

VERSION 1.0
JUNE 2023
702P09022

Xerox® B410 and C410 Printers Embedded Web Server

Administrator Guide

© 2023 Xerox Corporation. All rights reserved. Xerox® is trademark of Xerox Corporation in the United States and other countries.

Adobe®, Adobe PDF logo, Adobe® Reader®, Adobe® Type Manager®, ATM™, Flash®, Macromedia®, Photoshop®, and PostScript® are trademarks or registered trademarks of Adobe Systems, Inc.

Apple®, Bonjour®, EtherTalk™, TrueType®, iPad®, iPhone®, iPod®, iPod touch®, AirPrint® and the AirPrint Logo®, Mac®, Mac OS®, and Macintosh® are trademarks or registered trademarks of Apple Inc. in the U.S. and other countries.

Gmail™ webmail service, and Android™ mobile technology platform are trademarks of Google, Inc.

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

IBM® and AIX® are registered trademarks of International Business Machines Corporation in the United States and/or other countries.

McAfee®, ePolicy Orchestrator®, and McAfee ePO™ are trademarks or registered trademarks of McAfee, Inc. in the United States and other countries.

Microsoft®, Windows Vista®, Windows®, Windows Server®, and OneDrive® are registered trademarks of Microsoft Corporation in the United States and other countries.

Mopria is a trademark of the Mopria Alliance.

PANTONE® and other Pantone, Inc. trademarks are the property of Pantone, Inc.

UNIX® is a trademark in the United States and other countries, licensed exclusively through X/ Open Company Limited.

Linux® is a registered trademark of Linus Torvalds.

Wi-Fi CERTIFIED Wi-Fi Direct® is a trademark of the Wi-Fi Alliance.

PCL® is a registered trademark of the Hewlett-Packard Company. PCL is a designation of a set of printer commands (language) and functions included in its printer products. This printer is intended to be compatible with the PCL language. This means the printer recognizes PCL commands used in various application programs, and that the printer emulates the functions corresponding to the commands.

All other trademarks are the property of their respective owners.

BR38770

Contents

Overview	5
Overview.....	6
Supported Printer Models.....	7
Supported Web Browsers.....	8
Accessing the Embedded Web Server.....	9
Understanding Helper Text.....	10
Managing Printers.....	11
Checking the Status of Parts and Supplies from the Embedded Web Server.....	12
Generating Reports and Logs.....	13
Configuring Supply Notifications.....	14
Customizing the Home Screen.....	15
Editing the Home Screen.....	15
Adding an Application to the Home Screen.....	15
Arranging the Application on the Home Screen.....	15
Restoring the Home Screen.....	16
Importing and Exporting Home Screen Settings.....	16
Exporting Home Screen Settings.....	16
Importing Home Screen Settings.....	16
Managing Contacts.....	17
Adding Contacts.....	17
Adding Groups.....	17
Editing Contacts or Groups.....	17
Deleting Contacts or Groups.....	18
Activating a Supplies Plan.....	19
Activating a PagePack® or Metered Supplies Plan.....	19
Activating a Subscription Service Plan.....	19
Networking.....	21
Configuring the HTTP/FTP Settings.....	22
Selecting the Active Network Adapter.....	23
Connecting to a Wireless Network.....	24
Securing Printers.....	25
Securing Network Connections.....	26
Configuring the TLS Settings.....	26
Configuring TCP/IP Port Access Settings.....	26
Configuring IP Security Settings.....	26
Configuring 802.1x Authentication.....	27
Setting the Restricted Server List.....	28
Managing Devices Remotely.....	29
Using HTTPS for Printer Management.....	29

Setting Up SNMP.....	29
Configuring Security Audit Log Settings	30
Managing Security Audit Logs.....	31
Updating Firmware.....	31
Managing Login Methods	32
Restricting Public Access on the Guest Account	32
Using Local Accounts	32
Using LDAP or LDAP+GSSAPI	34
Using Kerberos.....	36
Using Active Directory	38
Creating LDAP, LDAP+GSSAPI, or Active Directory Groups.....	40
Editing or Deleting LDAP, LDAP+GSSAPI, or Active Directory Groups.....	41
Understanding Access Controls	41
Managing Certificates.....	44
Configuring Printer Certificate Defaults.....	44
Creating a Printer Certificate.....	44
Installing Certificates Manually	45
Installing Certificates Automatically.....	45
Viewing, Downloading, and Deleting Certificates.....	45
Managing Other Access Functions.....	46
Universal Print.....	46
Scheduling Access to USB Devices	48
Setting Login Restrictions	48
Configuring Confidential Printing.....	49
Enabling Solutions LDAP Settings.....	49
Showing Secured Applications or Functions on the Home Screen.....	50
Enabling Print Permission	50
Enabling the Security Reset Jumper.....	50
Securing Data.....	52
Configuring Printer Settings.....	52
Erasing Printer Memory.....	53
Erasing Printer Hard Disk Memory.....	53
Configuring Printer Hard Disk Encryption.....	53
Restoring Factory Default Settings	53
Troubleshooting.....	55
Login Troubleshooting.....	56
User Is Locked Out.....	56
User Is Logged Out Automatically	56
User Cannot Access Applications or Functions.....	56
KDC and Printer Clocks Are Out of Sync	56
Domain Controller Certificate Is Not Installed.....	56
KDC Is Not Responding Within the Required Time	57
LDAP Troubleshooting	58
LDAP Lookups Fail.....	58
Networking Problems	59
Printer Is Not Communicating on the Network.....	59

Overview

This chapter contains:

- Overview6
- Supported Printer Models7
- Supported Web Browsers.....8
- Accessing the Embedded Web Server.....9
- Understanding Helper Text 10

Overview

Use this document to manage and configure printer, network, and security settings using the Embedded Web Server. To secure the printer, combine login methods and access controls to define users who are allowed to use the printer and the functions that they can use.

Before you begin, ensure that the printer settings are configured for email. For details, refer to the User Guide for your printer model.

Also, identify the following conditions:

- The login method to use:
 - **Local Accounts:** Use the authentication methods available on the printer. User credentials are stored in the printer memory.
 - **Lightweight Directory Access Protocol (LDAP)**
 - **Generic Security Services Application Program Interface (LDAP+GSSAPI)**
 - **Kerberos**
 - **Active Directory**
- Other solutions that you want to include:
 - **Smart Card Authentication:** A collection of applications used to secure access to printers and their functions. The applications allow you to log in to a printer manually or with a smart card, then send emails and release print jobs securely. In an application, you can configure more security settings, such as email signing and encryption.
 - **Card Authentication:** Secure access to a printer using a card reader. When users badge in, their credentials are authenticated by a master printer, LDAP, or identity service provider (ISP).
- The group to which the users belong. You can create groups after creating the login methods.
- The applications, functions, and printer management settings that users can access.



Note: Administrator rights are required to configure or troubleshoot the security settings.

Supported Printer Models

The supported printer models are:

- Xerox® B410 Printers
- Xerox® C410 Color Printers


Supported Web Browsers

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

Accessing the Embedded Web Server

1. Obtain the printer IP address. Do one of the following:
 - Locate the IP address on the printer home screen.
 - View the IP address in the Network Overview section or in the TCP/IP section of the Network/Ports menu.
2. Open a web browser, then type the printer IP address.



	SECTION	DESCRIPTION
1	Top	<ul style="list-style-type: none"> • Shows the printer information and current status. • Allows the user to change the language of the web page. <p> Note: Changing the language of the web page does not affect the language on the printer display.</p>
2	Left	<ul style="list-style-type: none"> • Allows the user to search for items in the Embedded Web Server. • Contains links to the printer settings and other major sections of the Embedded Web Server.
3	Center	<ul style="list-style-type: none"> • Shows specific information on the selected section of the web page. • Allows the user to change configurations and settings. • Generates reports and logs. For more information, refer to Generating Reports and Logs.

Understanding Helper Text

Helper text is a short and concise description of a setting or page that indicates its usage or provides details on printer behavior when you apply a change. Helper text appears to the right of the setting field, below page or section headers, or at the bottom of the web page. Helper text also provides the user with a range of acceptable data entries.

Managing Printers

This chapter contains:

- Checking the Status of Parts and Supplies from the Embedded Web Server 12
- Generating Reports and Logs 13
- Configuring Supply Notifications..... 14
- Customizing the Home Screen..... 15
- Managing Contacts..... 17
- Activating a Supplies Plan..... 19

Checking the Status of Parts and Supplies from the Embedded Web Server



Note: Ensure that the computer and printer are connected to the same network.

1. To obtain the printer IP address, do one of the following:
 - Locate the IP address on the printer home screen.
 - View the IP address in the Network Overview section or in the Ethernet section of the Network/Ports menu.
2. Open a web browser, then type the printer IP address.
3. To view the status of the parts and supplies, click **Status > Supplies**.

