a pre-scanned sample section of the document.</li> </ul>	High Quality

FEATURE	DEFAULT SETTING
<ul style="list-style-type: none"> <li>• <b>High Quality:</b> This option allows the device to detect the background color on a pre-scanned image of the entire document.</li> </ul>	
<p><b>Background Suppression (BIW copy):</b> 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.</p> <ul style="list-style-type: none"> <li>• <b>High Speed:</b> This option allows the device to detect the background color on a pre-scanned sample section of the document.</li> <li>• <b>High Quality:</b> This option allows the device to detect the background color on a pre-scanned image of the entire document.</li> </ul> <p> 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.</p>	High Quality
<p><b>Background Suppression (scan jobs):</b> This feature sets the method of background High Quality suppression for scan operations. Select an option for density detection and background color deletion.</p>	High Quality
<p><b>Image Enhancement:</b> When enabled, this feature gives the printed image a smoother appearance.</p>	On

4. Touch **Change Settings**.
5. Select an option.
6. Touch **Save**.
7. Touch **Close**.

## 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.

When color gradation of a printed image shifts, to calibrate the color of the image and to maintain quality of the output at a certain level, you can use the Calibration feature at the control panel.

To calibrate image color:

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. Select **Common Service Settings > Image Quality Adjustment > 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. Load A3, A4, 11" x 17" or 8.5" x 11" paper, then for Paper Supply, select an option.

5. To print the calibration chart for the color correction, on the screen, select **Start**.
6. Continue following the steps on the control panel.
7. To perform calibration, place the calibration chart face down with both magenta patches against the left edge of the document glass.
8. To prevent light from bleeding through the sheet, place 5 or more sheets of blank white paper over the chart.
9. Lower the document glass, then on the screen, select **Start**.
10. Select **Confirm**.
11. Select **Target**, then select a job type to be impacted by the calibration: **Copy and Print Jobs**, **Copy Jobs Only**, **Print Jobs Only**, or **None**.
12. Touch **Save**.
13. Continue calibrating another screen type or touch **Close**.

## TWO-SIDED COLOR SCANNING CALIBRATION

### Calibrating Two-Sided Color Scanning

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. Select **System Settings > Common Service Settings > Image Quality Adjustment > 2 Sided Color Scanning Calibration**.
3. Touch **Print Chart**, select a Paper Supply tray, then touch **Save**.
4. Press **Start**.  
The Calibration Chart prints.
5. Follow the on-screen directions.
6. Touch **Confirm**.
7. Touch **Close**.

### Restoring Previous 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. Select **Common Service Settings > Image Quality Adjustment > 2 Sided Color Scanning Calibration**.
3. Touch **Restore Previous Values**, then touch **Start**.
4. Touch **Close**.

### 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**.

## 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.
- To view the effect the settings will have on the image, select an adjustment, then select **Change Settings**.

### 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 **Machine Status** button, then touch the **Tools** tab. For details, refer to [Administrator Access at the Control Panel](#).
2. Touch **System Settings > Common Service Settings > Maintenance Settings**.
3. To scroll down and select **Alignment Adjustment**, touch the arrows.
4. Select **Alignment Adjustment Type Setup**, then press **Change Settings**.
5. Select **Type**.
6. To assign a type name, touch **Change Settings**.
7. Press **Save**.



Note: To identify the paper type in the tray, use a name such as A4 Plain.

8. Press **Sample Printout**.

9. Select the paper tray from which you are printing, then select 1-Sided. Using the Number of Sheets option, run at least 3 sheets.
10. 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.

11. Make adjustments to the image in the following order: Perpendicular, Skew, Magnification, Print Position.
12. Select **Save**.
13. Repeat steps 9 – 11 until Side 1 reaches the desired state.
14. Select 2-Sided print and align Side 2 to match Side 1.



Note: To help you match the images on both sides, you can hold the sheet up to a light source, which can help you see through the sheet.

15. After you finish making adjustments, to print another output sample, press **Sample Printout**, then verify the adjustment results.
16. Make adjustments again as needed.
17. Press **Close**.
18. To assign the set type, select the tray, then press **Change Settings**.
19. Select the adjusted type, then press **Save**.