Generating Reports and Logs

1. From the Embedded Web Server, click **Settings > Reports**.
2. Select a report or log.
 - **Menu Settings Page:** Shows the current printer preferences, settings, and configurations
 - **Device:**
 - **Device Information:** Shows information about the printer
 - **Device Statistics:** Shows printer usage and supply status
 - **Profiles List:** Shows a list of profiles that are stored on the printer
 - **Print, Print Directory:** Shows the resources that are stored on the flash drive or printer hard disk.



Note: This report appears only when a flash drive or printer hard disk is installed.

- **Shortcuts:**
 - **All Shortcuts:** Shows a list of all the shortcuts that are stored on the printer
 - **Email Shortcuts:** Shows a list of all email shortcuts that are stored on the printer
 - **FTP Shortcuts:** Shows a list of all FTP shortcuts that are stored on the printer
 - **Network Folder Shortcuts:** Shows a list of all network folder shortcuts that are stored on the printer
- **Network:**
 - **Network Setup Page:** Shows the configured network and wireless settings on the printer



Note: This report is available only in network printers and printers connected to print servers.

- **Wi-Fi Direct Connected Clients:** Shows the list of devices that are connected to the printer using Wi-Fi Direct



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

Configuring Supply Notifications

1. Open a web browser, then in the address field, type the printer IP address.

2. View the printer IP address on the printer home screen.

The IP address appears as four sets of numbers separated by periods, such as 123 . 123 . 123 . 123.

If you are using a proxy server, to load the web page correctly, disable the proxy server temporarily.

3. Click **Settings > Device > Notifications**.
4. From the Supplies menu, click **Custom Supply Notifications**.
5. For each supply item, select a notification.
6. Apply the changes.

Customizing the Home Screen

This feature lets users customize the applications in their printer display. Users can add, remove, or rearrange applications from the home screen and other pages. Users can also customize the application labels.



Note: For printers with a 4.3-inch screen, the home screen can accommodate eight applications. For printers with a 7-inch screen, the home screen can accommodate 15 applications.

EDITING THE HOME SCREEN

1. From the Embedded Web Server, click **Settings > > Device > > Home Screen Customizations**.
2. Select an application from the list, and then do the following:
 - a. Click **Edit**.
 - b. In the **App Label** field, type the name of the application.
 - The application label can have a maximum of 20 characters.
 - Click **Restore** app to restore the application label.
3. Click **Save**.
 - Click **Remove** to remove the application from the list.
 - The **Edit** option is disabled for BLANK SPACE and eSF applications

ADDING AN APPLICATION TO THE HOME SCREEN

To add an application to the home screen, perform the following procedure:

1. Click + to add an application.
2. Select the applications that you want to add.
3. Click **Add**.



Note:

- You can limit the applications to show on a particular page.
- If the number of applications on a particular page reaches the limit, the add icon for that page is disabled.

ARRANGING THE APPLICATION ON THE HOME SCREEN

To arrange an application on the home screen, perform the following procedure:

1. Select an application.
2. Drag and drop the application on the page where you want it to appear.

3. Click **Save**.



Note:

- Page 1 represents the first page of the home screen, while Other Pages represents the subsequent pages of the home screen. You can drag and drop applications to and from Page 1 to Other Pages.
- You can rearrange the order of applications for Page 1, but not for Other Pages.
- You cannot drag and drop any applications on a page which has reached the limit for the number of applications.
- If only one application remains, then you cannot drag an application out of that page.

RESTORING THE HOME SCREEN

To restore the home screen, perform the following procedure:

1. To restore the applications to their default label and location, click **Restore home screen**.
2. Click **Restore**.

IMPORTING AND EXPORTING HOME SCREEN SETTINGS

You can import or export home screen settings from one printer to another. If a native or eSF application is not supported, then it appears as a BLANK SPACE application in the home screen of that printer.

EXPORTING HOME SCREEN SETTINGS

To export the Home Screen Settings, perform the following:

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



Note: The files are exported in ZIP format.

IMPORTING HOME SCREEN SETTINGS

To import the home screen settings, perform the following:

1. From the Embedded Web Server, click **Import Configuration**.
2. Select the folder, and then click **Import**.
3. Click **OK**.



Note: If the files are not imported properly, then a warning message appears.

Managing Contacts

ADDING CONTACTS


 Note: This setting is available only in some printer models.

1. Open a web browser, then in the address field, type the printer IP address.
2. View the printer IP address on the printer home screen.

The IP address appears as four sets of numbers separated by periods, such as 123 . 123 . 123 . 123.

If you are using a proxy server, to load the web page correctly, disable the proxy server temporarily.

3. Click **Address Book**.
4. In the Contacts section, add a contact.

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

5. If necessary, specify a login method to allow application access.
6. Apply the changes.

ADDING GROUPS


 Note: This setting is available only in some printer models.

1. Open a web browser, then in the address field, type the printer IP address.
2. View the printer IP address on the printer home screen.

The IP address appears as four sets of numbers separated by periods, such as 123 . 123 . 123 . 123.

If you are using a proxy server, to load the web page correctly, disable the proxy server temporarily.

3. Click **Address Book**.
4. In the Contact Groups section, type a group name.

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

5. Apply the changes.

EDITING CONTACTS OR GROUPS

 Note: This setting is available only in some printer models.

1. Open a web browser, then in the address field, type the printer IP address.
2. View the printer IP address on the printer home screen.

The IP address appears as four sets of numbers separated by periods, such as 123 . 123 . 123 . 123.

If you are using a proxy server, to load the web page correctly, disable the proxy server temporarily.

3. Click **Address Book**.

4. Do one of the following:
 - In the Contacts section, click a contact name, then edit the information.
 - In the Contact Groups section, click a group name, then edit the information.
5. Apply the changes.

DELETING CONTACTS OR GROUPS



Note: This setting is available only in some printer models.

1. Open a web browser, then in the address field, type the printer IP address.
2. View the printer IP address on the printer home screen.

The IP address appears as four sets of numbers separated by periods, such as 123 . 123 . 123 . 123.

If you are using a proxy server, to load the web page correctly, disable the proxy server temporarily.

3. Click **Address Book**.
4. Do one of the following:
 - In the Contacts section, select a contact that you want to delete.
 - In the Contact Groups section, select a group name that you want to delete.

Activating a Supplies Plan

Your Xerox representative offers supplies and service plans.

- PagePack™ and Metered plans are based on a cost per page and include all service and supplies for your printer in one contract. When a starter cartridge is replaced with a PagePack® or Metered cartridge, the printer sets the plan automatically.
- A Subscription Service plan enables the printer to monitor supplies and when low, replacement supplies are ordered automatically.



Note: Subscription Service plans are not offered in all geographic locations.

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

ACTIVATING A PAGEPACK® OR METERED SUPPLIES PLAN

When you are enrolled in a supplies program, you need to activate the supplies plan at regular intervals. To enable your printer for your purchased plan, contact your Xerox representative to get a Supplies Activation Code.

To enter your Supplies Activation Code, do the following:

1. In the Embedded Web Server, log in as the administrator.
2. For Settings, click **Supplies Plan**.
3. For Supplies Plan, click **Plan Activation**.
4. In the Activation Code field, type the Supplies Activation Code.
5. Click **Activate Plan**.

ACTIVATING A SUBSCRIPTION SERVICE PLAN

For a Subscription Service plan, do the following:

1. In the Embedded Web Server, log in as the administrator.
2. For Settings, click **Supplies Plan**.
3. For Supplies Plan, click **Subscription Service**.
4. For the Subscription Service, click **Check Subscription**, then follow the directions provided by your Xerox representative.

Networking

This chapter contains:

Configuring the HTTP/FTP Settings	22
Selecting the Active Network Adapter	23
Connecting to a Wireless Network.....	24

Configuring the HTTP/FTP Settings



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

1. From the Embedded Web Server, click **Settings > Network/Ports > HTTP/FTP Settings**.
2. Configure the settings.

Proxy

- **HTTP Proxy IP Address:** Configure the HTTP server settings.
- **HTTP Default IP Port:** The factory default port for HTTP is 80.
- **FTP Proxy IP Address:** Configure the FTP server settings.
- **FTP Default IP Port:** The factory default port for FTP is 21.
- **Authentication:** Specify the authentication credentials.
- **Username:** Specify the unique user name.
- **Password:** Specify the unique password.
- **Local Domains:** Specify domain names for HTTP and FTP servers.

Other Settings

- **Enable HTTP Server:** Allow access to the Embedded Web Server for printer monitoring and management.
 - **Enable HTTPS:** Configure the HyperText Transfer Protocol Secure (HTTPS) settings.
 - **Force HTTPS Connections:** Force the printer to use the HTTPS connections.
 - **Enable FTP/TFTP:** Send files using FTP.
 - **HTTPS Device Certificate**
 - **Timeout for HTTP/FTP Requests:** Specify the time before the server connection stops.
 - **Retries for HTTP/FTP Requests:** Set the number of retries to connect to the HTTP/FTP server.
3. Click **Save**.

Selecting the Active Network Adapter

1. From the Embedded Web Server, click **Settings > Network/Ports > Network Overview > Active Adapter**.
2. Select the network adapter.

- **Auto:** Switch automatically to an available network connection.



Note: Ethernet connection takes precedence over wireless connection. Remove the Ethernet cable to allow the printer to detect the configured wireless network.

- **Standard Network:** Disable the wireless network connection and set the printer to connect only through Ethernet connection.
- **Wireless:** Disable the Ethernet network connection and set the printer to connect only through wireless connection.



Note: This setting appears only when a wireless network adapter is installed in the printer.

3. Click **Save**.

Connecting to a Wireless Network

Before you begin, ensure that:

- Your printer is connected temporarily to an Ethernet network.
- A wireless network adapter is installed in your printer and working properly. For details, refer to the instruction sheet that came with your wireless network adapter.

1. From the Embedded Web Server, click **Settings > Network/Ports > Wireless**.
2. Modify the settings to match the settings of your wireless router.



Note: Ensure that you type the correct network name.

3. Click **Save**.
4. Disconnect the Ethernet cable, then wait for at least one minute.
5. Ensure that your printer is connected to the network. Print a network setup page, then in the Wireless section, ensure that the Card Status is Connected.
For details, refer to the *Networking* section of the User Guide for your printer model.

Securing Printers

This chapter contains:

- Securing Network Connections 26
- Managing Devices Remotely 29
- Managing Login Methods 32
- Managing Certificates 44
- Managing Other Access Functions 46
- Securing Data 52


Securing Network Connections

CONFIGURING THE TLS SETTINGS


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

To configure TLS:

1. From the Embedded Web Server, click **Settings > Network/Ports > TCP/IP**.
2. For TLS Version for Secure Device Communication over a Network, enable TLSv1.0, TLSv1.1, or TLSv1.2. These settings pertain to the Embedded Web Server only. They do not pertain to clients using TLS.

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

3. Click **Save**.

 Note: View the SSL Cipher List and TLSv1.3 SSL Cipher List for the Saved TLS configuration.


CONFIGURING TCP/IP PORT ACCESS SETTINGS

You can control device network activities by configuring your device to filter out traffic on specific network connections. You can disable protocols, such as FTP, HTTP, and Telnet.

Port filtering on devices disables network connections individually. When a port is closed, a device does not respond to traffic on the specified port even if the corresponding network application is enabled.

We recommend that you close any ports that you do not plan to use during standard operation.

1. From the Embedded Web Server, click **Settings > Network/Ports > TCP/IP**.
2. Enable access to the TCP/IP ports.
3. Click **Save**.

 Note: View the SSL Cipher List and TLSv1.3 SSL Cipher List for the Saved TLS configuration.

CONFIGURING IP SECURITY SETTINGS


Apply IP Security (IPsec) between the printer and the workstation or server to secure traffic between the systems with a strong encryption. The printers support IPsec with pre-shared keys (PSK) and certificates. You can use both options simultaneously.

When you use PSK authentication, printers are configured to establish a secure IPsec connection with up to seven other systems. The printers and systems are configured with a key or passphrase that is used to authenticate the systems and to encrypt the data.


When you use the CA certificate authentication, printers are configured to establish a secure IPsec connection with up to five systems or subnets. Printers exchange data securely with many systems, and the process is integrated with a PKI or CA infrastructure. Certificates provide a robust and scalable solution, without configuring or managing keys or passphrases.

1. From the Embedded Web Server, click **Settings > Network/Ports > IPsec**.


2. Select **Enable IPSec**.
3. To specify the encryption and authentication methods of the printer, configure the following settings:
 - Base Configuration
 - DH (Diffie-Hellman) Group Proposal

 Note: This feature is enabled when Base Configuration is set to **Compatibility**.


 - Proposed Encryption Method

 Note: This feature is enabled when Base Configuration is set to **Compatibility**.


 - Proposed Authentication Method

 Note: This feature is enabled when Base Configuration is set to **Compatibility**.


 - IPSec Device Certificate

 Note: Before you can select a device certificate, ensure that the certificate is installed. For details, refer to [Managing Certificates](#).

 - IKE SA Lifetime (Hours): Default is 24.


 Note: When the Base Configuration is set to **Secure**, this feature is enabled.

 - IPSec SA Lifetime (Hours): Default is 8.


 Note: When the Base Configuration is set to **Secure**, this feature is enabled.
4. Do one or more of the following:
 - In the Pre-Shared Key Authenticated Connections section, type the IP address of the client printer that you want to connect to the printer using Pre-Shared Key based IPSec Authentication.
 - In the Certificate Authenticated Connections section, type the IP address of the client printer that you want to connect to the printer using Certificate based IPSec Authentication.
5. Click **Save**.
 - If no CA certificates are added, then the default certificate is used.
 - If you are using PSK authentication, then type the corresponding key. Retain the key to use later when configuring client printers.

CONFIGURING 802.1X AUTHENTICATION

Though normally associated with wireless devices and connectivity, 802.1x authentication supports both wired and wireless environments.

 Note: If you are using digital certificates to establish a secure connection to the authentication server, then configure the certificates on the printer before changing 802.1x authentication settings.

For details, refer to [Managing Certificates](#).

 Note: Ensure that all printers on the same network using 802.1x are supporting the same EAP authentication type.

1. From the Embedded Web Server, click > **Settings > Network/Ports > 802.1x**.
2. In the 802.1x Authentication section, do the following:
 - a. Select **Active**.
 - b. Type the login name and password that the printer uses to log in to the authentication server.
 - c. Select **Validate Server Certificate**.



Note: Server certificate validation is necessary when using Transport Layer Security (TLS), Protected Extensible Authentication Protocol (PEAP), and Tunneled Transport Security Layer (TTLS).

- d. Select **Enable Event Logging**.

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

- e. In the 802.1x Device Certificate list, select a digital certificate.



Note: If only one certificate is installed, then Default is the only option that appears.

3. In the Allowable Authentication Mechanisms section, select one or more authentication protocols.
 - **EAP-MD5, EAP-MSCHAPv2, LEAP, and PEAP:** These options require a login name and password.
 - **EAP-TLS:** This option requires a login name, a CA certificate, and a signed printer certificate.
 - **EAP-TTLS:** This option requires a login name and password and a CA certificate.
4. From the TTLS Authentication Method menu, select an authentication method.
5. Click **Save**.

SETTING THE RESTRICTED SERVER LIST

You can configure printers to connect only from a list of specified TCP/IP addresses. This action blocks all TCP connections from other addresses, and protects the printer against unauthorized printing and configuration.

1. From the Embedded Web Server, click **Settings > Network/Ports > TCP/IP**.
2. In the Restricted Server List field, type up to 50 IP addresses, separated by commas, that are allowed to make TCP connections.
3. Click **Save**.
4. Configure the **Restricted Server List** options:
 - **Block All Ports:** This option addresses the ports that are not in the restricted server list, and blocks all access to the ports (default).
 - **Block Printing Only :** This option addresses the ports that are not in the restricted sever list, and blocks only the printing.
 - **Block Printing and HTTP Only:** This option addresses the ports that are not in the restricted server list and blocks only printing and HTTP.

Managing Devices Remotely

USING HTTPS FOR PRINTER MANAGEMENT

To restrict the access of the printer Embedded Web Server to HTTPS only, disable the HTTP port and leave the HTTPS port (443) active. This action ensures that all communication with the printer using the Embedded Web Server is encrypted.

1. From the Embedded Web Server, click **Settings > Network/Ports > TCP/IP**, then select **TCP/IP Port Access**.
2. Clear **TCP 80 (HTTP)**.
3. Click **Save**.

SETTING UP SNMP

Configuring Settings for SNMP Versions 1 or 2c

1. From the Embedded Web Server, click **Settings > Network/Ports > SNMP**.
2. In the SNMP Versions 1 and 2c section, select **Enabled**.
3. In the SNMP Versions 1 and 2c section, select **Allow SNMP Set**.
4. In the GET SNMP Community field, type a name for the GET SNMP Community identifier. The default community name is `public`.
5. In the SET SNMP Community field, type a variable for SET SNMP. The default variable is `private`.
6. To facilitate the automatic installation of print drivers and other printing applications, select **Enable PPM MIB** (Printer Port Monitor MIB).
7. Click **Save**.

Configuring Settings for SNMP Version 3

Before you begin, disable SNMP versions 1 and 2c.

1. From the Embedded Web Server, click **Settings > Network/Ports > SNMP**.
2. In the SNMP Version 3 section, select **Enabled**.
3. If required, to configure the following options, provide your authentication credentials.
 - **Set Read/Write Credentials:** Allow remote installation and configuration changes and printer monitoring.
 - **Set Read-only Credentials:** Allow printer monitoring only.
4. In the Authentication Hash menu, select the hash function of your SNMP server.
5. For Minimum Authentication Level, select **Authentication, Privacy**.
6. In the Privacy Algorithm menu, select the strongest setting that is supported by your network environment.
7. Click **Save**.

Configuring SNMP Traps

After configuring SNMP settings, you can customize which alerts are sent to the network management system by designating events (SNMP traps) that trigger an alert message.