## 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, press the **Machine Status** button, then touch the **Tools** tab. For details, refer to [Administrator Access at the Control Panel](#).
3. Touch **System Settings > Common Service Settings > Maintenance Settings**.
4. Touch **Finisher Adjustment**.
5. Touch **Adjust Fold Position**.
6. Touch **Fold Position Type Setup**, then press **Change Settings**.
7. Select the paper fold position type you want to set or adjust, then press **Change Settings**.
8. Touch **Name**, then press **Change Settings**.

9. Type a type name, then press **Save**.



Note: Use a name that identifies the fold type, such as Single Fold Plain.

10. Select the fold type, then press **Change Settings**.



Note: For details on making each fold adjustment, refer to the on-screen instructions.

11. Select the desired settings, then press **Sample Printout**.
12. Select the tray, then press the **Start** button.
13. Measure the fold position via the output sample and adjust the fold position accordingly.
14. Make adjustments to the items as needed.
15. After you finish making adjustments, print another output sample with **Sample Printout** and check the adjustment results.
16. Press **Save**.
17. Make adjustments accordingly. If necessary, repeat Steps 11 - 13.
18. Press **Close** until the **Adjust Fold Position** screen appears.
19. To assign the set type (the tray in which you loaded the paper in Step 1), select the tray, then press **Change Settings**.
20. Select the adjusted fold position type, then press **Save**.

### Single Fold Position Adjustment

To adjust single fold settings:

1. Select **Single Fold**, then press **Change Settings**.
2. Specify **Sheets to be folded**, then press **Sample Printout**.
3. Select the tray, then press the **Start** button.
4. Press **Close**.
5. Check the output sample printout and measure the offset amount.
6. Select **Long at Left** or **Long at Right**.
7. 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.
8. Press **Adjust**.
9. To check the adjustment result, press **Sample Printout** again, then check the result in the output sample printout.
10. Make adjustments again, as needed.
11. Press **Save**.

### Booklet Position Adjustment

To adjust booklet fold positioning:

1. Select **Booklet**, then press **Change Settings**.
2. Press **Sample Printout**.
3. Select the tray, select **2-Sheet Stack**, then press the **Start** button. An output sample prints.
4. Select the tray, select **15-Sheet Stack**, then press the **Start** button.
5. Press **Close**.
6. Check the output sample, then measure the position offset amount for 2-sheet stack and 15-sheet stack.
7. Press **Booklet Fold State (2 Sheets)**.
8. For **Values A**, select the state of the fold and staple position of the output paper, then type the 2-sheet stack offset amount you measured previously.
9. Press **Save**.



Note:

- The values between 2-sheet stack and 15-sheet stack are adjusted automatically.
  - To specify the number of sheets separately, use the Set Variable-Sheet Booklet option and make selections as needed.
10. To print an output sample and check the adjustment results, press **Sample Printout** again.
  11. Make adjustments again, as needed.
  12. Press **Save**.

### C Fold Position Adjustment

To adjust the C fold position:

1. Select **C Fold-A4** or **C Fold-8.5x11**, then press **Change Settings**.
2. Press **Sample Printout**.
3. Select the tray, then press the **Start** button.
4. Press **Close**.
5. Check the output sample, then measure the A and B fold position movement amounts.
6. 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.

7. To print an output sample and check the adjustment results, press **Sample Printout** again.
8. Make adjustments again, as needed.
9. Press **Save**.

### Z Fold Position Adjustment

To adjust the Z fold position:

1. Select **Z Fold-A4** or **Z Fold-8.5x11** and press **Change Settings**.

2. Press **Sample Printout**.
3. Select the tray and press the **Start** button.
4. Press **Save**.
5. Check the output sample, and measure the A and B fold position movement amounts.
6. Enter the measurement value you obtained in the previous step in **Values A**.



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.

7. Press **Sample Printout** again, then check the adjustment result on the output sample printout.
8. Make adjustments again, as needed.
9. Press **Save**.

### **Z Fold Half Sheet Position Adjustment**

To adjust Z-fold positioning:

1. Select **Z Fold Half Sheet-A3**, **Z Fold Half Sheet-B4**, **Z Fold Half Sheet-11x17**, or **Z Fold Half Sheet -8K**, then press **Change Settings**.
2. Press **Sample Printout**.
3. Select the tray, then press the **Start** button.
4. Press **Save**.
5. Check the output sample and measure the A and B fold position movement amounts.
6. For Values A, enter the measurement value that you obtained in the previous step.



Note: Set 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.

7. Press **Sample Printout** again, then check the adjustment result on the output sample printout.
8. Make adjustments again, as needed.
9. Press **Save**.