1. From the Embedded Web Server, click **Settings > Network/Ports > SNMP > Set SNMP Traps**.
2. In one of the IP Address fields, type the IP address of the network management server or monitoring station.
3. Select the conditions for which you want to generate an alert.
4. Click **Save**.

CONFIGURING SECURITY AUDIT LOG SETTINGS

The security audit log allows administrators to monitor security-related events on a device, including failed user authorization, successful administrator authentication, and Kerberos file uploads to a device. By default, security logs are stored on the device, but can also be transmitted to a network system log (syslog) server for processing or storage.



Note: Security Audit Log settings are available for selected printer models only.

Xerox recommends that you enable audit in secure environments.

1. From the Embedded Web Server, click **Settings > Security > Security Audit Log**.
2. To activate security audit logging, select **Enable Audit**.
The transmission to a network syslog server option lets you use both the remote syslog server and the internal logging.
3. Configure transmission to a network syslog server.
 - a. Select **Enable Remote Syslog**.
 - b. Configure the Remote Syslog settings.
 - **Remote Syslog Server:** Type the IP address or host name of the server.
 - **Remote Syslog Port:** Type the port number used for the destination server. The default number is 514.
 - **Remote Syslog Method:** To send log messages and events using a lower-priority transmission protocol, select **Normal UDP**. Otherwise, select **Stunnel**.
 - **Remote Syslog Facility:** Select a facility code for events logged to the destination server. All events sent from the device are tagged with the same code, which aids in sorting and filtering by network monitor or intrusion detection software.
 - **Severity of Events to Log:** Select the priority level cutoff for logging messages and events. The highest severity is 0. The lowest severity is 7. Events with the selected severity level and higher are logged. For example, if you select 4 - Warning, then severity levels 0-4 are logged.
 - **Remote Syslog Non-Logged Events:** Send all events to the remote server, regardless of severity.

4. Configure the email notification settings.
To ensure that the printer settings have been configured for email, in the Admin's Email Address field, type one or more email addresses separated by commas.
 - **Email Log Cleared Alert:** Send a notification when the user clicks the Delete Log button.
 - **Email Log Wrapped Alert:** Send a notification when the log becomes full and begins to overwrite the oldest entries.
 - **Log Full Behavior:** Wrap over oldest entries or email the log and then delete all entries.
 - **Email % Full Alert:** Send a notification when log storage space reaches a certain percentage of capacity.
 - **% Full Alert Level:** Specify how full the log is before an alert is triggered.
 - **Email Log Exported Alert:** Send a notification when the log file is exported.
 - **Email Log Settings Changed Alert:** Send a notification when the log settings are changed.
 - **Log Line Endings:** Specify how the log file terminates the end of each line.
 - **Digitally Sign Exports:** Add a digital signature to each exported log file.
5. Click **Save**.

MANAGING SECURITY AUDIT LOGS

1. To delete the syslog, in the Clear Log menu, click **Clear**.
2. To view or save the syslog, in the Export Log menu, select the file type, and then click **Export**.

UPDATING FIRMWARE

Printers inspect all downloaded firmware packages for some required attributes before they adopt and execute the packages. The firmware is packaged in a proprietary format and encrypted with a symmetric encryption algorithm through an embedded key that is known only to the manufacturer. However, the strongest security measure comes from the requirement that all firmware packages include multiple digital 2048-bit RSA signatures from the manufacturer. If these signatures are not valid, or if the message logs indicate a change in firmware after the signatures were applied, then the firmware is discarded.

1. From the Embedded Web Server, click **Settings > Device > Software Update**.
2. Do one of the following:
 - Browse to the firmware file, then click **Upload**.
 - Click **Check now > I agree, start update**.

Managing Login Methods

RESTRICTING PUBLIC ACCESS ON THE GUEST ACCOUNT

The guest account can use the printer without logging in. To control the access of guest account users, restrict the functions, applications, printer management, and security options for the guest account.

1. From the Embedded Web Server, click **Settings > Security > Login Methods**.
2. In the Public section, click **Manage Permissions**.
3. Select the access controls that the guest account can access. For details, refer to [Understanding Access Controls](#).
4. Click **Save**.

USING LOCAL ACCOUNTS

Creating Local Accounts

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

1. From the Embedded Web Server, click **Settings > Security > Login Methods**.
2. In the Local Accounts section, click **Add User**.
3. Select the type of authentication method that you want the account to use to log in to the printer.
 - **User Name/Password:** Add an account with a user name and password.
 - **User Name:** Add an account with a user name only.
 - **Password:** Add an account with a password only.
 - **PIN:** Add an account with a personal identification number (PIN) only.
4. From the User Information section, type the user information and authentication credentials.
5. From the Permission Groups section, select one or more groups.



Note: To create a group for the user, select **Add New Group**. For details, refer to [Creating Local Account Groups](#).

6. Click **Save**.

Editing and Deleting Local Accounts

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

1. From the Embedded Web Server, click **Settings > Security > Login Methods**.
2. In the Local Accounts section, click the authentication method to which the user account belongs.
3. Click the user account that you want to edit or delete.

4. Do one of the following:
 - To edit the user account, update the user information, then click **Save**.
 - To delete the user account, click **Delete User**.



Note: To delete multiple user accounts, select the accounts, then click **Delete**.

Creating Local Account Groups

Use groups to customize access for the user to applications and printer functions.

1. From the Embedded Web Server, click **Settings > Security > Login Methods**.
2. Do one of the following:
 - Add a group when managing permissions, or
 - Add a group when creating or editing a user account.
3. To add a group when managing permissions, perform the following:
 - a. From the Local Accounts section, click **Manage Groups/Permissions**.
 - b. Click **Add Group**.
4. To add a group when creating or editing a user account, perform the following:
 - a. Create or edit a user account.
 - b. In the Permission Groups section, select **Add New Group**.
5. Type a unique group name.
6. In the Access Controls section, select the functions, menus, and applications that the group can access.
7. Click **Save**.

To import access controls from another group, click **Import Access Controls**, then select a group. For details on access controls, refer to [Understanding Access Controls](#).

Editing or Deleting Local Account Groups

1. From the Embedded Web Server, click **Settings > Security > Login Methods**.
2. In the Local Accounts section, click **Manage Groups/Permissions**.
3. Click the group, then do one of the following:
 - Configure the access controls, then click **Save**.
 - Click **Delete Group**.



Note: Refer to the following information:

- To import access controls from another group, click **Import Access Controls**, then select a group.
- To delete multiple groups, select the groups, then click **Delete**.

For details on access controls, refer to [Understanding Access Controls](#).

USING LDAP OR LDAP+GSSAPI

LDAP is a standards-based, cross-platform, extensible protocol that runs directly on top of the TCP/IP layer. LDAP is used to access information stored in a specially organized information directory. LDAP can interact with many different kinds of databases without special integration, which makes LDAP more flexible than other authentication methods.

When you want your transmission always to be secure, use LDAP+GSSAPI. Instead of authenticating directly with the LDAP server, the user is first authenticated using Kerberos to obtain a Kerberos ticket. This ticket is presented to the LDAP server using the GSSAPI protocol for access. LDAP+GSSAPI is typically used for networks that run Active Directory.

- LDAP+GSSAPI requires a Kerberos network account. For details, refer to [Creating a Kerberos Login Method](#).
- Supported printers can store a maximum of eight unique LDAP or LDAP+GSSAPI login methods. A unique name is required for each method.
- Administrators can create up to 32 user-defined groups that apply to each unique login method.
- LDAP and LDAP+GSSAPI rely on an external server for authentication. If the server is down, then users cannot access the printer using LDAP or LDAP+GSSAPI.
- To help prevent unauthorized access, log out from the printer after each session.

Creating an LDAP or LDAP+GSSAPI Login Method


1. From the Embedded Web Server, click **Settings > Security > Login Methods**.
2. In the Network Accounts section, click **Add Login Method > LDAP**.
3. Select the authentication type:
 - **LDAP**
 - **LDAP+GSSAPI**
4. Configure General Information settings.
 - **Setup Name:** Type a unique name for the LDAP network account.
 - **Server Address:** Type the IP address or the host name of the LDAP server.
 - **Server Port:** Type the port number to which LDAP queries are sent.

 Note: If you are using SSL, then use port 636. Otherwise, use port 389.

- **Required User Input:** Select the required LDAP authentication credentials to be used when a user logs in to the printer. This setting is available only in the LDAP setup.
- **Use Integrated Windows Authentication:** Select one of the following:
 - **Do not use**
 - **Use if available:** Use Windows operating system authentication credentials, if available.
 - **Require:** Use Windows operating system authentication credentials only.