## 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:

- **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.
- **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.
- **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.

Device calibration with the SIQA tools consists of the following sets of steps:

1. Print the SIQA targets.
2. Scan the targets using the Document Feeder or the Platen Glass.
3. Save the adjustment data to a file on the device and give the file a unique name.

After the adjustment profile is complete, users can select the profile for print runs, as needed.

### ACCESSING THE SIQA TOOLS

To access the SIQA tools:

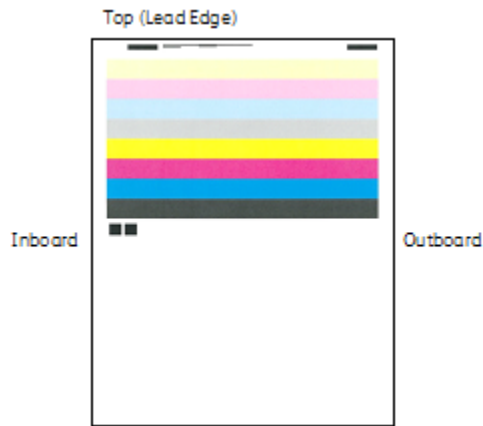
1. At the device control panel, log in as Administrator, press the **Machine Status** button, then touch the **Tools** tab. For details, refer to [Administrator Access at the Control Panel](#).
2. In the Features column, scroll down and touch **Maintenance**.
3. To access the SIQA tools on the next screen, touch the down arrow.

### Image Orientation Definitions

Inboard and outboard are as follows:

- On the device, **inboard** and **outboard** are defined as follows:

- **Inboard:** This term refers to the rear of the device, which is the side of the device that is farthest from you as you are using the device.
- **Outboard:** This term refers to the front of the device, which is the side of the device that is nearest to you as you are using the device.
- On the printed output, as you hold the sheet with the top facing up, **inboard** refers to the left side of the sheet and **outboard** refers to the right side of the sheet. The short black line indicates the top of the sheet. The top of the sheet is also referred to as the lead edge.



## IMAGE TRANSFER ADJUSTMENT

The purpose of the Image Transfer Adjustment is to correct for mottle (uneven toner coverage) and color shift (inconsistent color). These image quality issues may occur on heavy-weight stocks. The Image Transfer Adjustment applies only to the media type selected during the procedure. You must perform this adjustment for each media type loaded in the device.



Note: It is important to perform Image Transfer Adjustment before performing Auto Alignment Adjustment or Density Uniformity Adjustment.

### Adjust Image Transfer

The Image Transfer Adjustment applies only to the paper type selected during the procedure. You must perform this adjustment for each paper type loaded in the device.

To perform a Simple Image Quality Adjustment (SIQA) for image transfer:


1. At the device control panel, log in as Administrator. Refer to [Administrator Access at the Control Panel](#).
2. Access the SIQA tools screen. Refer to [Accessing the SIQA Tools](#).
3. Touch **Adjust Image Transfer**.
4. Touch **Paper Type**, then select a paper type from the list.
5. Touch **Close**.

6. Load the selected paper type into Tray 5 (bypass).  
Acceptable paper sizes:
  - 11 x 17 in.
  - 8.5 x 11 in.
  - A3
  - A4
  - SRA3
7. Touch **Print Sample**.
8. Select a paper size.
9. Select **1 Sided** or **2 Sided** for the calibration chart.
10. To print the calibration chart, on the control panel, press the **Start** button.

IMAGE SAMPLES



11. Touch **Confirm**.
12. Touch **Close**.
13. Touch **Scan Calibration Chart**.
 

 Note: If you printed a 2-sided sample, scan both sides.
14. To complete the calibration, follow the instructions on the control panel touch screen.
15. To exit the scan, touch **Confirm**.
16. View the adjustment numbers for Side 1 and Side 2.
17. To complete and save the calibration, touch **Adjust**.
18. To exit the SIQA tool, touch **Close**, then touch **Close** again.
19. To log out of Administrator mode, on the top right corner of the screen, select the **Admin** icon, then touch **Logout**.

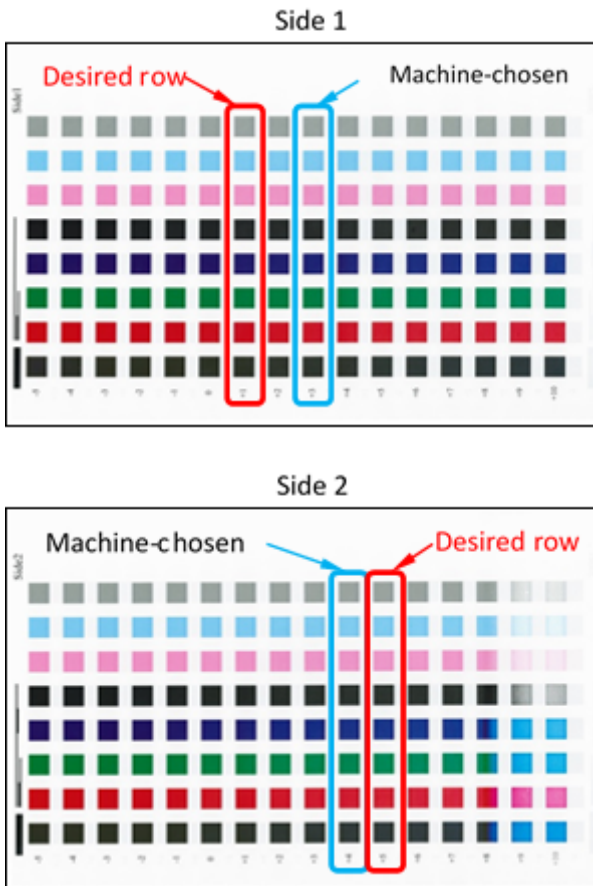
### Adjust Image Transfer Manually

If you are not satisfied with the results achieved after completing the Image Transfer Adjustment procedure, you can run the calibration again using a different row of squares on the calibration chart. You can also change the adjustment values directly.

1. Select the row of transfer samples that you wish to use for the calibration.



Note: The key to choosing the best row of samples is to select a row with the fewest white spots in each square.



2. Type the number that represents the desired sample row. The number for the row appears next to the row on the side of the sheet.

Using the image above as an example, for Side 1 type **1** and for Side 2, type **5**

3. To save the values for image adjustment, touch **Adjust**.
4. To exit the SIQA tool, touch **Close**, then touch **Close** again.
5. Touch **Close**.
6. To log out of Administrator mode, touch the **Admin** icon on the top right corner of the screen, then touch **Logout**.

## AUTO ALIGNMENT ADJUSTMENT

The Auto Alignment procedure generates an individual alignment profile, or Type, for each stock/tray combination selected when performing the procedure. These Types ensure that images are placed correctly on the media. You can create up to 50 Types. Each time a stock is used, the Type associated with the stock/tray will be used automatically, ensuring optimal print quality.

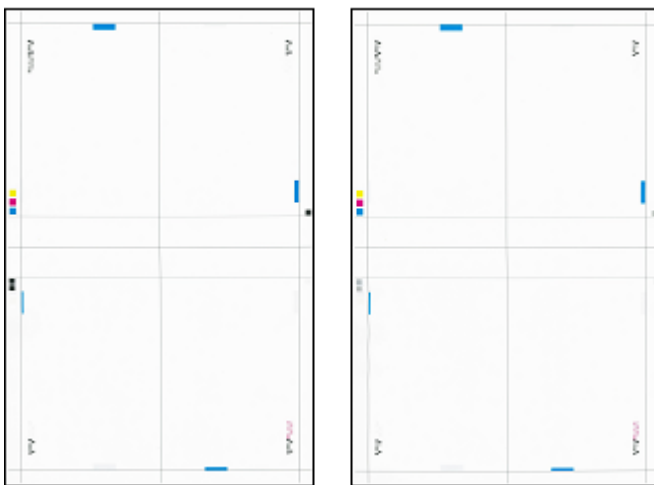


Note: Before you can perform Auto Alignment Adjustment, you must perform Image Transfer Adjustment. For details, refer to [Adjust Image Transfer](#).

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/PLC9065\\_PLC9070docs](http://www.xerox.com/office/PLC9065_PLC9070docs) in the documentation for the Xerox® PrimeLink™ C9065/C9070 Printer.
  - 11 x 17 in.: **SIQA Black Paper for Adjustment-Tabloid.pdf**
  - A3: **SIQA Black Paper for Adjustment-A3.pdf**
2. At the device control panel, log in as Administrator, then access the SIQA Tools. For details, refer to [Accessing the SIQA Tools](#).
3. Touch **Alignment Adjustment**.
4. Touch **Auto Alignment Adjustment**.
5. Touch **Print Calibration Chart**.
6. Select a paper tray with 11 x 17 in. or A3 size paper.
7. For Coverage 1 and Coverage 2, set the value to **1**.
8. To print the calibration chart, touch **Print**.