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

5. Configure Device Credentials settings.
 - **Anonymous LDAP Bind:** Bind the printer with the LDAP server anonymously. This option is applicable only if your LDAP server allows anonymous binding. Enabling this option does not require you to provide authentication credentials. This option is available only in the LDAP setup.
 - **Use Active Directory Device Credentials:** Use user credentials and group designations that are pulled from the existing network comparable to other network services. This option is available only in the LDAP +GSSAPI setup.
 - If **Anonymous LDAP Bind** or **Use Active Directory Device Credentials** is disabled, then provide the authentication credentials used to bind the printer with the LDAP server.
 - **Device Username**
 - For LDAP setup, type the fully qualified distinguished name (DN) of a user registered to the LDAP server.
 - For LDAP+GSSAPI setup, type the DN of a user registered to the Kerberos server.
 - **Device Realm:** The realm used for the Kerberos server. This setting is available only for the LDAP +GSSAPI setup.
 - **Device Password:** Type the password for the user.
6. Configure Advanced Options settings.
 - **Use SSL/TLS:** If the LDAP server requires SSL, then select **SSL/TLS**.
 - **Require Certificate:** If the LDAP server requires a certificate, then select **Yes**.
 - **Userid Attribute:** Type the LDAP attribute to search for when authenticating user credentials. The default value is `sAMAccountName`, which is common in a Windows operating system environment. For other directories, you can type `uid`, `cn`, or a user-defined attribute. For details, contact your system administrator.
 - **Mail Attribute:** Type the LDAP attribute that contains the email addresses for users. The default value is `mail`.
 - **Full Name Attribute:** Type the LDAP attribute that contains full names for users. The default value is `cn`.
 - **Home Directory Attribute:** Type the LDAP attribute that contains the home directory for users. The default value is `homeDirectory`.
 - **Group Membership Attribute:** Type the LDAP attribute required for group search. The default value is `memberOf`.
 - **Search Base:** This setting is the node in the LDAP server where user accounts reside. You can type multiple search bases, separated by commas.

 Note: A search base consists of multiple attributes separated by commas, such as `cn (common name), ou (organizational unit), o (organization), c (country), and dc (domain)`.

 - **Search Timeout:** Type a value from 5 to 30 seconds or 5 to 300 seconds, depending on your printer model.
 - **Follow LDAP Referrals:** Search the different servers in the domain for the logged-in user account.

7. Configure Search Specific Object Classes settings.

- **person:** Search the person object class.
- **Custom Object Classes:** Type the name of the custom object class to search.



Note: A maximum of three custom object classes can be searched. Type the other object class in the other Custom Object Class field.

8. Configure Address Book Setup settings.

The following settings are used to configure the address book used when scanning to an email address.

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

9. Click **Save and Verify**.

Editing or Deleting the LDAP or LDAP+GSSAPI Login Method

1. From the Embedded Web Server, click **Settings > Security > Login Methods**.

2. In the Network Accounts section, click the **LDAP** or **LDAP+GSSAPI** login method.

3. Do one of the following:

- To edit the login method, update the LDAP or LDAP+GSSAPI settings, then click **Save and Verify**.
- To delete the login method, click **Delete LDAP**.

USING KERBEROS

You can use the Kerberos login method alone or in conjunction with the LDAP+GSSAPI login method.


- Only one Kerberos configuration file can be saved to the printer memory. This configuration file can apply to multiple realms and Kerberos Domain Controllers.
- When you upload another configuration file or update the Kerberos settings, the saved configuration file is overwritten.
- If you want to delete a Kerberos file, before you delete the file, first delete the LDAP+GSSAPI login method that is using the file.
- Administrators are required to anticipate the different types of authentication requests the Kerberos server can receive, and to configure the configuration file to handle the requests.
- Kerberos relies on an external server for authentication. If the server is down, then users cannot access the printer using Kerberos.
- To help prevent unauthorized access, after each session, log out from the printer.

Creating a Kerberos Login Method

1. From the Embedded Web Server, click **Settings > Security > Login Methods**.
2. In the Network Accounts section, click **Add Login Method > Kerberos**.
3. Do one of the following:
 - Create a simple Kerberos configuration file.
 - Import a Kerberos configuration file.
4. To create a simple Kerberos configuration file, from the Generate Simple Kerberos File section, configure the following:
 - **KDC Address:** Type the IP address or host name of the KDC IP.
 - **KDC Port:** Enter the port number used by the Kerberos server.
 - **Realm:** Type the realm used by the Kerberos server. It is required that you type the realm in uppercase.
5. To Import a Kerberos configuration file, in the Import Kerberos File field, browse to the `krb5.conf` file.
6. In the Miscellaneous Settings section, configure the following settings, as needed:
 - **Character Encoding:** Select the character encoding used for the configuration file.
 - **Disable Reverse IP Lookups**
7. Click **Save and Verify**.

Setting the Date and Time

When you use Kerberos authentication, ensure that the time difference between the printer and the domain controller does not exceed five minutes. You can update the date and time settings manually, or to sync the time with the domain controller automatically, you can use the Network Time Protocol (NTP).

1. From the Embedded Web Server, click **Settings > Device > Preferences > Date and Time**.
2. To configure the date and time manually, perform the following:
 -  Note: Manual configuration disables NTP.
 - a. From the Configure section, in the Manually Set Date and Time field, enter the appropriate date and time.
 - b. Select the date format, time format, and time zone.
3. To set the date and time automatically, configure NTP:
 - a. In the Network Time Protocol section, select **Enable NTP**, then type the IP address or host name of the NTP server.
 - b. If the NTP server requires authentication, then in the Enable Authentication menu, select **MD5 key**.
 - c. Depending on your printer model, either type the key ID and password, or browse to the file containing the NTP authentication credentials.
4. Click **Save**.

USING ACTIVE DIRECTORY

You can use the Active Directory login method alone or in conjunction with the LDAP+GSSAPI login method.

- Only one Kerberos configuration file can be saved in the printer memory. This configuration file can apply to multiple realms and Kerberos Domain Controllers.
- Administrators are required to anticipate the different types of authentication requests the Kerberos server can receive, and to configure the configuration file to handle the requests.
- Uploading another configuration file or updating the Kerberos settings overwrites the saved configuration file.
- Active Directory relies on an external server for authentication. If the server is down, then users cannot access the printer using Active Directory.
- To help prevent unauthorized access, after each session, log out from the printer.

Creating an Active Directory Login Method


1. From the Embedded Web Server, click **Settings > Security > Login Methods**.
2. In the Network Accounts section, click **Add Login Method > Active Directory**.
3. Configure the settings.
 - **Domain:** Type the realm or domain name of the Active Directory server.
 - **User Name:** Type the name of the user that can authenticate to the Active Directory.
 - **Password:** Type the password of the user.
 - **Organizational Unit:** Type the organizational unit attribute to which the user belongs.
4. Click **Join Domain**.

Editing or Deleting an Active Directory Login Method

1. From the Embedded Web Server, click **Settings > Security > Login Methods**.
2. In the Network Accounts section, click the **Active Directory** login method.
3. To delete the login method, click **Unjoin Domain**.
4. Configure the General Information settings.
 - **Setup Name:** Type a unique name for the Active Directory login method.
 - **Server Address:** Type the IP address or the host name of the LDAP server.
 - **Server Port:** Enter the port where queries are sent.
 - **Required User Input:** Select the required authentication credentials when logging in to the printer.
 - **Use Integrated Windows Authentication.** Select one of the following:
 - **Do not use**
 - **Use if available:** Use Windows operating system authentication credentials, if available.
 - **Require:** Use only Windows operating system authentication credentials.


5. Configure the Device Credentials options.
 - **Use Active Directory Device Credentials:** Use user credentials and group designations that are pulled from the existing network comparable to other network services.
 - If **Use Active Directory Device Credentials** is disabled, then provide the authentication credentials used to bind the printer with the Active Directory server.
 - **Device Username:** Type the fully qualified DN of a user registered to the Active Directory server.
 - **Device Realm:** The Active Directory domain name.
 - **Device Password:** Type the password for the user.

6. Configure the Advanced Options settings.
 - **Use SSL/TLS:** If the LDAP server requires SSL, then select **SSL/TLS**.
 - **Require Certificate:** If the LDAP server requires a certificate, then select **Yes**.
 - **Userid Attribute:** Type the LDAP attribute to search for when authenticating user credentials. The default value is `sAMAccountName`, which is common in a Windows environment. For other directories, you can type `uid`, `cn`, or a user-defined attribute. For more information, contact your system administrator.
 - **Mail Attribute:** Type the LDAP attribute that contains the email addresses for users. The default value is `mail`.
 - **Full Name Attribute:** Type the LDAP attribute that contains the full names for users. The default value is `cn`.
 - **Home Directory Attribute:** Type the LDAP attribute that contains the home directory for users. The default value is `homeDirectory`.
 - **Group Membership Attribute:** Type the LDAP attribute required for group search. The default value is `memberOf`.
 - **Search Base:** This setting is the node in the LDAP server where user accounts reside. You can type multiple search bases, separated by commas.

 Note: A search base consists of multiple attributes separated by commas, such as `cn` (common name), `ou` (organizational unit), `o` (organization), `c` (country), and `dc` (domain).

 - **Search Timeout:** Enter a value from 5 to 30 seconds or 5 to 300 seconds, depending on your printer model.
 - **Follow LDAP Referrals:** Search the different servers in the domain for the logged-in user account.