IMAGE SAMPLES



9. Touch **Confirm**.
10. Touch **Document Feeder Scan Precision Adjustment**.
11. To complete the scan using the Document Feeder and Document Glass, follow the instructions on the control panel touch screen.
  - a. Position the Black Paper and Calibration Chart as shown on the Black Paper.

- b. Reposition the Calibration Chart as indicated on the control panel touch screen and on the Black Paper, then for each scan, touch **Scan**.
  - c. After you have completed all scans, touch **Start**.
12. Touch **Confirm**.
13. Touch **Print Calibration Chart**.
14. Select a paper tray with the correct paper size.
15. For Coverage 1 and Coverage 2, select a coverage value. Use the table below as a guide.


**Table 11.1 Area Coverage 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

16. Touch **Print**.
17. Touch **Confirm**.
18. Select a scan method:
  - Touch **Scan Chart with Document Feeder**: Select this option for a target media size of 11 x 17 in. / A3 or smaller and less than 220 gsm. Accuracy is within 0.2 mm.
  - Touch **Scan Chart with Document Glass**: Select this option for a target media size of larger than 11 x 17 in. / A3 and more than 220 gsm. Accuracy is within 0.1 mm.
19. To complete the adjustment, touch **Start**.
20. Touch the tray name that displays on the control panel touch screen. This is the paper tray to which the alignment adjustment is applied.
21. In the Items area, select a type.
22. Touch **Change Settings**.

 Note: Selecting **Save** overwrites the existing settings.

23. In the Items area, select **1. Name**.
24. To name the Type, touch **Change Settings**.

 Note: Use a name that identifies the paper type that is loaded in the tray.

25. To save the settings, touch **Save** four times.
26. To log out of administrator mode, select the **Admin** icon on the top right corner of the screen, then touch **Logout**.

## Setting the Type when Loading Media

Each time you load media, you must associate the paper type with the tray.

To associate the correct Type with the loaded media:

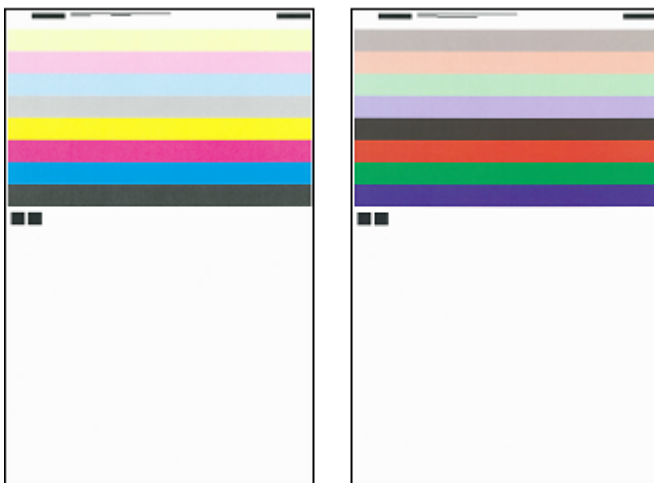
1. At the device control panel, log in as Administrator. Refer to [Administrator Access at the Control Panel](#).
2. Access the SIQA tools screen. Refer to [Accessing the SIQA Tools](#).
3. Touch **Alignment Adjustment**.
4. Touch **Manual Alignment Adjustment**.
5. Select the paper tray just loaded.
6. Touch **Change Settings**.
7. Touch the desired Type.
8. Touch **Save**.
9. To save the settings and exit the SIQA tool, touch **Close** three times.
10. To log out of Administrator mode, on the top right corner of the screen, select the **Admin** icon, then touch **Logout**.

## DENSITY UNIFORMITY ADJUSTMENT

To perform the Density Uniformity Adjustment:

1. At the device control panel, log in as Administrator. Refer to [Administrator Access at the Control Panel](#).
2. Access the SIQA tools screen. Refer to [Accessing the SIQA Tools](#).
3. Touch **Density Uniformity Adjustment**.
4. Touch **Semi Auto Process Using Scanner**.
5. Touch **Print Calibration Chart**.
6. Touch **Print** and follow the instructions on the control panel touch screen to print the two charts.