7. Configure the Search Specific Object Classes settings.
 - **person:** Search the person object class.
 - **Custom Object Classes:** Type the name of the custom object class to search.

 Note: You can search a maximum of three custom object classes. In the other Custom Object Class field, type the other object class.

8. Configure the Address Book Setup settings.
Use the following settings to configure the address book used when scanning to an email address:
 - **Displayed Name:** Select the LDAP attribute that you want to show on the address book.
 - **Max Search Results:** Type the maximum search results shown on the address book.
 - **Use User Credentials:** Connect to the LDAP server with the credentials for the logged-in user.
 - **Search Attributes:** Select LDAP attributes used as search filters.
 - **Custom Attributes:** Type LDAP custom attributes used as search filters.
9. Click **Save and Verify**.

CREATING LDAP, LDAP+GSSAPI, OR ACTIVE DIRECTORY GROUPS

To customize user access to applications and printer functions, you can use groups.

1. From the Embedded Web Server, click **Settings > Security > Login Methods**.
2. In the Network Account section, click the **LDAP, LDAP+GSSAPI, or Active Directory** login method.
3. Click **Manage Groups > Add Group**.
4. Choose one of the following:
 - Search for the group name or user name, or
 - Add the group manually.
5. To search for the group name or user name, perform the following:
 - a. Select how you want to search for the group in your LDAP server.
 - b. Depending on the search scope selected, type the group name or the user name.
 - c. Click **Search**.
 - d. Select the group that you want to add.
 - e. Click **Add Selected**.
6. To add the group manually, perform the following:
 - a. Click **Manual Add**.
 - b. In the Group Name field, type the name of the group.
 - c. In the Group Identifier field, type the LDAP identifier for the group.
 - d. Click **Submit**.
7. Select the group, then in the Access Controls section, select the functions, menus, and applications that the group can access.
8. Click **Save**.
9. To import access controls from another group, click **Import Access Controls**, then select a group.
For details on access controls, refer to [Understanding Access Controls](#).

EDITING OR DELETING LDAP, LDAP+GSSAPI, OR ACTIVE DIRECTORY GROUPS

1. From the Embedded Web Server, click **Settings > Security > Login Methods**.
2. Click the **LDAP, LDAP+GSSAPI, or Active Directory** login method, then click **Manage Groups**.
3. Click the group, and then do one of the following:
 - Configure the access controls, and then click **Save**.
 - Click **Delete Group**.
 - To import access controls from another group, click **Import Access Controls**, then select a group.
 - To delete multiple groups, select the groups, then click **Delete**.

For details on access controls, refer to [Understanding Access Controls](#).

UNDERSTANDING ACCESS CONTROLS

Access controls allow you to limit user access to functions, applications, and printer management.



Note: Some access controls are available only in some printer models.

Function Access

The following access controls modify user access to available printer functions:

- **Access Address Book in Apps:** Use Address Book from eSF applications that support Address Book.
- **Manage Shortcuts:** Access the Manage Shortcuts menu, and enable the Save as Shortcut option available in the Email, and FTP functions.
- **Modify Address Book:** Enable the Search Address Book option available in the Email, and FTP functions when accessed from the printer home screen.
- **Create Profiles:** Create profiles for printing or emailing.
- **Manage Bookmarks**
- **Flash Drive Print:** Print from a flash drive.
- **Flash Drive Color Printing:** Print from a flash drive in color.
- **Email Function:** Use the email function.
- **FTP Function:** The FTP icon is hidden by default. To show the FTP icon on the home screen:
 1. From the Embedded Web Server, click **Settings > Device > Visible Home Screen Icons**.
 2. Select **FTP**.
- **Held Jobs Access:** Enable the Held Jobs and Search Held Jobs options on the printer home screen.
- **Use Profiles:** Restrict access to protected profiles. If a user accesses a protected profile, then the printer prompts for credentials to execute the profile. Enable this access control for the application that does not specify permission to access the profiles.
- **Cancel Jobs at the Device:** Cancel jobs from the printer home screen.
- **Change Language:** Enable the Change Language option on the printer home screen.

- **Internal Printing Protocol (IPP):** Allow authenticated users to configure and use the IPP port.
- **B/W Print:** Allow authenticated users to print in black and white.
- **Color Print:** Allow authenticated users to print in color.

Administrative Menus

The following access controls modify user access to the menus in the Embedded Web Server that are used to manage functions, applications, and security:

- **Security Menu:** Manage login methods and configure other security options.
- **Network/Ports Menu:** Configure network connections.
- **Paper Menu:** Configure the paper settings.
- **Reports Menu:** View reports.
- **Function Configuration Menus:** Configure the settings for the functions that are available in the printer.
- **Supplies Menu:** Manage printer supplies.
- **Option Card Menu:** Configure the option cards installed in the printer. This control is available only when an option card is installed.
- **SE Menu:** View diagnostic logs.
- **Manage Shortcuts:** Manage shortcuts that are available in the printer.
- **Address Book:** Manage the address book.
- **Device Menu:** Configure the printer firmware settings.

Device Management

The following access controls modify user access to use printer management options:

- **Remote Management:** Access the printer remotely.
- **Firmware Updates:** Update the printer firmware through any port.
- **Apps Configuration:** Configure the installed applications. If this control is enabled, then users can configure, start/stop, uninstall, and view logs of applications that are installed in the printer.
- **Operator Panel Lock:** Configure the locking function of the printer home screen. If this control is enabled, then users can lock and unlock the printer home screen.
- **Import / Export All Settings:** Import or export a printer settings file (.zip and .ucf) from the Embedded Web Server.
- **Out of Service Erase:** Clear all settings, applications, and pending jobs stored in the printer memory, or erase all data in the printer hard disk.
- **Embedded Web Server Access:** Control access to the Embedded Web Server. If this control is restricted, then access to the EWS requires login.

Apps

- **New Apps:** Use applications from the printer home screen.
- **Forms and Favorites:** Use Forms and Favorites from the printer home screen.

Managing Certificates

Certificates are used when you want the printer to establish an SSL/TLS, IPsec, or 802.1x connection and to identify other devices on the network securely. Printers can also use these certificates for LDAP over SSL authentication and address book lookups.

Certificate Authorities (CA) are trusted locations established on the network that are required in secure environments. Otherwise, the default printer certificate is used to identify devices on the network.

CONFIGURING PRINTER CERTIFICATE DEFAULTS

1. From the Embedded Web Server, click **Settings > Security > Certificate Management**.
2. In the Device Certificates section, click **Configure Certificate Defaults**.
3. Configure the settings.
 - **Friendly Name:** Type a unique name for the certificate.
 - **Common Name:** Type the name for the printer.



Note: If you want to use the printer host name, then leave this field blank.

- **Organization Name:** Type the name of the company or organization that issues the certificate.
- **Unit Name:** Type the name of the unit within the company or organization that issues the certificate.
- **Country/Region:** Type the country or region where the company or organization that issues the certificate is located.
- **Province Name:** Type the name of the province or state where the company or organization that issues the certificate is located.
- **City Name:** Type the name of the city where the company or organization that issues the certificate is located.
- **Subject Alternate Name:** Type the alternate name and prefix that conforms to RFC 2459. For example, type an IP address using the format `IP : 1 . 2 . 3 . 4`, or a DNS address using the format `DNS : ldap . company . com`.



Note: If your printer is using an IPv4 address, then leave this field blank.

4. Click **Save**.

CREATING A PRINTER CERTIFICATE

1. From the Embedded Web Server, click **Settings > Security > Certificate Management**.
2. In the Device Certificates section, click **Generate**.
3. Configure the settings. For details, refer to [Configuring Printer Certificate Defaults](#).
4. Click **Generate** or **Generate and Download**.

INSTALLING CERTIFICATES MANUALLY

For details on how to download the CA certificate automatically, refer to [Installing Certificates Automatically](#).

Before you configure Kerberos or domain controller settings, install the CA certificate used for domain controller validation. If you want to use chain validation for the domain controller certificate, then install the entire certificate chain. Each certificate requires a separate PEM (.cer) file.

1. From the Embedded Web Server, click **Settings > Security > Certificate Management**.
2. In the Manage CA Certificates section, click **Upload CA**, then browse to the PEM (.cer) file.

The following is a sample certificate:

```
-----BEGIN CERTIFICATE-----
MIIE1jCCA76gAwIBAgIQY6sV0KL3tIhBt1r4gHG85zANBgkqhkiG9w0BAQUFADBs
...
13DTbPe0mnIbTq0iWqKEaVne1vvaDt52iSpEQyevwgUcHD16rFy+sOnCaQ==
-----END CERTIFICATE-----
```

3. Click **Save**.

INSTALLING CERTIFICATES AUTOMATICALLY

1. From the Embedded Web Server, click **Settings > Security > Certificate Management > Configure Certificate Auto Update**.
2. If you are prompted to join an Active Directory domain, click **Join Domain**, then type the domain information.
3. Select **Enable Auto Update**.



Note: If you want to install the CA certificate without waiting for the scheduled run time, select **Fetch Immediately**.

4. Click **Save**.

VIEWING, DOWNLOADING, AND DELETING CERTIFICATES

1. From the Embedded Web Server, click **Settings > Security > Certificate Management**.
2. Select a certificate from the list.
3. Select one or more of the following:

- **Delete:** Remove a previously stored certificate.



Note: To delete multiple certificates, select the certificates, then click **Delete**.

- **Download To File:** Download or save the certificate as a PEM (.cer) file.
- **Download Signing Request:** Download or save the signing request as a .csr file.
- **Install Signed Certificate:** Upload a previously signed certificate.

Managing Other Access Functions

UNIVERSAL PRINT

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

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

Prerequisites

- Microsoft Azure AD Account
- Windows 10 Client version 1903 or higher

Universal Print Status

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

- `Device is not currently registered with Universal Print`: This status appears when Universal Print is not registered.
- `Waiting for user to authenticate`: This status appears when registration is in process and the device is waiting for the user to authenticate to Microsoft.com.
- `Waiting to finish registration`: This status appears when registration is in process and the user has authenticated to Microsoft.com.
- `Device is online and registered with Universal Print`: This status appears when registration is successful.
- `Successfully deregistered printer from Universal Print`: This status appears when your local device deregistration is successful.

Registering a Device for Universal Print

1. In the Embedded Web Server, click **Settings > Network/Ports > Universal Print**.
2. To change the default printer name, in the Printer Name field, enter a new name.
3. Click **Register**.

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

4. The Register Device window appears. To copy the registration code, click **Copy**, then click the displayed link: <https://microsoft.com/devicelogin>.



Note:

- The registration process needs to complete before the code expires.
 - The registration code expires after 15 minutes.
5. A Microsoft-managed Web page opens. Do the following:

- a. At the Enter code window, paste the registration code into the Code field, then click **Next**.
- b. At the Pick an account window, select the appropriate Microsoft® account.



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

- c. The Xerox Universal Print window appears. Click **Continue**, then close the window.
6. If the code expires or registration fails, the status appears as `Device is not currently registered with Universal Print` in the Universal Print area. Repeat the registration process.
7. If registration is successful, the status appears as `Device is online and registered with Universal Print` in the Universal Print area. The device is available as a cloud printer in the Universal Print service.
8. To allow users to access the device, the Azure® administrator needs to share the printer in the Microsoft® Azure® portal.
 - a. In a Web browser, go to <https://portal.azure.com/#home>, then log in using the account previously used to register the device.
 - b. For Azure services, click **Universal Print**.
 - c. In the Manage area, click **Printers**.
The list of registered printers appears.
 - d. Select your printer, then click **Share**.
The Share printers window appears.
 - e. To change the default printer name, update the Share name field for the cloud printer. A unique share name allows the users to easily identify the cloud printer in the network.
 - f. To allow access to the cloud printer for everyone in the organization, click the toggle button.
 - g. To select the users that you need to share the printer with, in the Select member(s) area, click the names of the users. To locate users, use the search by name option.
 - h. Click **Share Printer**. When printer sharing is complete, a confirmation message appears.
After the printer is shared, an authorized user can discover the device using the Add Printer feature in Windows 10. The device appears as a cloud printer in the discovered printers list.
9. To add a cloud printer in Windows 10 and later or Windows 10 and 11:
 - a. Click **Settings > Printers > Add a printer**.
 - b. Select the cloud printer in the list of discovered printers, then click **Add device**.

Administrator Functions for Universal Print

To Deregister your local device from Universal Print:

1. In the Embedded Web Server, click **Settings > Network/Ports > Universal Print**.
2. In the Registration area, click **Deregister**.
3. At the prompt, click **OK**.

4. Wait a few minutes until the displayed status changes to `Successfully deregistered printer from Universal Print`.
5. Click **Continue**.
6. To remove the printer from the Universal Print server, in a Web browser, go to the Azure portal <https://portal.azure.com/#home>, then log in with your credentials.
7. In the Azure portal, for Manage, click **Printers**, then select your printer.
8. Click **Delete Printer Share**, then click **OK**.
9. Click **Unregister**, then at the prompt, click **Unregister Printer**.

Upon completion, a message appears stating that `This printer has been successfully unregistered`. Additionally, the printer is removed from the list of registered devices.

SCHEDULING ACCESS TO USB DEVICES

In secure environments, you can configure devices to limit or disable the capabilities of USB host ports.

You can disable the front USB port using access control restrictions. Devices also have a rear USB port designed for card readers and human interface devices, such as a keyboard.

1. From the Embedded Web Server, click **Settings > Security > Schedule USB Devices**.
2. Select a device action, then specify when the device performs the action.
3. Click **Save**.

To reactivate use of the USB host ports, for each Disable schedule entry, create an Enable schedule entry.

You can create multiple schedules.

SETTING LOGIN RESTRICTIONS

To prevent malicious access to a device, you can restrict the number of invalid login attempts and require a lockout time before a user can try to log in again.


Many organizations establish login restrictions for information assets such as workstations and servers. Ensure that device login restrictions also comply with organizational security policies.

1. From the Embedded Web Server, click **Settings > Security > Login Restrictions**.
2. Set the login restrictions.
 - **Login Failures:** Specify the number of times a user can attempt to log in before being locked out.
 - **Failure Time Frame:** Specify how long a user can attempt to log in before lockout takes place.
 - **Lockout Time:** Specify how long the lockout lasts.
 - **Web Login Timeout:** Specify how long a user can be logged in remotely before being logged out automatically.
3. Click **Save**.


CONFIGURING CONFIDENTIAL PRINTING

Users that print confidential or sensitive information can use the confidential print option. This option allows print jobs to remain in the print queue until the user enters a PIN on the printer control panel.


1. From the Embedded Web Server, click **Settings > Security > Confidential Print Setup**.
2. Enter an option for the following:
 - **Max Invalid PIN:** Set the number of times an invalid PIN can be entered.
 - When the limit is reached, the print jobs for that user name and PIN are deleted.
 - This setting appears only when a formatted, working printer hard disk is installed.
 - To turn off this setting, type 0.
 - **Confidential Job Expiration:** Set the expiration time for confidential print jobs.
 - When set to **Off**, confidential held jobs are stored in the printer until they are released or deleted manually.
 - Changes in this setting do not affect the expiration time for confidential print jobs that are already in the printer memory or hard disk.
 - If the printer is powered off, then all confidential jobs held in the printer memory are deleted.
 - **Repeat Job Expiration:** Set the expiration time for a repeat print job.

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

 - **Verify Job Expiration:** Set the expiration time for job verification. After the printer prints the first copy, the printer waits until the expiration time, then prints the remaining copies.

 Note: The Verify Jobs option prints one copy to ensure that the quality is satisfactory before printing the remaining copies.


 - **Reserve Job Expiration:** Set the expiration time for reserve job storage. The printer stores print jobs until the expiration time.

 Note: Reserve held jobs are automatically deleted after printing.

 - **Require All Jobs to be Held:** Set the printer to hold all print jobs.
 - **Keep Duplicate Documents:** Set the printer to print other documents with the same file name without overwriting any of the print jobs.
3. Click **Save**.

ENABLING SOLUTIONS LDAP SETTINGS

1. From the Embedded Web Server, click **Settings > Security > Solutions LDAP Settings**.
2. Select one or more of the following:
 - **Follow LDAP Referrals:** Search the different servers in the domain for the logged-in user account.
 - **LDAP Certificate Verification**

 Note: To effectuate the changes, restart the device.

3. Click **Save**.

SHOWING SECURED APPLICATIONS OR FUNCTIONS ON THE HOME SCREEN

By default, the secured applications or functions are hidden from the printer home screen.

1. From the Embedded Web Server, click **Settings > Security > Miscellaneous**.
2. From the Protected Features menu, select **Show**.
3. Click **Save**.

ENABLING PRINT PERMISSION

Use this feature for cost control. Whether users are allowed to print color or black and white depends on the permission configuration for the user. For details, refer to [Managing Login Methods](#).

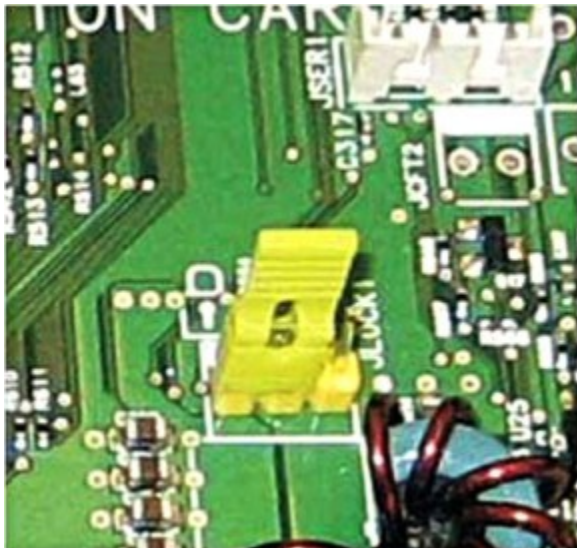
1. From the Embedded Web Server, click **Settings > Security > Miscellaneous**.
2. Select **Print Permission**.
3. Click **Save**.