IMAGE SAMPLES



7. Touch **Confirm**.

8. Touch **Scan Calibration Chart**.
9. Using the instructions on the control panel touch screen, scan the two calibration charts.
10. To begin the density uniformity adjustment, touch **Start**.
11. When the adjustment completes, touch **Confirm**.
12. To save the adjustment, touch **Save**.
13. To exit the SIQA tool, touch **Close** three times.
14. To log out of Administrator mode, on the top right corner of the screen, select the **Admin** icon, then touch **Logout**.

# Customization and Expansion

This chapter contains:

- Xerox® Extensible Interface Platform® ..... 234
- Customizing Apps on the Printer ..... 236
- Setting Up Stored Programming ..... 237
- Plug-ins and Kits ..... 238
- Setting Up the Inserter Module ..... 240

## 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](http://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 **Properties > General Setup > Extensible Service Setup**.
2. For Extensible Services Registration, click **Edit**.
3. Select the remote system management, apps, hardware, authentication and accounting, and security that you want to enable. Click **Apply**.
4. In the Enable Extensible Services area, 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**.
5. If necessary, in the Browser Settings area, select **Enable the Extensible Services Browser**.
6. If necessary, select **Verify server certificates**.
7. For 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, click **Edit**. To specify the trusted domains, use a comma-separated list. Click **Apply**.
8. To configure proxy settings, in the Proxy Server area, select **Use Proxy Server**, then click **Configure**.

- a. 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 **Apply**.
9. Click **Apply**.

## 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 pre-installed 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 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](http://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](http://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 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 **Properties > Services > Apps**.
2. To show or hide an app on the control panel:
  - a. For the app that you want to show or hide, click **Edit**.
  - b. Click **Show** or **Hide**.
  - c. Click **Apply**.

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 **Edit**.
  - b. Click **Delete**.

You cannot delete standard apps. You can delete apps that you have installed on the printer.

## Setting Up Stored Programming

Stored programming allows users to store the settings of a commonly used job. 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 STORED PROGRAMMING

To add the Stored Programming feature to the Services Home menu:

1. At the control panel, press the **Machine Status** button, then touch the **Tools** tab.
2. Touch **System Settings > Common Services Settings**.
3. Touch **Screen/Button Settings**.
4. Touch **Services Home**, then touch **Change Settings**.
5. Touch **Add**, scroll to Stored Programming, then select **Save**.

### SETTING THE AUDIO TONES FOR STORED PROGRAMMING REGISTRATION

You can set the tone that is sounded while a stored program is being registered, and when registration is complete. To set the audio tones:

1. At the control panel, press the **Machine Status** button, then touch the **Tools** tab.
2. Touch **System Settings > Common Service Settings > Audio Tones**.
3. Select an option:
  - **Stored Programming Tone:** This option sets the volume of the tone that is sounded while the program is registered. You cannot disable this tone.
  - **Stored Programming Complete Tone:** This option sets the volume of the tone that is sounded when the program registration is complete. If needed, you can disable this tone.
4. Touch **Change Settings**.
5. Select a volume setting for the tone.



Note: To disable the Stored Programming Complete Tone, select **Off**.

6. Touch **Save**.

## 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](http://www.xerox.com), then store the file on your computer.

### ENABLING PLUG-INS

To enable plug-ins:

1. In the Embedded Web Server, click **Properties > Security > Plug-in Settings > Embedded Plug-ins**.
2. For Embedded Plug-ins, select **Enabled**.
3. Click **Apply**.

### 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](http://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 **Properties > Security > Plug-in Settings > List of Embedded Plug-ins**.
2. Select an option to manage your plug-ins:
  - **Upload:** 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, then click **Details**.
  - **Stop:** To deactivate a plug-in, select a plug-in, then click **Stop**. If prompted, restart the printer.
  - **Start:** To start a deactivated plug-in, select a plug-in, then select **Start**. 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 **Properties > Security > Plug-in Settings > Signature Verification**.
2. For Signature Verification when Adding / Updating, select **Enabled**.
3. Click **Apply**.

## 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, press the **Machine Status** button, then touch the **Tools** tab.
2. Touch **System Settings > Common Service Settings > 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 **Confirm**.  
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, then touch **Save**.  
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 **Confirm / Change**, then touch **Close**.
6. Log out as administrator. To restart the printer, follow the onscreen prompts.