ENABLING THE SECURITY RESET JUMPER

If the device is locked down because of a forgotten administrator password or lost network connectivity, to recover the device, you can reset it. Access the controller board and move the reset jumper to cover the middle and exposed prongs.

To ensure that the device is not maliciously reset, secure access to the controller board with a cable lock.

Warning—Potential Damage: Resetting the device deletes all customer data.



The secure reset feature requires that, in the Embedded Web Server, you specify the effect of using the security reset jumper, which is on the controller board.

1. From the Embedded Web Server, click **Settings > Security > Miscellaneous**.
2. From the Security Reset Jumper menu, select one of the following:
 - **Enable Guest Access:** Provide guests with full access control.
 - **No Effect:** All protected access controls remain protected.

Warning—Potential Damage: If this option is selected, then the device is locked down and you cannot access the security menus. To replace the device controller board and regain access to the security menus, a service call is required.

3. If required, in the Minimum Password Length field, type a value.
4. To enable the password or to reveal the PIN, click **Enable Password/PIN Reveal**.
5. Click **Save**.

Securing Data

CONFIGURING PRINTER SETTINGS



Note: Some settings are available only in some printer models.

1. From the Embedded Web Server, click **Settings > Device > Maintenance**.
2. Depending on the printer model, click **Config Menu** or **Configuration Menu**.
3. Configure the USB Configuration settings.
 - **USB PnP:** Change the USB driver mode of the printer to improve its compatibility with a personal computer.
 - **USB Speed:** Set the USB port to run at full speed and disable its high-speed capabilities.
4. Configure the Tray Configuration settings.
 - **Show Tray Insert Message:** Show a message about the tray status.
 - **A5 Loading:** Specify the page orientation when loading A5 paper size.
 - **Paper Prompts:** Set the paper source that the user fills when a prompt to load paper appears.
 - **Envelope Prompts:** Set the paper source that the user fills when a prompt to load envelope appears.
 - **Action for Prompts:** Set the printer to resolve paper- or envelope-related change prompts.
5. Configure the Reports settings.
Print reports about printer menu settings, status and event logs.
 - **Menu Settings Page**
 - **Event Log**
 - **Event Log Summary**
6. Configure the Supply Usage and Counters setting.
For the **Clear Supply Usage History**, reset the supply page counter or view the total printed pages.
7. Configure the Print Configuration settings.
 - **Font Sharpening:** Set a text point-size value below which the high-frequency screens are used when printing font data. For example, if the value is 24, then all fonts sized 24 points or less use the high-frequency screens.
 - **Print Density:** Adjust the toner density when printing documents.
8. Configure the Device Operations settings.
 - **Quiet Mode:** Set the printer to reduce the amount of noise that it makes when printing.



Note: This setting slows down the overall performance of the printer.

- **Panel Menus:** Set the printer to show the control panel menus.
 - **Clear Custom Status:** Erase all custom messages.
 - **Clear all remotely-installed messages**
9. Click **Save**.

ERASING PRINTER MEMORY

To erase volatile memory or buffered data in your printer, power off the printer.

To erase nonvolatile memory or individual settings, printer and network settings, security settings, and embedded solutions, do the following:

1. From the Embedded Web Server, click **Settings > Device > Maintenance**.
2. In the Erase Printer Memory section, select **Sanitize all information on nonvolatile memory**.
3. If required, in the After erasing all nonvolatile memory section, select either **Start initial setup wizard** or **Leave printer offline after erasing the printer memory**.
4. Click **Start**.

ERASING PRINTER HARD DISK MEMORY



Note: This process can take from several minutes to more than an hour. During this time, the printer is unavailable for other tasks.

The following instructions are available only in printer models with a hard disk installed.

1. From the Embedded Web Server, click **Settings > Device > Maintenance**.
2. In the Erase Hard Disk section, select **Sanitize all information on hard disk**.
3. Click **Start**.

CONFIGURING PRINTER HARD DISK ENCRYPTION



Note: Before performing this procedure, read the following information.

- Disk encryption erases the contents of the hard disk. If needed, back up important data from the printer before starting the encryption.
- Do not power off the printer during the encryption process. Loss of data can occur.
- Disk encryption can take from several minutes to more than an hour. During this time, the printer is unavailable for other tasks.

The following instructions are available only in printer models with a hard disk installed.

1. From the Embedded Web Server, click **Settings > Security > Disk Encryption**.
2. Click **Start encryption**.



Note: In the latest firmware version, disk encryption is by default enabled without the option to disable it.

RESTORING FACTORY DEFAULT SETTINGS



Note: Some settings are available only in some printer models.

1. From the Embedded Web Server, click **Settings > Device > Restore Factory Defaults**.

2. Select the settings that you want to restore.
 - **Restore printer settings:** Restore all the printer settings to their default values.
 - **Restore network settings:** Restore all the network settings to their default values.
 - **Restore app settings:** Restore all the app settings to their default values.
3. Click **Start**.

Troubleshooting

This chapter contains:

- Login Troubleshooting 56
- LDAP Troubleshooting..... 58
- Networking Problems..... 59

Login Troubleshooting

USER IS LOCKED OUT


To resolve the problem, try one or more of the following:

1. Update the allowed number of login failures and lockout time.


 Note: This solution is applicable only to some printer models.

It is possible that the user has reached the maximum allowed number of login failures.

2. From the Embedded Web Server, click **Settings > Security > Login Restrictions**.
3. Update the allowed number of login failures and the lockout time.
4. Click **Save**.

 Note: The new settings take effect after the lockout time expires.

5. Reset or replace the smart card.

 Note: Check whether the type of smart card that you are using can be reset. If the card cannot be reset, then replace the card.

USER IS LOGGED OUT AUTOMATICALLY

To resolve the problem, increase the Screen Timeout value.

1. From the Embedded Web Server, click **Settings > Device > Preferences**.
2. Increase the Screen Timeout value.
3. Click **Save**.

USER CANNOT ACCESS APPLICATIONS OR FUNCTIONS

Ensure that the user is assigned to a group that has access to the applications and functions.

For details, refer to [Managing Login Methods](#).

KDC AND PRINTER CLOCKS ARE OUT OF SYNC

Ensure that the date and time settings on the printer are correct.

For details, refer to [Setting the Date and Time](#).

DOMAIN CONTROLLER CERTIFICATE IS NOT INSTALLED

Ensure that the correct certificate is installed on the printer.

For details, refer to [Managing Certificates](#).

KDC IS NOT RESPONDING WITHIN THE REQUIRED TIME

To resolve the problem, try one or more of the following:

- Ensure that the IP address or host name of the KDC is correct.
- Ensure that the KDC is available in the configuration file. You can add multiple KDCs in the configuration file.
- Ensure that the server and firewall settings are configured to allow communication between the printer and the KDC server on port 88.

LDAP Troubleshooting

LDAP LOOKUPS FAIL

To resolve the problem, try one or more of the following:

1. Ensure that the server and firewall settings are configured to allow communication between the printer and the LDAP server on port 389 and port 636.
The default ports are port 389 and port 636.

If reverse DNS lookup is not used in your network, then disable Reverse IP Lookups in the Kerberos settings.
2. To disable Reverse IP Lookups:
 - a. From the Embedded Web Server, click **Settings > Security**.
 - b. In the Network Accounts section, click **Kerberos**.
 - c. In the Miscellaneous Settings section, select **Disable Reverse IP Lookups**.
 - d. Click **Save and Verify**.
3. If the LDAP server requires SSL, then enable SSL for LDAP lookups.
Some solutions that provide authentication require you to enable SSL for LDAP lookups.
4. Narrow the LDAP search base to the lowest possible scope that includes all necessary users.
5. Ensure that all LDAP attributes that are being searched for are correct.

Networking Problems

PRINTER IS NOT COMMUNICATING ON THE NETWORK

Try one or more of the following:

1. Check the network status.
 - a. From the Embedded Web Server, click **Reports > Network > Network Setup Page**.
 - b. In the Ethernet and/or Wireless section, check the Card Status.
 - c. If the printer is disconnected, for a wired connection, ensure that the Ethernet cable is properly connected.
 - d. If the printer is disconnected, for a wireless connection, check the printer wireless connection.
For details, refer to [Connecting to a Wireless Network](#).
2. Check the printer port access.
 - a. From the Embedded Web Server, click **Settings > Network/Ports > TCP/IP > TCP/IP Port Access**.
 - b. If necessary, enable ports.
For details, refer to [Configuring TCP/IP Port Access Settings](#).
 - c. Click **Save**.
3. Check the Restricted Server List.
 - a. From the Embedded Web Server, click **Settings > Network/Ports > TCP/IP**.
 - b. Locate the Restricted Server List, then check for the printer IP address.
 - c. If the printer IP address is listed, then remove it.
 - d. Click **Save**.
4. Ensure that communication is not blocked by a firewall or workplace VPN.

